

# **Digital Forensic Readiness for Wireless Local Area Networks**

by

**Sipho Josia Ngobeni**

Submitted in fulfilment of the requirements for the degree

**Magister Scientiae (Computer Science)**

in the

**Faculty of Engineering, Built Environment and Information Technology**

at the

**University of Pretoria**

June 2016

# Digital Forensic Readiness for Wireless Local Area Networks

by

Sipho Josia Ngobeni

Supervised by

Prof. H.S. Venter

Department of Computer Science

Magister Scientiae (Computer Science)

## Abstract

Over the past decade, wireless mobile communication technology based on the IEEE 802.11 Wireless Local Area Networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cybercrime. WLAN digital forensics is seen as not only a response to cybercrime in wireless networks, but also a means to stem the increase of cybercrime in WLANs. The main challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation on them. In an attempt to address this issue, the study presents firstly how a WLAN functions by simply studying the association mechanism between mobile stations and the Access Point (AP), and secondly how traffic is transmitted from a source to a destination address and the security attacks associated with such transmission. Furthermore, the dissertation analyses different digital forensic process models because every digital forensic investigation should follow a digital forensic investigation process. The study also looks at various tools for extracting the ever-increasing amount of evidential data that passes through the WLAN. These tools are scrutinised to observe if they possess any digital forensic capabilities and a model is proposed to implement digital forensic readiness in WLANs. The proposed model is designed to

monitor, log, preserve, analyse and report wireless network traffic for digital forensic investigations. Thus, the information needed by the digital forensic experts is rendered readily available, should it become necessary to conduct a digital forensic investigation. The availability of this digital information maximises the chances of its being used as digital evidence and reduces the cost of conducting the entire digital forensic investigation process. The proposed model is then translated into a prototype to show its viability. The results of the prototype are then analysed through experiments. The experiments were found to increase the usefulness of the forensically captured network traffic. The experiments showed that organisations that use WLANs can greatly benefit by deploying the forensic readiness model and if an incident were to be reported later on and a digital forensic investigation is warranted, the organisation would simple extract the forensically captured and stored data and conduct an analysis rather than conducting the investigation from the beginning. The dissertation also provides a critical analysis of the proposed solution and lastly, the dissertation provides the legal issues with regard to traffic interception in the South African context.

## **Keywords**

*Wireless Local Area Network, Access point, mobile station, association, basic service set, passive attacks, active attacks, digital forensics, digital forensic readiness, digital forensic process model, digital evidence, network traffic, monitoring, logging, preservation, hash value, prototype, experiments, Wireshark, Tshark, Kali Linux, Driftnet, and NetWitness Investigator.*

# Acknowledgements

I would like to express my sincere gratitude to the following people for their assistance during the preparation and completion of this dissertation:

- God – Thank you for the talents and strength you gave me to complete this research.
- Prof. Hein Venter – Thank you for your guidance and support, and for positioning my mind to realise that this research work is achievable.
- Ignatius Swart – Thank you sincerely for your continuous support and encouragement throughout the entire life cycle of the dissertation.
- Angel Shozi – Thank you so much for your contribution to the development of the prototype as a proof of concept.
- My parents – Thank you sincerely for your continuous support, love, and encouragement throughout the entire lifecycle of this dissertation.
- Gugulethu Mashele – Thank you sincerely for the undivided love, support and encouragement amidst difficult times.
- Isabel Claassen – Thank you sincerely for your assistance with emergency language editing, even at the most inconvenient of times.



# Table of Contents

<b>Abstract.....</b>	<b>I</b>
<b>Keywords .....</b>	<b>II</b>
<b>Acknowledgements .....</b>	<b>III</b>
<b>Table of Contents .....</b>	<b>IV</b>
<b>List of Figures.....</b>	<b>XI</b>
<b>List of Tables .....</b>	<b>XIV</b>
<b>Part I: Introduction .....</b>	<b>XV</b>
<b>Chapter 1 Introduction.....</b>	<b>16</b>
1.1 Introduction .....	16
1.2 Motivation for this Study .....	17
1.3 Problem Statement .....	18
1.4 Goal and Objectives .....	19
1.5 Research Methodology.....	20
1.6 Layout of the Dissertation .....	20
1.7 Concluding Remarks .....	23
<b>PART II: Background .....</b>	<b>24</b>
<b>Chapter 2 Wireless Local Area Networks .....</b>	<b>25</b>
2.1 Introduction .....	25
2.2 Wireless Local Area Network Architecture .....	26



2.2.1	Station .....	27
2.2.2	Access Point (AP) .....	27
2.2.3	Basic Service Set (BSS).....	27
2.2.4	Extended Service Set (ESS).....	29
2.3	WLAN Services .....	30
2.3.1	Station Services.....	30
2.3.2	Distribution System Services .....	31
2.4	Attacks Against Wireless Local Area Networks.....	33
2.4.1	Passive Attacks .....	34
2.4.1.1	War-driving .....	35
2.4.1.2	Eavesdropping.....	35
2.4.1.3	Evil Twin Attack .....	35
2.4.1.4	Shoulder-Surfing .....	35
2.4.2	Active Attacks.....	35
2.4.2.1	MAC Address Spoofing.....	36
2.4.2.2	ARP Spoofing .....	36
2.4.2.3	Denial-of-Service Attack.....	36
2.4.2.4	Man-in-the-Middle Attack .....	36
2.4.2.5	Session Hijacking.....	37
2.4.2.6	Attack Against WEP .....	37
2.5	Concluding Remarks .....	37

<b>Chapter 3 Digital Forensics and Digital Forensic Readiness.....</b>	<b>38</b>
3.1 Introduction .....	38
3.2 Defining Digital Forensics .....	38
3.3 Digital Forensic Process Models.....	39
3.4 Defining Digital Forensic Readiness.....	44
3.4.1 Usefulness of Incident Evidence Data .....	44
3.4.2 The Cost of Digital Forensics During an Incident Response.....	45
3.5 Achieving Digital Forensic Readiness .....	46
3.6 Concluding Remarks .....	47
<b>Chapter 4 Wireless LAN Digital Forensics .....</b>	<b>48</b>
4.1 Introduction .....	48
4.2 Defining WLAN Digital Forensics .....	49
4.3 WLAN Traffic Monitoring Tools .....	49
4.3.1 Types of Packet Sniffers .....	50
4.3.1.1 Wireshark .....	50
4.3.1.2 Tcpcmdump.....	51
4.3.1.3 Kismet .....	51
4.3.2 DF Challenges Associated with Packet Sniffers.....	52
4.4 Concluding Remarks .....	53
<b>PART III: Modelling .....</b>	<b>54</b>
<b>Chapter 5 The Wireless Digital Forensic Readiness Model.....</b>	<b>55</b>

5.1	Introduction .....	55
5.2	Block Diagram of the Wireless Digital Forensic Readiness Model.....	56
5.2.1	Traffic Monitoring .....	57
5.2.2	Logging .....	58
5.2.3	Preservation of Logs .....	60
5.2.4	Analysis and Reporting.....	61
5.3	The WDFRM as an Integrated Whole.....	63
5.4	Concluding Remarks .....	65
<b>PART IV: Prototype and Experiment Tools .....</b>		<b>66</b>
<b>Chapter 6 Prototype Tools .....</b>		<b>67</b>
6.1	Introduction .....	67
6.2	Tools Used to Develop the Prototype .....	68
6.2.1	Computer/ Physical System Requirements .....	68
6.2.2	Microsoft Visual Studio Express 2012 for Windows Desktop.....	69
6.2.3	Tshark .....	70
6.2.4	Microsoft SQL Server 2012 Management Studio .....	71
6.2.5	Hash Utility - HashIt.....	71
6.3	Tools Used to Conduct the Experiments.....	73
6.3.1	Wireshark.....	73
6.3.2	NetWitness Investigator.....	74
6.4	Concluding Remarks .....	75

<b>Chapter 7 Prototype Development .....</b>	<b>76</b>
7.1 Introduction .....	76
7.2 Prototype Setup .....	77
7.3 Phase 1 (Monitoring).....	78
7.4 Phase 2 (Logging) .....	79
7.5 Phase 3 (Preservation).....	82
7.5.1 Hashing .....	82
7.5.2 Hashing Verification.....	84
7.6 Concluding Remarks .....	86
<b>Chapter 8 Prototype Experiments.....</b>	<b>87</b>
8.1 Introduction .....	87
8.2 Phase 4 (Analysis) – Prototype Experiments .....	87
8.2.1 Experiment 1: Identifying Illegal Usage of Corporate Resources .....	88
8.2.1.1 Purpose of the Experiment.....	88
8.2.1.2 Test Scenario.....	88
8.2.1.3 Execution of the Experiment .....	88
8.2.2 Experiment 2: Identification of Email Containing Company Trade Secrets .....	99
8.2.1.1 Purpose of the Experiment.....	99
8.2.1.2 Test Scenario.....	99
8.2.1.3 Experiment Setup.....	99
8.2.1.4 Execution of the Experiment .....	102

8.2.3	Experiment 3: Man-in-the-Middle Attack .....	107
8.2.3.1	Purpose of the Experiment .....	107
8.2.3.2	Test Scenario.....	108
8.2.3.3	Experiment Setup.....	108
8.2.3.4	Execution of the Experiment .....	109
8.3	Phase 5 (Reporting).....	115
8.4	Concluding Remarks .....	116
<b>PART V: Conclusion .....</b>		<b>118</b>
<b>Chapter 9 Critical Evaluation of the WDFRM.....</b>		<b>119</b>
9.1	Introduction .....	119
9.2	Wireless Digital Forensic Readiness Model .....	119
9.3	WLAN Digital Forensic Readiness Prototype .....	120
9.3.1	Digital Forensic Readiness .....	120
9.3.2	Forensic Analysis of Network Traffic .....	121
9.4	Evaluation of the Wireless Digital Forensic Readiness Model.....	123
9.4.1	IEEE 802.11 Performance and Characteristics .....	123
9.4.2	Average Data Rate of an IEEE 802.11g AP .....	124
9.4.3	Expert Opinion.....	124
9.5	Legal Issues with Regard to Interception of Communication.....	125
9.6	Limitations of the WDFRM .....	126
9.7	Concluding Remarks .....	127

<b>Chapter 10 Conclusion .....</b>	<b>129</b>
Final Remarks .....	129
<b>Bibliography .....</b>	<b>132</b>
<b>Appendix A: Source Code .....</b>	<b>143</b>
A.1 Hash File.....	143
A.2 Data Access Component .....	146
A.3 Hash Table.....	148
A.4 Design.....	149
A.5 Application Configuration.....	151
<b>Appendix B: Published Papers .....</b>	<b>152</b>

# List of Figures

Figure 1.1. A graphical representation of the layout of the dissertation.....	21
Figure 2.1. Independent basic service set .....	28
Figure 2.2. Infrastructure basic service set .....	29
Figure 2.3. Extended service set .....	30
Figure 2.4. Passive eavesdropping.....	34
Figure 4.1. Relation of WLAN digital forensics.....	49
Figure 5.1. Block diagram of the WDFRM .....	57
Figure 5.2. Traffic monitoring component .....	58
Figure 5.3. Traffic logging component .....	59
Figure 5.4. Preservation component .....	61
Figure 5.5. Analysis and reporting.....	62
Figure 5.6. Wireless digital forensic readiness model .....	64
Figure 6.1. Prototype and experiment tools .....	67
Figure 6.2. Microsoft Visual Studio .....	69
Figure 6.3. Tshark.....	70
Figure 6.4. SQL server.....	71
Figure 6.5. HashIt .....	72
Figure 6.6. HashIt utility.....	72
Figure 6.7. Wireshark .....	73
Figure 6.8. NetWitness Investigator .....	74
Figure 7.1. Wireless digital forensic readiness model (duplication of Figure 5.6).....	77
Figure 7.2. Overview of prototype setup .....	78
Figure 7.3. Start or stop capturing network traffic.....	80



Figure 7.4. One output file of Tshark .....	81
Figure 7.5. Two output files of Tshark .....	81
Figure 7.6. Ten output files of Tshark .....	82
Figure 7.7. Dialog box indicating that traffic capturing has been stopped .....	83
Figure 7.8. MD5 and SHA-1 of output file number 00001 .....	84
Figure 7.9. MD5 and SHA-1 of output file number 00002 .....	85
Figure 7.10. MD5 and SHA-1 of output file number 00003 .....	85
Figure 8.1. Ten output files of Tshark (duplication of Figure 7.6).....	89
Figure 8.2. Output file replayed in Wireshark .....	89
Figure 8.3. Choosing the “Follow TCP Stream” option .....	90
Figure 8.4. The “Follow TCP Stream” dialog box .....	91
Figure 8.5. Merging pcap files with Wireshark .....	92
Figure 8.6. MD5 and SHA-1 hash values of the merged pcap file.....	93
Figure 8.7. Creating a new local collection in NetWitness Investigator .....	94
Figure 8.8. Specifying a directory for a local collection.....	94
Figure 8.9. Importing the merged pcap file .....	95
Figure 8.10. Viewing packets in the merged pcap file .....	95
Figure 8.11. Detailed view of the packets in the merged pcap file.....	96
Figure 8.12. Extraction of files from common protocols into a directory .....	96
Figure 8.13. Specifying the type of files to be extracted from the merged pcap file.....	97
Figure 8.14. Files extracted from the merged pcap file .....	98
Figure 8.15. Digital evidence – mp3 audio files .....	98
Figure 8.16. Ten output files of Tshark (duplication of Figure 7.6).....	100
Figure 8.17. Setup and configuration of Experiment 2.....	101
Figure 8.18. Merged pcap files of Figure 8.16 .....	103

Figure 8.19. Resolving the noipmail.com email server to an IP address.....	103
Figure 8.20. Filtered SMTP traffic .....	104
Figure 8.21. Following TCP stream of packet number 2001.....	105
Figure 8.22. Man-in-the-middle attack experiment setup.....	109
Figure 8.23. Determining the IP address of the Kali Linux machine – attacker.....	110
Figure 8.24. Determining the address of the gateway .....	111
Figure 8.25. Determining the IP address of the legitimate user.....	111
Figure 8.26. Pinging the legitimate user .....	111
Figure 8.27. Determine IP forwarding .....	112
Figure 8.28. The attacker convinces the gateway that it is the legitimate user.....	113
Figure 8.29. The attacker convinces the legitimate user that it is the gateway.....	114
Figure 8.30. Determine content accessed by the legitimate user .....	114
Figure 8.31. Driftnet - digital evidence.....	115

# List of Tables

Table 2.1. Summary of WLAN services.....	33
Table 3.1. Summary of digital forensic process models.....	43
Table 7.1. Tshark flags.....	80
Table 7.2. SQL server database with MD5 and SHA-1 hash values of Tshark output files....	83
Table 7.3. Excel Hash Table with MD5 and SHA-1 hash values of the Tshark output files ..	83
Table 7.4. Comparison of MD5 and SHA-1 hash table for the prototype and HashIt.....	85
Table 9.1. IEEE 802.11 specification .....	123

# Part I: Introduction

## Chapter 1 Introduction

### 1.1 Introduction

Information technology has evolved tremendously over the years. For example, the Internet which is the largest of all networks, is now affecting virtually every aspect of our daily lives, just as electricity once did. Today, a large number of individuals depend on information technologies such as mobile phones that are equipped with third-generation (3G) technology to surf the web, manage appointments and social networking, do online banking and shopping, and navigate through streets using Global Positioning Systems (GPS) – to mention but a few. This not only shows that the Internet has been embraced wholeheartedly by mankind, but also implies that the legacy networks have become inadequate to meet the dynamic expectations of a modern lifestyle. The next-generation network (NGN), in turn, provides even more exciting and state-of-the-art possibilities for wireless networking (Ergen, 2004; ITU-T, 2006; Mouton, 2012; Adamczyk et al., 2007; ITU-T, 2004). One example of an exciting NGN includes the Wireless Local Area Network (WLAN), which is discussed in more detail in this dissertation.

One would agree that even though such information technologies provide some benefits in our daily lives, they also possess a dark side in the form of Internet fraud. Internet fraud takes many forms, for example, from phony items offered for sale on eBay, scurrilous rumours that manipulate stock and market prices, to scams that promise great riches should the victim help to facilitate a foreign financial transaction by offering his own bank account, and many other scams that play with the innocent mind of a computer user (Wu, 2006; Huang et al., 2009). This type of Internet fraud is called phishing (Jakobsson and Myers, 2007).

As new technologies such as Wireless Fidelity (Wi-Fi) or WLAN emerge, a paradigm shift often occurs with regard to the way in which mobile devices communicate with the access point. The biggest advantages provided by WLAN are its mobility, coverage and broadcasting over the Industrial, Scientific and Medical (ISM) band (ICASA, 2015). These characteristics all provides the “any-where” and “any-time” connectivity (Souppaya and Scarfone, 2012; Ergen, 2004; Salem et al., 2005), which in turn, enables the mobile client to join and leave the WLAN at any time.



The open nature of the WLAN environment often makes it a perfect breeding ground for pernicious individuals to launch vicious security attacks. For example, in 802.11 WLAN, Medium Access Control (MAC) addresses are often openly broadcasted over the air. The attackers can therefore sniff and spoof these MAC addresses associated with authorised users, a scheme called MAC identity spoofing (Lackner et al., 2009).

One of the major threats of WLAN that can be orchestrated by the MAC identity spoofing is the Denial of Service (DoS) attack where malicious individuals flood the WLAN with large amounts of network traffic, which in turn may exhaust the resources of the WLAN (Arockiam et al., 2012). The situation is even worse because sophisticated attacks on WLANs usually occur at the hardware level, so even security protocols such as WEP, WPA, WPA2 and WLAN security often have no effect (Humble and Sundholm, 2004; Gupta and Garg, 2010). To respond to all these threats, the Scientists have adopted the digital forensics discipline which is a product of the law enforcement to help retrieve digital evidence from Wireless LANs. This strategy is discussed in more detail in this dissertation.

The remainder of this chapter is structured as follows: Section 1.2 provides the motivation for this research, which gives the reader a brief overview of WLAN and discusses the foreseeable problems within WLAN. In Section 1.3 the reader is introduced to the research problem focused on by the researcher and given an overview of how the research problem is addressed. The reader is then provided with the goal and objectives of this dissertation in Section 1.4, and the research methodology in Section 1.5. Chapter 1 is concluded with a brief summary that provides an overview of the chapters to follow.

## 1.2 Motivation for this Study

The research undertaken for this study was motivated by several realisations, which are discussed below.

The first realisation is that wireless technologies have become very popular around the world. WLANs or “hotspots” blanket public places such as convention centres, airports, schools, railway stations, coffee shops and other locations to provide seamless public access to the Internet (Velasco et al., 2008). These hotspots provide several advantages over hard-wired networks, including user mobility and flexibility of Internet access.

However, due to their open nature, WLANs remain an attractive target for a large number of security attacks (Nguyen et al., 2008; Lackner et al., 2009). The second realisation is that electronic data may be deleted or changed easily. It is therefore of paramount importance to collect and preserve it as quickly as possible. Also, in wireless networks, network traffic may only exist for a split second, and information stored in volatile computer memory may only exist for a few hours. Due to their volume, log files may be retained for a few days. However, attackers with the necessary skills can destroy or modify digital evidence to protect themselves (Casey, 2007).

The third realisation is that digital forensics often involves working with a large volume of data. Therefore, searching for specific digital evidence in a large volume of network traffic would be like looking for a needle in a haystack (Dripps, 2013; Casey, 2007).

The fourth realisation is that, locating and preserving digital evidence is even more difficult when intruders are actively attempting to conceal and destroy digital evidence. In addition, when intruders use customised toolset to commit crime, it may even be more challenging to apprehend them (Casey, 2006).

Having introduced the reader to the realisations that motivated the researcher to conduct this research, the next section explores the problem statement that constitutes the focus of this study.

### **1.3 Problem Statement**

The advantages of using a WLAN represent only one side of the coin; the fact is that it faces some challenges as well. For example, conducting a digital forensic investigation in a WLAN environment is problematic. This is because a WLAN is an open environment where mobile clients join and leave the network at any time, making it a real challenge to monitor and/or seize and investigate these mobile devices. By the time the investigation is required, the devices have long since left the network and communications have long been lost. Even when used legitimately to analyse protocols, packet sniffers are prone to miss some of the packets that pass through the network (Broadway et al., 2008). This is because packet sniffers are configured in such a way that they must be able to receive a packet, save it to disk and return

to the listening mode before the next packet arrives (Broadway et al., 2008; Casey, 2004). The large amount of traffic that passes through the network makes it difficult for packet sniffers to capture and store the data of all the packets that are received (Broadway et al., 2008; Casey, 2004). The result is that the digital information being collected is often incomplete.

The main problem in WLAN digital forensics is an inability to intercept and preserve all the communications generated by mobile devices on the networks and hence a failure to conduct a proper digital forensic investigation. This problem is exacerbated by the fact that network traffic exists only for a short period of time, and because of its large volume, it can only be retained for a short period of time before storage space is depleted. It is evident that WLANs are not forensically ready to gather enough digital information to be used for successful digital forensic investigations. Therefore, the research question for this dissertation is that: Is it possible to intercept and preserve all the communications generated by the mobile devices in a WLAN and conduct a digital forensic investigation?

The purpose of this research therefore is to design a Digital Forensic Readiness Model and implement it in a form of prototype to help log, monitor, preserve, analyse and report digital evidence in a forensically sound manner.

## 1.4 Goal and Objectives

The goal of this dissertation is to design a Wireless Digital Forensic Readiness Model (WDFRM) that can help to monitor, log and preserve wireless network traffic for subsequent digital forensic investigation. The specific objectives that are pursued as part of the goal above are as follows:

- (i) Analyse existing related work on WLANs, on digital forensics and digital forensic readiness, as well as on wireless digital forensics.
- (ii) Design the Wireless Digital Forensic Readiness Model (WDFRM).
- (iii) Develop a prototype of the WDFRM as a proof of concept.
- (iv) Interpret the results of the prototype through experiments.



## 1.5 Research Methodology

The research approach followed in this study involves four methods: literature review, modelling, development and analysis. A more detailed description of these methods follows below:

1. *Literature review*: This part involves conducting a state-of-the-art literature survey on WLANs, digital forensics and digital forensic readiness, as well as wireless digital forensics in order to determine related work in these areas of interest.
2. *Modelling*: The theoretical knowledge gained from the literature review is used as the basis for formulating the Wireless Digital Forensic Readiness Model (WDFRM) that can help monitor, log and preserve wireless network traffic for digital forensic investigations.
3. *Prototyping*: A prototype is developed to validate the implementation of digital forensic readiness in a WLAN environment.
4. *Experimentation*: The developed prototype is analysed through experiments.

## 1.6 Layout of the Dissertation

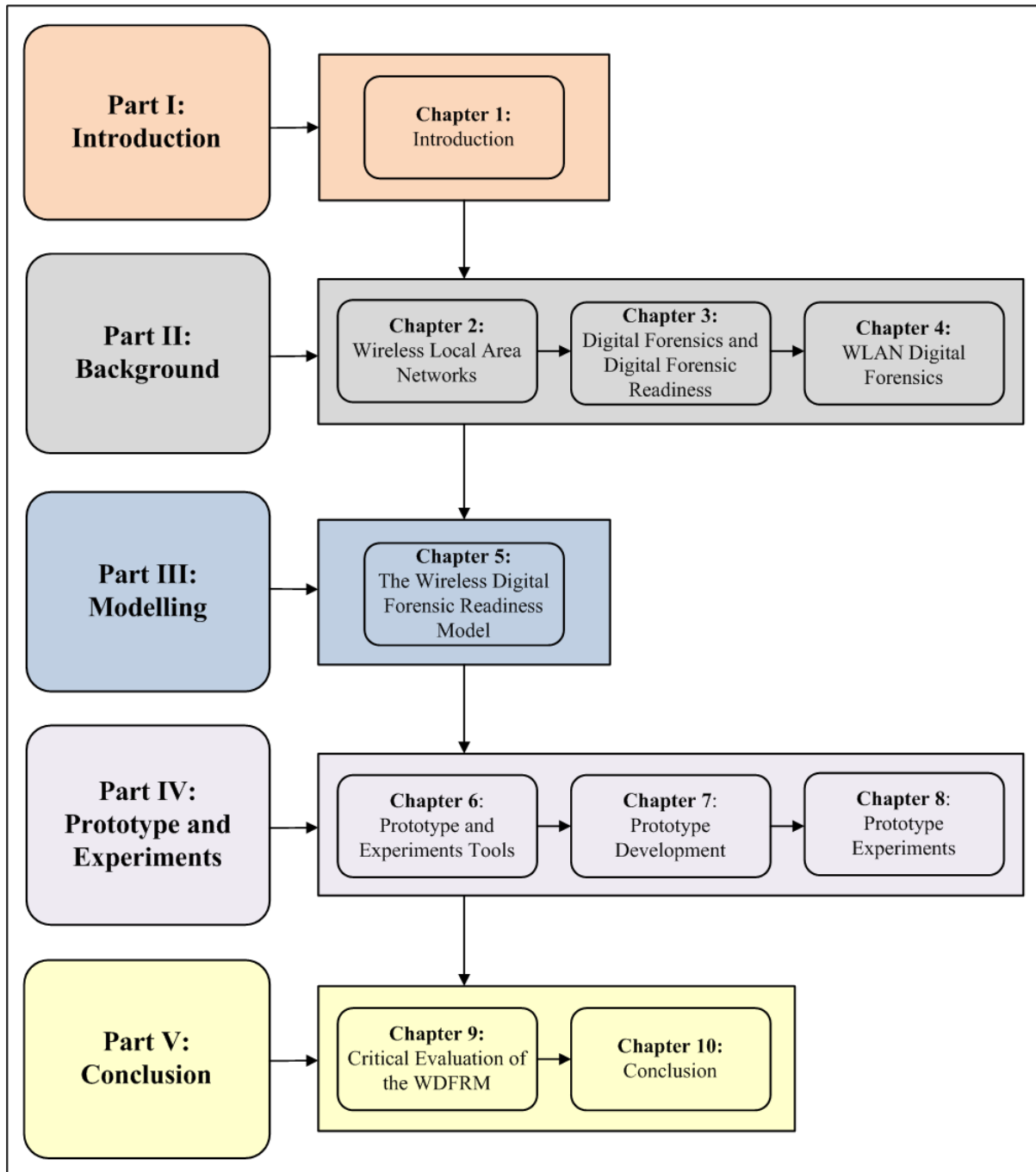
This dissertation consists of ten chapters divided into five parts. Figure 1.1 gives a graphical representation of the overall layout of the dissertation and the relationship among the chapters.

Part I consists of Chapter 1, which serves as the introduction to the entire research. The research problem, motivation, goal and objectives, and methodology are introduced in this chapter.

Part II consists of three chapters, namely Chapters 2, 3 and 4. In general, this part gives to the reader the necessary background information on the area of interest of this dissertation.

Chapter 2 in particular provides the reader with background knowledge on Wireless Local Area Networks (WLANs) and starts off by presenting an overview on wireless network technologies in general. The chapter proceeds by presenting various components of WLAN architecture with a view to understanding the association mechanism between a mobile station and an access point. The chapter further points out how network traffic is transmitted from the source address to the intended destination address.

A WLAN is said to be vulnerable to a number of security attacks that are classified into either passive or active. A discussion of these security attacks is also presented in Chapter 2.



**Figure 1.1.** A graphical representation of the layout of the dissertation

Chapter 3 focuses briefly on digital forensics and digital forensic readiness as the underlying concepts in the dissertation as a whole. Since it is necessary to understand the concept of digital forensics before embarking on the concept of digital forensic readiness, the chapter starts off by defining the former.

It proceeds by presenting the concept of digital forensic readiness, as the main goal of this research is to implement digital forensic readiness in a WLAN environment. Chapter 3 concludes by presenting a set of requirements that are necessary for achieving digital forensic readiness.

Chapter 4 presents a background study on WLAN digital forensics. The chapter starts off with a brief overview of WLAN digital forensics in general, after which various tools are explored for intercepting the traffic that flows through the WLAN. The tools are then critically scrutinised to observe if they possess any digital forensic capabilities, and the technical challenges associated with WLAN digital forensics are studied.

Part III and Part IV constitute the ‘contribution’ parts of this dissertation. Part III consists of one chapter, Chapter 5, devoted to the model proposed in this research. The chapter starts off with an overview of the proposed model in a form of black box, which gives the user a holistic view of the entire model without delving into details about the functions of every component. Chapter 5 next explains each component of the proposed model on a high level to illustrate its contribution towards addressing the problem statement. The components are subsequently integrated to give a full picture of the proposed model before the focus shifts to the phases of the digital forensic process as adopted by the proposed model.

Part IV consists of three chapters, Chapters 6, 7 and 8. This part is devoted to the development of a prototype as a means to prove the viability of the proposed model. Chapter 6 introduces the reader to the various sets of tools that are used to develop the prototype and to conduct the experiments. Chapter 7 deals with the development of the prototype and the implementation of digital forensic readiness in a WLAN environment. The prototype shows how traffic is captured from a WLAN and stored in a digitally forensic sound manner to maintain its integrity. Chapter 8 presents the actual two prototype experiments and their analysis of the network traffic that was captured and stored (as described in Chapter 7). An additional wireless specific prototype is also presented.

Part V, which contains two chapters, Chapters 9 and 10, is devoted to the conclusion of the entire dissertation. Chapter 9 highlights the two main contributions that this research has made.

It further explains why these items should be considered contribution to the field of WLAN digital forensics. The chapter proceed by presenting an expert opinion, to show that employing digital forensic readiness in a WLAN environment can minimise the cost and time needed to conduct a fully-fledged digital forensic investigation. The chapter continue by providing a brief summary of legal issues with regard to traffic interception in the South African context. The chapter further discusses a more critical analysis of the proposed solution and its disadvantages. The chapter is then concluded with a brief summary. Chapter 10 concludes the research undertaken in this dissertation by outlining the extent to which the research problem has been solved and suggests possible areas of future research. Appendices and the bibliography of resources consulted in this research are listed at the end of the dissertation.

## **1.7 Concluding Remarks**

Chapter 1 introduced the reader to the research problem addressed in this dissertation. The motivation, goal, objectives and methodology of the research, as well as the layout of the dissertation, are also presented in this chapter.

The next part, Part II of the dissertation covers the background sections that deal with WLANs, digital forensics and digital forensics readiness as well as WLAN digital forensics.

## **PART II: Background**



## Chapter 2      **Wireless Local Area Networks**

### **2.1 Introduction**

Wireless networks are classified into three main categories, i.e. Wireless Wide Area Networks (WWANs), Wireless Personal Area Networks (WPANs), and Wireless Local Area Networks (WLANs). The WWAN uses cellular technologies and covers a wide geographic area. WPAN has a short coverage range of up to 100m, and the most talked about technologies of this type of wireless network are Bluetooth and infrared (IR). A WLAN also spans a finite coverage range for example at an airport, a university, coffee shop, hospital or railway station, and its popular networking technology is the Institute of Electronic and Electrical Engineering (IEEE) 802.11 standards (Al-Wakeel, 2009; Karyagiannis and Owens, 2008). The WLAN is the key focus of this chapter.

Wireless Local Area Networks (WLANs) are based on a ubiquitous technology that provides seamless internet connectivity at public locations. It utilises and uses electromagnetic waves that are spread by spectrum technology and depends on high-speed radio waves to transfer data in the form of signals between nodes within a limited area (Negus and Petrick, 2008). Unlike traditional Local Area Networks (LANs), a WLAN can connect computers to the network without any physical or wired connections and can also be point-to-point without using access point. This suggests that the devices participating in a WLAN environment can move around the network within a broader coverage range without experiencing disruption in network connectivity (Rahman, 2009).

The essence of Chapter 2 is to provide the reader with some background on Wireless Local Area Networks. When taking a closer look at the history of wireless networks, it appears that the first WLAN was developed in 1971 by researchers at the University of Hawaii. This WLAN was named ALOHAnet (Schwartz and Abramson, 2009), designed as a bi-directional star topology consisting of seven computers that were made to communicate with a central station without using any telephone lines for connection or data transfer. At this time, WLAN hardware proved to be extremely expensive for most vendors, and was only used as an alternative to wired LANs in places where it was impossible to use cables for data transfer purposes (Rahman, 2009). The early improvement of WLAN technologies included vendor-specific solutions and proprietary protocols. However, in the late 1990s these were replaced by the IEEE 802.11 standards. Vendors began introducing products that operated within the



900 Megahertz(MHz) frequency band and the data transfer rate of a WLAN were estimated to be approximately 1 to 2 Megabits per second (Mbps). At this time, the wired LANs had a data transfer rate of 10Mbps, thus the WLAN was even slower than its counterpart. In 1992, the market started selling WLAN technologies that operated at a 2.4 Gigahertz (GHz) frequency band, which proved to be faster compared to the 900MHz. However, the 2.4 GHz frequency band was expensive and more prone to radio interference, and it was designed to use only proprietary Radio Frequency (FR) technologies (Scarfone et al., 2008).

As part of the current research, a literature study was conducted to identify the components that constitute the basic architecture of a WLAN, and to determine how wireless traffic is nowadays forwarded from one mobile client to another through the access point. The next section (2.2) therefore presents the WLAN architecture. This is important to discuss in this dissertation in order to ensure that the reader understands how a WLAN functions. The chapter proceeds by presenting the different WLAN services in Section 2.3. These services introduce the reader to how a mobile station associates with and get authenticated to an access point (AP); and how the AP transmits a frame or packet from the source to the destination.

Despite the convenience provided by a WLAN, every technology is said to possess its own dark side. A WLAN is an open environment, which renders it vulnerable to quite a number of security attacks. To substantiate this, the chapter shifts its focus in Section 2.4 and discusses some of the attacks that may threaten the security of a WLAN.

## 2.2 Wireless Local Area Network Architecture

The art of assembling computer hardware components is called computer architecture. Similarly, when this technique is applied in WLANs, it is called WLAN architecture. Section 2.2 briefly describes several elements that make up WLAN architecture. WLAN has two types of network elements, namely stations (STAs) and access points (APs). When these actors are combined, they can form a network categorised as a Basic Service Set (BSS), Infrastructure Basic Service Set (IBSS), and Extended Service Set (ESS). Below follows a description of the WLAN elements with different networks that can be formed by these elements.



### 2.2.1 Station

A station is a device with the conformant of the IEEE 802.11 Medium Access Control (MAC) and Physical Layer (PHY) to the wireless medium (Yang et al., 2005). Examples may include a laptop, handheld device, desktop, surveillance equipment, and an Access Point (AP). As the IEEE 802.11 and its variants continue to increase in popularity, many other types of devices could be stations as well, such as scanners, printers and digital cameras.

### 2.2.2 Access Point (AP)

An AP is an entity of a WLAN that has the station functionality and it logically connects the station to the wired Local Area Network (LAN) (Yang et al., 2005). It acts as a communication hub that can transmit and receive WLAN radio signals. In general, an AP is analogous to the base station used in cellular phone networks.

### 2.2.3 Basic Service Set (BSS)

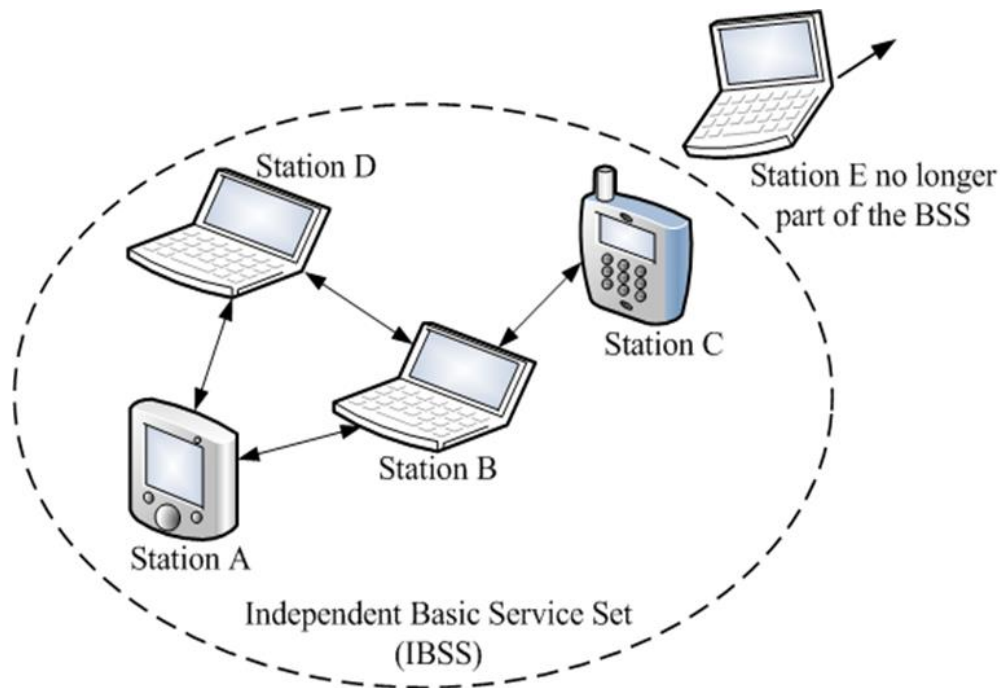
The BSS is the simplest and most fundamental structure of the IEEE 802.11 WLAN architecture. It consists of a set of stations that communicate with one another in a peer-to-peer or ad hoc mode (Ergen, 2002). In a BSS, stations are mobile and there is no backbone infrastructure or relay connection to the wired network. A BSS configured in this way is called an Independent BSS (IBSS). Figure 2.1 gives a graphical representation of an IBSS. In an IBSS, mobile stations communicate directly with one another. However, not every mobile station may be able to communicate directly with every other mobile station, but they all belong to the same IBSS. If one station must communicate with another station, the two stations must be in direct communication range.

It is important to note that the association between a station and a BSS within an IBSS constitutes a dynamic relationship. This suggests that a mobile station can join or leave the BSS at any time, and a station only becomes part of the BSS when it joins the BSS structure. It can be noted in Figure 2.1 that station E is no longer associated with the BSS structure; hence it cannot communicate with any of the other stations (A, B, C and D).

An IBSS is said to be a short-lived network with a small number of stations, that is, two or more stations that are created for a particular purpose (e.g. exchanging data with a vendor in



the lobby of the company's building or even collaborating on a presentation at a conference) (Ilyas and Ahson, 2005; Sherman, 2007).

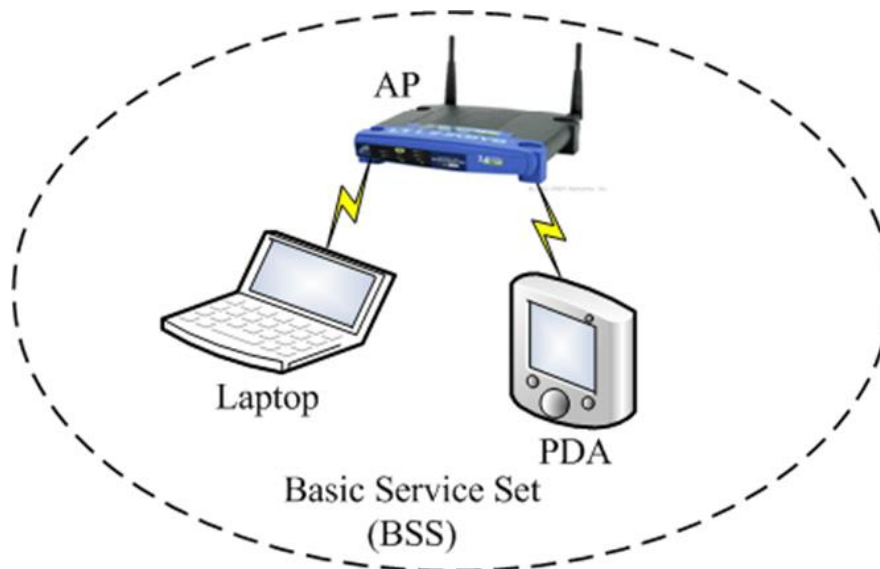


**Figure 2.1.** Independent basic service set

Though it is convenient to set up an ad hoc network, managing a large number of nodes is still a challenge; thus, it should be used only when security is not an issue.

When a BSS includes an AP, the BSS is no longer independent and it is called an infrastructure BSS. However, it is often still referred to as a BSS. In an infrastructure BSS, all mobile stations communicate with the AP. The AP in a BSS provides both the connection to the wired LAN, if any, and the locally relayed function for the BSS. Therefore, if one mobile station must communicate with another mobile station within the same BSS, the communication must be sent first to the AP and then from the AP to the other mobile station (O'Hara and Petrick, 2005). Figure 2.2 gives a diagrammatical illustration of the infrastructure BSS.

A BSS configured like that in Figure 2.2 confines the mobility of the mobile stations to a limited range, for example in a cafe, restaurant, lecture hall, conference room, etc. On the other hand, large-sized areas such as office complexes, apartment buildings, hospitals, factories, university campuses and warehouses cannot be covered by a single BSS but need to be covered by an ESS, which is described next.



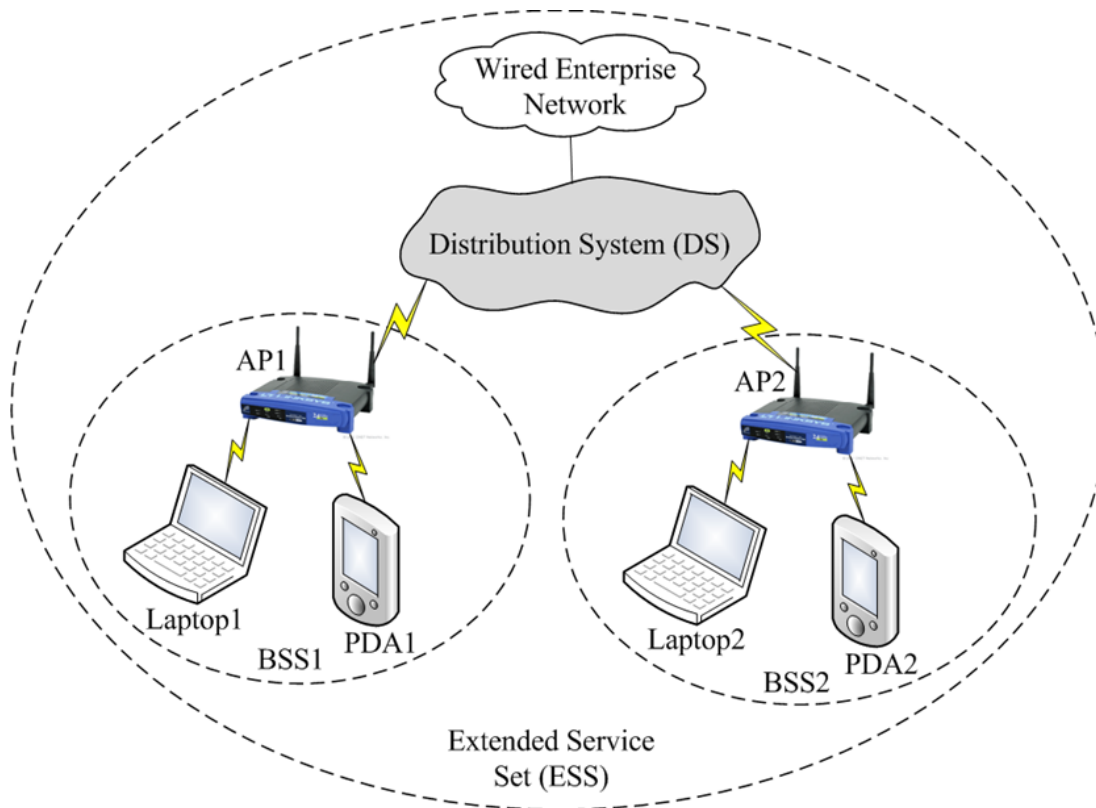
**Figure 2.2.** Infrastructure basic service set

#### 2.2.4 Extended Service Set (ESS)

The IEEE 802.11 extends the range of mobility of the mobile stations to an arbitrary range through an architectural component called an Extended Service Set (ESS). An ESS is viewed as a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The AP performs all the communications through an abstract layer called the Distribution System (DS). The DS acts as the backbone component of a WLAN and may be constructed of either wired or wireless connections. The DS determines if communication received from the BSS should be relayed back to a destination in the BSS, forwarded on the DS to another AP, or sent into the wired network infrastructure to a destination not in the ESS. Communications received by the AP from the DS is sent to the BSS to be received by the destination mobile station (O'Hara and Petrick, 2005). Figure 2.3 gives a diagrammatical illustration of the ESS. In an ESS, it should be noted that all the APs can also be stations and as such they have addresses.

Another component of the ESS is the Distribution System (DS), which is a system component, used to interconnect a set of BSSs and integrated LANs (Yang et al., 2005). The DS enables mobile station support in a WLAN by providing logical services necessary to perform address-to-destination mapping and seamless integration of multiple BSSs (Mullet,

2006). Since the DS is not necessarily a network, the IEEE 802.11 standard does not place any restrictions on how the DS should be implemented, but only on the network services it provides. The network services referred to here are described in the following section.



**Figure 2.3.** Extended service set

## 2.3 WLAN Services

One way to define a wireless network is to look at the services it provides. The IEEE 802.11 standard provides the station services and Distribution System (DS) services as part of the DS functions for moving data and network management operations. The services are discussed next.

### 2.3.1 Station Services

The DS consists of four station services as described by the IEEE 802.11 standard, namely authentication, deauthentication, privacy and data delivery. These services are implemented in all the stations of the 802.11 WLAN, including the APs, and are discussed below. The main objective of the services is to provide the security and data delivery functions of the messages that traverse the vulnerable wireless link.



- **Authentication** – This is a process whereby a station verifies who it claims to be, usually based on its identity (Bansal and Lalar, 2007). Similarly, if a station wants to join the WLAN, it must first authenticate itself by verifying its identity to the AP before any communication can commence. In 802.11, the identity of any mobile station is a Medium Access Control (MAC) address (Gast, 2002). Unless such proof of identity is provided, a station will not be able to join the wireless network and use the available resources.
- **Deauthentication** – This is the opposite of authentication, and usually takes place at the end of a session to terminate association between a station and an AP (Wood, 2008). When a previously authenticated station wants to leave the WLAN, it must first send a deauthentication frame to the AP. The deauthentication service will then be used to terminate the service of the mobile station and prevent any further use of the network resources (Nguyen, 2008).
- **Confidentiality** – This refers to the limiting of access to information and its restricted disclosure to authorised users (Privacy, 2006). The confidentiality service is also designed to provide some level of protection for the traffic that traverses the WLAN, as attackers may eavesdrop on this traffic in an attempt to compromise its confidentiality. The 802.11 standard provides optional security protocols called Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access-2 (WPA-2) as a means to thwart eavesdroppers. However, certain flaws, such as the deauthentication/disassociation attack, have not been addressed by these protocols (Gast, 2002). Section 2.4 provides a detailed discussion on the security flaws of the protocols.
- **Data delivery**– Networks will not be useful if they are not capable of getting data delivered to the intended recipient. Stations therefore utilise the MAC Service Data Unit (MSDU) delivery service as a reliable delivery mechanism of data to the intended recipient (Zhang et al., 2008).

### 2.3.2 Distribution System Services

The IEEE 802.11 standard defines five DS services – association, reassociation, disassociation, distribution and integration – that are necessary to allow mobile stations to roam freely within the ESS and that allow the IEEE.802.11 WLAN to connect to the wired LAN infrastructure outside the ESS. The services are discussed below.



- **Association** – This service is the same as authentication. A station is authenticated once it is associated, and it will not be associated unless it has been authenticated. The delivery of frames to the correct recipient in a wireless network is made possible because stations register or associate themselves with the APs. The DS then uses the registration information to determine where and how to deliver data to the mobile stations (Gast, 2005). In general, the DS uses the association service to provide a logical connection between a station and the AP.
- **Reassociation** – This service is similar to the association service, with the exception that it includes information about the AP in which a mobile station was previously associated. When a mobile station roams within an extended service area, it must evaluate its signal strength and perhaps switch from an AP in which it was associated to another. Reassociation takes place when the signal strength of a mobile station indicates that a different association would be beneficial. When the reassociation is complete, the DS updates its location records to reflect the reachability of the mobile station through a different AP (O’Hara and Petrick, 2005; Geier, 2001).
- **Disassociation** – This service is similar to that of deauthentication. It can either be invoked by the AP to inform mobile stations that they can no longer associate with it, or it can be invoked by the mobile stations to inform the AP that they no longer require the service of the WLAN. This may inter alia be due to the demand exceeding available resources in the AP, causing the AP to shut down (Perahia and Stacey, 2013).
- **Distribution** – This service is used in an infrastructure network. The AP uses the distribution service to determine how to deliver the frames it receives from mobile stations. When a mobile station sends a frame to the AP for delivery to another mobile station, the AP invokes the distribution service to determine if the frame should be delivered to a destination mobile station within the same BSS; to the DS for delivery to another mobile station associated with a different AP, or to a network destination outside the WLAN (O’Hara and Petrick, 2005).
- **Integration** – The integration service is provided by the DS. Its main function is to connect IEEE 802.11 WLAN with non-IEEE 802.11 networks. The integration service achieves this by translating IEEE 802.11 frames into frames that may traverse other networks and vice versa (i.e. translating frames from other networks to frames that can be delivered by the IEEE 802.11 WLAN) (Chen and Guizani, 2006).

Table 2.1 summarises the WLAN services that have been discussed above.

Table 2.1. Summary of WLAN services

Network Service	Station / Distribution Service	Description
<b>Authentication</b>	Station	Verifies mobile station identity prior to establishing association.
<b>Deauthentication</b>	Station	Terminates an authenticated mobile station's association with the network.
<b>Privacy</b>	Station	Protects traffic that traverses the WLAN against eavesdropping.
<b>Data delivery</b>	Station	Delivers data to the intended recipient.
<b>Association</b>	Distribution	Provides a logical connection between mobile station and AP.
<b>Reassociation</b>	Distribution	Allows mobile station to move from one BSS to another within an ESS.
<b>Disassociation</b>	Distribution	Terminates connection between a mobile station and an AP.
<b>Distribution</b>	Distribution	Invoked by the AP to determine how to deliver the frame it receives to the intended destination.

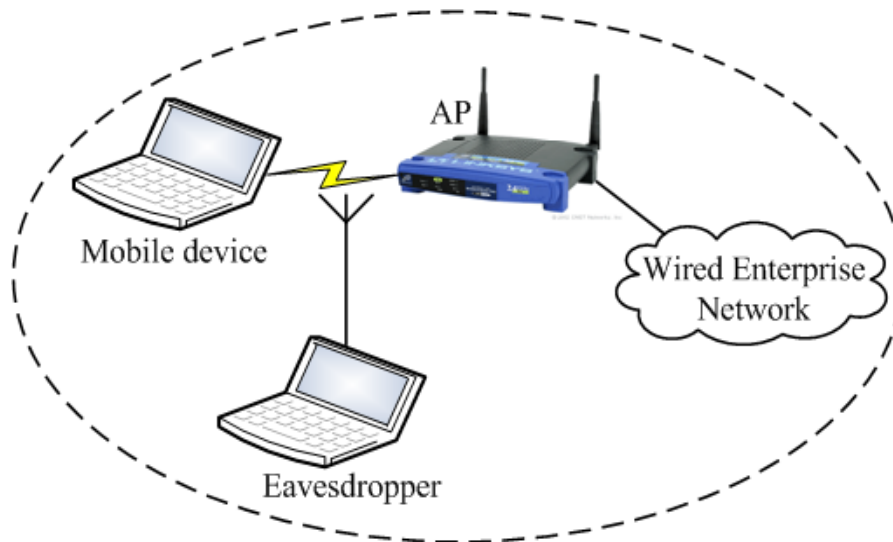
Following this discussion of the Wireless Local Area Network services, that is, the station and Distribution System (DS) services, the next section highlights some WLAN security attacks.

## 2.4 Attacks Against Wireless Local Area Networks

Unlike wired networks, wireless networks are difficult to protect because its transmission medium is the air. This renders wireless networks vulnerable to several types of attack, which can be classified into passive and active attacks.

### 2.4.1 Passive Attacks

In a passive attack, the eavesdropper monitors the traffic of a particular wireless session. This suggests that the attacker only listens to the transmitted traffic without altering or destroying it. In a wireless environment, anyone with a transceiver within the transmission range can listen to communication between a mobile device and its associated access point (AP) (Ilyas and Ahson, 2005). Figure 2.4 gives a graphical representation of a typical scenario where passive eavesdropping occurs between a mobile device and an AP. Passive attacks mostly include traffic analysis, monitoring of unencrypted traffic, the decryption of weakly encrypted traffic, and the capturing of authentication information such as passwords and other sensitive information that can be used in other types of attack or be sold in the black market at a premium (Computer networking notes, 2010).



**Figure 2.4.** Passive eavesdropping

It is difficult to detect a passive eavesdropping attack because the attacker does not delete or modify the traffic. Also, the attacker may use more powerful antennas to receive 802.11 transmissions even hundreds of feet away from the transmission range. The effects of passive eavesdropping may be mitigated by encrypting all the traffic that traverses the wireless network. However, depending on the encryption method used, this encryption can still be compromised. Strong encryption algorithms should therefore be used (Alkhawaja and Sheibani, 2011). A brief summary of these types of attacks is presented below.





### 2.4.1.1 War-driving

War driving typically involves detecting and collecting Wi-Fi signals by scanning them from nearby locations with a portable antenna (Tsui et al., 2010). This attack is typically carried out driving around, sometimes with a GPS that hackers use to plot out areas with vulnerabilities on a map. As mentioned, the attacker in a war-driving attack does not actively change anything on the scanned nearby network but merely listen to network traffic with an intention to identify vulnerabilities.

### 2.4.1.2 Eavesdropping

Eavesdropping is a process whereby an attacker intercepts, listen or sniff electronic communication between communicating parties (McGraw, 2005). The sniffed or recorded data packets can later be analysed or decrypted if encrypted in order to identify information such passwords, open ports, and other vulnerabilities on the network.

### 2.4.1.3 Evil Twin Attack

An evil twin attack is a rogue access point that masquerades as a legitimate Wi-Fi access point and entices end-users to connect to it. It is similar to website spoofing or a phishing scam. An adversary fools the wireless users into connecting to the tainted hotspot by posing as a legitimate provider. Once the end user connects to it, the rogue access point can eavesdrop on wireless communications of users' internet access (Song et al., 2010).

### 2.4.1.4 Shoulder-Surfing

Shoulder surfing is an act of observing displays and keystrokes over someone's shoulder (Bianchi et al., 2011). This form passive attack is seen as the most effective way of getting information from someone since its relatively easy to stand next to someone and watch them as they fill out a form, enter a PIN number at a bank machine, or credit card information as you enter it on a web based shopping cart, or enter a username and password to access emails.

## 2.4.2 Active Attacks

In contrast to a passive attack, an active attack not only monitors the traffic that traverses the wireless network, but it also alters or destroys data, or creates fraudulent packets to jam the



network. There are several types of active attack that can be launched against a WLAN, such as a Denial-of-Service (DoS) attack, a Man-in-the-Middle attack, session hijacking and attack against the Wired Equivalent Privacy (WEP). A brief summary of these attacks is presented below.

#### **2.4.2.1 MAC Address Spoofing**

Medium Access Control (MAC) address spoofing is a technique in which an attacker changes the factory-assigned MAC address of a network interface on a networked device. Typically, every single wireless interface has a global unique hardware address called MAC address which is used for identification. Though this address was initially meant not be changes, attackers has since find a way to spoof the address in order to perform nefarious actions on the network such as Denial of Service attacks (Chumchu et al., 2011).

#### **2.4.2.2 ARP Spoofing**

Address Resolution Protocol (APR) spoofing is a type of attack whereby an attacker sends a falsified ARP messages over a Wireless Local Area Network. The result of this is a link of the attacker's MAC address with the IP address of the legitimate computer on the network. The main idea behind this type of attack is to send bogus ARP communication to the Ethernet LANs which gives the attacker powers to modify the traffic or block it altogether (Technopedia, 2015).

#### **2.4.2.3 Denial-of-Service Attack**

Denial-of-Service (DoS) attacks are active attacks that are meant to cause disruption of network services such as bandwidth, disk space, memory, etc. The goal of DoS is to deny legitimate users access to these network or computing resources (Bicakci and Tavli, 2009).

#### **2.4.2.4 Man-in-the-Middle Attack**

A man-in-the-middle attack can be launched either for the purpose of eavesdropping on a wireless communication or to alter the content of the packets before they reach the intended recipient. This type of attack is very powerful because it enables the attacker not only to monitor the communication, but also to modify it (Ilyas and Ahson, 2005; Henk van Tilborg

and Jajodia, 2011).

#### **2.4.2.5 Session Hijacking**

In a session hijacking, the attacker gains unauthorised access to a session between legitimate users and intercepts the packets in between them. To launch this attack, the attacker must be able to masquerade as a legitimate user of the wireless network. In the end, the attacker is able to take over the whole communication session (Alkhawaja and Sheibani, 2011).

#### **2.4.2.6 Attack Against WEP**

This encryption mechanism has several security flaws, which undermines its encryption and authentication capabilities (Moen et al., 2004). The author acknowledged the fact that Wired Equivalent Privacy (WEP) is an old standard and can be easily cracked, however it is still a relevant standard since some novice users still use it, and even older equipment needs to use WEP since they won't run on newer standards. WPA has already demonstrated some vulnerability and can be cracked. WPA2 is the current standard and the best choice especially when used together with strong password and Advanced Encryption Standards (AES-128) encryption. Wi-Fi Protected Setup (WPS) has since been introduced to allow home users of WLAN to secure their networks.

### **2.5 Concluding Remarks**

This chapter provides the foundation for the entire dissertation by describing the Wireless Local Area Network, type of network on which the underlying environment of this research is based. This chapter discussed the basic elements that constitute the WLAN architecture, the WLAN services that look at how mobile stations get associated with the AP, and how traffic is transmitted from a source to a destination address.

The fact that a WLAN is an open environment suggests that it can be vulnerable to a number of security attacks that are referred to in this chapter. The field of digital forensics was developed to act on these security attacks, and to retrieve digital evidence from computers and networks. The next chapter provides the reader with an overview of digital forensics and, subsequently, digital forensic readiness.



## Chapter 3                    **Digital Forensics and Digital Forensic Readiness**

### **3.1 Introduction**

The main purpose of this chapter is to introduce the reader to the background concepts of digital forensics and digital forensic readiness. The current research aims to implement these concepts in the Wireless Local Area Network that has been discussed in the previous chapter.

The next section defines digital forensics in the way that the concept is used throughout this dissertation. Solving a digital forensic problem requires digital forensic experts to follow a certain digital forensic process. The chapter therefore presents various digital forensic process models in order to get some insight into the process model that is needed to solve the digital forensic readiness problem addressed in this dissertation. Once the reader has been introduced to the concept of digital forensics in general, the chapter continues by explaining to the reader the concept of digital forensic readiness, which plays a crucial role in solving the problem identified in this dissertation.

### **3.2 Defining Digital Forensics**

The literature presents a profuse number of digital forensic definitions. For example, the Digital Forensic Research Workshop (DFRW, 2001) defines digital forensics as “*the scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or gathering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations*”. Other scholars view digital forensics as:

- the process of analysing and evaluating digital data as evidence (Willassen and Mjølshnes, 2005);
- a scientific and technological process used to search and analyse digital objects in order to uncover digital evidence that can be entered into a court of law to answer questions about a digital criminal activity (Carrier, 2005);
- the preservation of digital evidence in a way that satisfies the criteria set by the jurisdiction (Leigland and Krings, 2004); and

- the use of scientific methods towards the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining the chain of custody (Kent et al., 2006)
- the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable (McKemmish, 1999).
- the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media (Noblett et al., 2000).

From the above definitions, the reader can note the following common factors:

- Digital forensics is a scientific field.
- It uses scientific methods or processes to conduct a digital crime investigation that yields digital evidence that can tie an adversary to an unethical activity.
- The resulting digital evidence should satisfy the jurisdiction.

Despite many attempts by various scholars to define digital forensics, it stands to reason that a digital forensic definition should include a reference to the digital forensic process. The researcher defines digital forensics as the scientific field that uses a standardised digital forensics process methodology to uncover digital evidence that satisfies the jurisdiction. This definition is adopted throughout this dissertation.

Having analysed the definitions of digital forensics by various scholars and proposed the working definition for this dissertation, the next section discusses the various digital forensic process models as they are found in the literature.

### 3.3 Digital Forensic Process Models

A digital forensic investigation should adhere to the prescriptions of a proper digital forensic process model for its evidence to be admissible in a court of law. However, to date, no single, standardised or consistent digital forensic investigation process model has been established. In this section, the author compares and contrasts various digital forensic investigation process models.

Numerous scholars have attempted to create rudimentary digital forensic process models. For example, Farmer and Venema describe some basic guidelines in their Computer Forensic Analysis Class hand-outs (Farmer and Venema, 1999). These guidelines include steps as

listed in Table 3.1 (a summary of the digital forensic models). Though it has to be admitted that these guidelines provide an appropriate foundation, the remaining portion of the note hand-outs focuses on specific UNIX forensic procedures. Farmer and Venema's definition of a digital forensic process for achieving the steps in Table 3.1 should have been abstracted to be applicable to computer systems in general; however, a lack of software tools did not allow them to explore non-UNIX systems. This prompted them to develop their own suite of tools known as the Coroner's Toolkit (Farmer and Venema, 2004), which assisted them to accomplish some of their defined digital forensic phases, especially phase number six (see Table 3.1). Without any doubt, this was a well-thought-out process model that provided a good foundation for a standardised digital forensic process model; however, it was platform-dependant and not an appropriate process model for digital forensics in general.

Another attempt to come up with a viable digital forensic process model was that of the first Digital Forensic Research Workshop (DFRW). The DFRW is one of the significant participants that took the initiative to develop a consistent and standardised digital forensic process model (DFRW, 2001). Their digital forensic process model includes the steps as listed in Table 3.1. The greatest challenge in respect of this process model is that analytical procedures and protocols are not standardised, nor do practitioners and researchers use standard terminology (Reith et al., 2002).

The US Department of Justice (DOJ) also attempted to propose a digital forensic process model, the steps of which are listed in Table 3.1. The significant difficulty with this process model is that the US DOJ does not make a distinction between digital forensics applied to computers or to other electronic devices. Instead, they attempt to build a generalised digital forensic process model that will be applicable to most electronic devices (US DOJ, 2001).

Mandia and colleagues also tried to define a viable digital forensic process model as listed in Table 3.1 (Mandia et al., 2003). They refer to their process model as an incident response methodology. The key problem with this methodology is that it focuses only on computer crime and does not address the digital forensic process in terms of other digital devices such as personal digital assistants (PDAs), smart appliances and other future electronic devices.

The researchers at the United State Air Force Institute of Technology (Reith et al., 2002) proposed an abstract digital forensic process model with traits that are common from previously published process models. This process model comprises the phases as listed in Table 3.1. The most salient aspect of this process model is its broad view, which enables it to

cover a range of incidents. However, this process model developed by Reith and colleagues and that of the US DOJ use examination and analysis to identify and collect digital evidence. The names of these phases may sometimes be confusing because their meanings are so slightly different. It is common to have two digital forensic investigators referring to the same task when they say they are “analysing a system” or “examining a system”. According to the American Heritage Dictionary of the English Language, the definition of examine is “to study or analyse” and the definition of analyse is “to examine methodically by separating into parts and studying their interrelations” (American Heritage Dictionary, 2001). Despite the fact that we acknowledge the differences between the two phases as described in this abstract digital forensic process model, their similarity may still lead to confusion.

James and Nordby (2005) proposed specific physical crime scene investigation procedures with phases as listed in Table 3.1. Their model highlights the importance of evidence that can be gathered at a physical crime scene. The model shows through its documentation phase that the physical crime scene should be properly documented and digital forensic investigators should then use their expertise to find useful pieces of evidence at the crime scene. Though this is a good starting point for a viable digital forensic process model, it is not only physical objects that can be found at the physical crime scene.

The National Institute of Standard and Technology proposed (Kent et al., 2006) proposed a digital forensic proposed model with four phases, that is, collection, examination, analysis, and reporting as listed in Table 3.1. Without any doubt, this is the most basic and simple digital forensic process model to follow and it is well described in the NIST standard. However, it possesses the same drawbacks as that of the process model developed by Reith and colleagues and that of the US DOJ which uses examination and analysis to identify and collect digital evidence. As mentioned earlier, the names of these phases may sometimes be confusing because their meanings are so slightly different. It is common to have two digital forensic investigators referring to the same task when they say they are “analysing a system” or “examining a system”.

The ISO/IEC 27043 proposes a harmonised digital forensic process model as listed in Table 3.1. The standard includes readiness, initialisation, acquisitive and investigative. This standard is an umbrella standard that describes the width of the overall process to be followed when conducting digital forensic investigation. The standard is deemed to pave the way for other international standards that will cover the depth of each sub-process within the overall



process. Without any doubt this is a good standard that like the one's presented above, the main challenge is that it is not encompassing, it does not cover all cases of digital forensic investigations from a general hard drive acquisition to a more advanced network intrusion forensic investigation.

Despite the fact that several digital forensic process models exist (as indicated above), consensus has not yet been reached about a single, standardised digital forensic process model that can be adopted internationally.

It should be noted that this section does not intend to come up with new digital forensic process models, but rather aims to identify, compare and contrast various process models as they are found in the literature. Hence, having identified, compared and contrasted various digital forensic process models as found in the literature, the next section defines what digital forensic readiness entails.

**Table 3.1.** Summary of digital forensic process models

<b>Digital Forensic Process Models</b>							
<b>DFRW</b>	<b>US DOJ</b>	<b>Mandia et al.</b>	<b>Reith et al.</b>	<b>Farmer and Venema</b>	<b>James and Nordby</b>	<b>Kent et al.</b>	<b>ISO/IEC 27043</b>
1. Identification	1. Collection	1. Pre-incident preparation	1. Identification	1. Secure and isolate crime scene	1. Securing the crime scene	1. Collection	1. Readiness
1. Preservation	2. Examination	2. Detection of incident	2. Preparation	2. Record crime scene	2. Crime scene survey	2. Examination	2. Initialisation
2. Collection	3. Analysis	3. Initial response	3. Approach strategy	3. Photograph crime scene	3. Crime scene documentat ion	3. Analysis	3. Acquisitive
3. Examination	4. Reporting	4. Formulation of response strategy	4. Preservation	4. Sketch crime scene	4. Crime scene searches	4. Examination	4. Investigative
5. Analysis		5. Investigation of the incident (data collection and analysis)	5. Collection	5. Maintain excellent notes	5. Crime scene reconstructi on		
6. Presentation		6. Reporting	6. Examination	6. Conduct systematic search for evidence	6. Securing the crime scene		
7. Decision		7. Resolution, recovery and implementat ion of security measures	7. Analysis	7. Collect and package physical evidence	7. Crime scene survey		
			8. Presentation	8. Maintain chain of custody			
			9. Return Evidence	9. Obtain standard/ reference samples			
			10. Identification	10. Submit evidence to library			
				11. Maintain safety at crime scene			



### 3.4 Defining Digital Forensic Readiness

Digital forensic readiness is defined as the process of maximising the ability of an organisation to collect credible digital evidence, while minimising the cost of conducting the entire digital forensic investigation (Tan, 2001). Mohay (2007) defines digital forensic readiness as the extent to which computer systems or computer networks record activities and data in a manner such that the records are sufficient for subsequent digital forensic purposes, and such that the records are acceptable in terms of their perceived authenticity as evidence in subsequent digital forensic investigations, while Moutaropoulos et al., 2012 perceive digital forensic readiness as the pre-incident plan for organisation's ability to maximise digital evidence usage and anticipate litigation.

From the definition of digital forensic readiness, one can note that collecting data or monitoring any network events in advance may accelerate the digital forensic investigation process while minimising its cost. However, to date, there has been little discussion of how to embed digital forensic readiness in networked systems, especially in WLANs, aside from recommending the use of specific tools to conduct a digital forensic investigation.

From the definition above, it is also evident that there are two main objectives of digital forensic readiness, namely to

- maximise the usefulness of incident evidence data, and
- reduce the cost of digital forensic investigation during an incident response.

These objectives are explored in more detail below.

#### 3.4.1 Usefulness of Incident Evidence Data

The data from an intrusion potentially has multiple uses. It can be used as leverage in an internal incident or as digital evidence in a court of law. It can be used to formulate plans during an incident response or to look for additional vulnerabilities or compromise (Tan, 2001). Digital evidence acquisition and preservation remain the most crucial phases in a digital forensic investigation process since these procedures can be performed simply, rapidly and effectively, while reducing the time and cost needed to conduct a digital forensic investigation.

However, the complexity of the environment requires that the acquisition and preservation of digital evidence be defined in detail ahead of time. This is due to the fact that any failure to preserve the digital data on the victim or attacking systems in a timely manner may cause the usefulness of the collected digital data to decrease. As such, some of the data may be residing in the victim's machine, which might be difficult to get hold of – especially in a wireless network environment. Tan (2001) suggests that, when designing a network, the importance of multi-tiered logging should not be overlooked. This is because the data on the attacking and compromised system is subject to modification by the intruder, especially if the said intrusion was successful. Multi-tiered logging not only provides various preservation sources of digital data, but also guarantees the usefulness of the collected digital data as potential digital evidence.

### 3.4.2 The Cost of Digital Forensics During an Incident Response

The corporate world is slowly but increasingly gaining an awareness of the importance and implications of computer-based or network-based digital evidence, but many of these organisations still believe that the challenges surrounding the collection of corporate digital evidence are unique to them. The effort to perform a digital forensic analysis should decrease, while at the same time the level of integrity of the digital evidence being collected should be maintained (Seifert et al., 2008).

The decrease in effort referred to here involves the time and cost required for an incident response during a digital forensic investigation. For example, if an organisation is digital forensically prepared, then there will be no huge difference between the amount of time spent by the intruder to launch an attack on the network and the amount of time required to respond to the incident. In general, the reduction in time to respond to an incident in a digital forensic investigation will definitely reduce the cost of the entire digital forensic process.

Dave Dittrich, head of the HoneyNet project (Tan, 2001; HoneyNet, 2011) discusses an incident that took an intruder a period of two hours to launch an attack, but it took the cyber forensic experts a period of 40 billable hours to respond to that incident. The reason why it took so long to respond to this incident is that the company to be investigated was not digital forensically prepared for any incident. We therefore argue that every business organisation has to be digital forensically ready, so that it will be able to collect any digital data in advance of a crime and use the collected data for subsequent digital forensic purposes.

### 3.5 Achieving Digital Forensic Readiness

The state of being prepared to deal effectively with events that may require digital forensic investigation is an issue that is growing in importance (Quinn, 2005). Digital evidence can easily be overwritten and lost, thus jeopardising the entire digital forensic investigation process. Digital data that is held on magnetic or other transient media only requires expert knowledge and special procedures to be preserved in a digital forensically sound manner. Achieving digital forensic readiness means that anyone who is expected to handle an organisation's digital data must be experienced and qualified (Rowlingson, 2004).

One inexpensive way in which an organisation can achieve digital forensic readiness is to have information security policies and procedures in place. An information technology organisation may have the best antivirus and firewall protection mechanisms available; however, unless the organisation has planned for digital forensic readiness, it could well find itself threatened if digital forensic evidence fails the admissibility test in the face of the judiciary. Another way to achieve digital forensic readiness is for an organisation to ensure data integrity and authentication; the methods used to collect the digital data must be able to prove that the collection of the digital evidence compromised neither the digital data nor the system used to collect the data (Mocas, 2004).

In light of all this, an organisation needs to be prepared to collect digital data that may be used in an event that requires digital forensic investigation (Ahmad, 2002). It is a commonly known fact that a digital forensically prepared organisation can protect itself against liabilities such as invasion of privacy and unfair dismissal claims when it has to deal with internal matters relating to policy violation (Casey, 2004). Rowlingson (2004) suggests a ten-step process for achieving digital forensic readiness within an organisation of any size:

1. Define the business scenarios that require digital evidence.
2. Identify available source and different types of potential evidence.
3. Determine the evidence collection requirements.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirements.
5. Establish a policy for secure storage and handling of potential digital evidence.
6. Ensure monitoring is targeted to detect and deter major incident.

7. Specify circumstances when a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of digital evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate the action in response to the incident (Rowlison, 2004).

### 3.6 Concluding Remarks

This chapter reviewed the attempts made by various scholars to define the concept of digital forensics. Based on these reviews, the researcher proposed a working definition of digital forensics in a way that is referred to throughout this dissertation. This chapter also pointed out that it would be appropriate for the digital forensics definition to incorporate a single and standardised digital forensic process model. However, to date, no such single and standardised digital forensic process model has been agreed upon.

Several scholars have attempted to come up with a digital forensic process model. These attempts were presented in this chapter. In addition, the chapter defined the concept of digital forensic readiness as a means to improve the efficiency of the entire digital forensic investigation process.

Extracting digital evidence residing in computers and networks, especially WLANs, remains a daunting task. However, various scholars and the industry have since developed a number of digital forensic tools to ease this process. The next chapter introduces the reader to ways in which digital evidence can be extracted and analysed in a WLAN environment through the use of specific digital forensic tools.



## Chapter 4      **Wireless LAN Digital Forensics**

### **4.1 Introduction**

The release of the IEEE 802.11 standard and its supported wireless devices has boosted the prospect of Wireless Local Area Networks (WLAN) as a universally accepted wireless networking technology (Cusack and Laurenson, 2011). Such universal acceptance is due to the inherent nature of the network, which provides flexibility, mobility and high speed internet access to its associated wireless clients. Such widespread usage nonetheless comes at a price, since the more popular the technology, the greater the chances for its potential misuse (Turnbull and Slay, 2008).

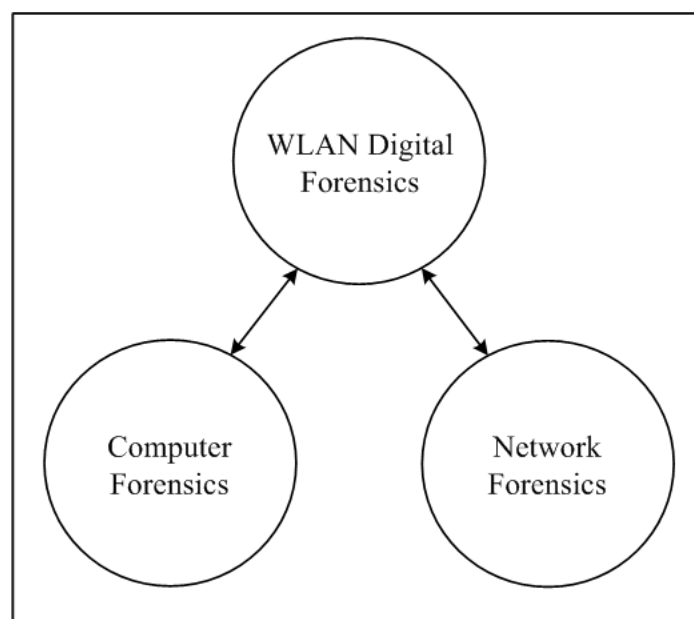
The security of WLANs has been subjected to extensive scrutiny by the industry and academia in order to minimise the potential misuse of the network. A common theme that was identified is that the WLAN is inherently insecure compared to its wired counterpart (Arbaugh, 2003). This stems from the peculiarities of a WLAN, an open environment where anyone with a capable device can receive the radio waves transmitted through the air.

Despite the continuing efforts made by the industry and academia about WLAN security mechanisms – in particular, their flaws and social impact – there has been very little focus on how to extract and analyse WLAN traffic without compromising its integrity, a discipline known as *wireless digital forensics* (Siles, 2010). It is for this very reason that the current research studies digital forensics within the WLAN computing environment.

This chapter now continues with a brief overview of WLAN digital forensics in general, after which the focus is shifted to exploring various tools for extracting the ever-increasing amount of evidential data that passes through the WLAN. The tools are scrutinised to observe if they possess any digital forensic capabilities. It should be noted that the extracted evidential data can be analysed at a later stage to draw conclusions about a case, should a need exist. The technical challenges associated with WLAN digital forensics are also studied, after which the chapter is concluded.

## 4.2 Defining WLAN Digital Forensics

The field of WLAN digital forensics, one of the digital forensic fields, is in the limelight as a new and emerging academic area of interest. Wireless LAN digital forensics shares some specific characteristics with both computer and network forensics (Yim et al., 2008). A graphic representation of this relation is given in Figure 4.1. Traditional computer forensics generally involves data acquisition from a storage medium such as a hard drive; while network forensics encompasses the capture, recording, and analysis of network traffic for subsequent digital forensics purposes (Cho et al., 2006).



**Figure 4.1.** Relation of WLAN digital forensics

WLAN digital forensics involves the application of methodologies and tools required to intercept and analyse wireless network traffic for presentation as digital evidence in a court of law (Siles, 2010). The methodologies referred to here are the digital forensic process models discussed in Chapter 3 (Section 3.3); while the tools referred to here are packet sniffers, which are discussed in Section 4.3.

## 4.3 WLAN Traffic Monitoring Tools

The most critical and necessary step towards a WLAN digital forensic investigation is the interception of wireless network traffic. However, this can be a daunting task since some packets that traverse the WLAN are encrypted; also, it is difficult to collect and synchronise a



large volume of data from multiple packet sniffers (Yeo et al., 2004). Though encrypted packets will not prevent a packet sniffer from sniffing the traffic, chances are it will not be able to decipher the encrypted traffic, resulting in a bunch of sniffed packets.

A packet sniffer is a software tool used to capture and analyse traffic that traverses across the network layer of the Transmission Control Protocol/ Internet Protocol (TCP/IP) (Ansari et al., 2002). It is complementary to wiretapping in telephone networks. Packet sniffers can be used legitimately by system and network administrators to monitor and troubleshoot a network, for example, finding out why computer A cannot communicate with computer B (Qadeer et al., 2010). On the other hand, other users can use packet sniffers for nefarious reasons, for example, sniffing out passwords and other sensitive information across the network for personal gain (Meehan et al., 2001; Northcutt, 2000).

### 4.3.1 Types of Packet Sniffers

There are different types of packet sniffers; however, the most widely used ones are Wireshark, tcpdump and Kismet.

#### 4.3.1.1 Wireshark

Wireshark is open-source cross-platform software that passively captures 802.11 packets transmitted through the Wireless Local Area Network (WLAN) (Seagren and Noonan, 2007; Wang et al., 2010). One could think of Wireshark as a measuring device used to examine what is going on inside a network cable, just like a voltmeter is used by electricians to examine what is going on inside an electric cable (Mohammad and Mohsen, 2009). WireShark was formerly known as Ethereal. It has a rich set of features that include but are not limited to the following:

- Support live traffic capture and offline analysis.
- Conduct deep inspection of hundreds of protocols.
- Reconstruct captured raw packets into a more meaningful format.
- Browse captured network traffic via a Graphical User Interface (GUI), or via a TShark utility.
- Search for packets on many criteria.
- Support VOIP analysis.
- Support multiple capture file format such as tcpdump, Pcap NG, and iplog.



- Support decompression of traffic.
- Support packet decryption mechanism for IPsec, WEP, WPA/WPA-2, SSL/TLS, and many other protocols.
- Support colouring rules for quick and intuitive analysis of the captured packets.
- Can export output to XML, PostScript, CSV, or plain text.

The main purpose of Wireshark is to troubleshoot network problems, examine security problems on the network and debug protocol implementation (Orebaugh et al., 2006). It is also sometimes used by students to learn network protocol internals (Wang et al., 2010). Though Wireshark is not designed for digital forensic purposes, it provides a key feature for the capturing and passive analysis of wireless network traffic, which can supply digital evidence – hence making it a suitable tool for WLAN digital forensics. Most of the other features, if not all, are a support of this key function.

#### 4.3.1.2 Tcpcap

Tcpcap, like Wireshark, is open-source cross-platform software that intercepts and displays packets that traverse the wireless network. Unlike Wireshark that uses a GUI to display the raw captured packets, tcpcap uses a command-line interface with the libcap library to capture packets. In some Unix-like operating systems, a user must login as a root user to use tcpcap, because the packet-capturing mechanisms on those systems require elevated privileges (Fuentes and Kar, 2005).

The fact that tcpcap can capture and display the raw packets makes it suitable for digital forensics investigation purposes. Despite this, neither tcpcap nor Wireshark acts as an Intrusion Detection System (IDS) (Mohammad and Mohsen, 2009). This suggests that neither of the two will generate an alert or warning message when something wrong happens on the network. However, when something wrong does happen, these tools might help the investigator to figure out what that was (Fuentes and Kar, 2005).

#### 4.3.1.3 Kismet

Kismet is also open-source cross-platform software that captures wireless network traffic (McClure et al., 2003). Unlike Wireshark and tcpcap, Kismet works passively. This suggests that, without sending any loggable packets on the network, Kismet is able to detect the presence of both a wireless access point and its associated clients. It also has IDS





capabilities and is able to detect other packet sniffers in a network and other wireless network attacks. Kismet has the capability to detect default or non-configured networks, probe requests, and even determine the level of encryption used by a closest wireless AP. It collects and permanently stores payload information, and uses the data payload as a means to collect and interpret information about a network (Turnbull and Slay, 2007).

Though Kismet was not initially designed for digital forensic purposes, its capability to passively capture wireless traffic and detect any closest existing wireless AP (as well as its associated devices) qualifies this tool to be used for wireless digital forensics. The fact is that intruders often use rogue wireless APs to lure wireless clients to associate with it, which amounts to unethical conduct. Kismet can be employed to detect such misconduct and the resulting evidence can be used in a digital forensic investigation.

Having explored the packet sniffers and their capabilities within a digital forensic context, Section 4.3.2 will explain the digital forensics challenges that are envisaged when using these tools.

#### **4.3.2 DF Challenges Associated with Packet Sniffers**

There are several challenges associated with packet sniffers, some of which are discussed below:

1. Law enforcement – In many jurisdictions, there are ramifications with regard to law enforcement when network traffic headers as opposed to headers and payload are captured; the first may be legally acceptable whereas the second may not. Applications that collect header information need to prove beyond any reasonable doubt and provide evidence that payload data is never stored permanently or used in the analysis. Unfortunately, Kismet is currently designed to capture and permanently store payload information, something that may have legal implications.
2. Limited capability of each sniffer – The sniffers discussed above have known limitations such as signal receiving range, limited disk space due to the large amount of traffic that passes through the network and limited amount of processing power (Yeo et al., 2004).
3. Not initially designed for digital forensics – Whilst all the packet sniffers discussed above (and others similar to them) possess some functionality that can be used for digital forensic purposes, some alterations and testing to these tools may need to be

performed to ascertain their wireless digital forensic suitability (Turnbull and Slay, 2007).

4. Cannot detect all the wireless attacks presented in Chapter 2 – Packet sniffers cannot detect all the wireless security attacks discussed in this dissertation. This is especially true for most of the passive attacks since they don't leave any digital footprint on the network; rather they sniff the network traffic looking for vulnerabilities which can be exploited.

#### **4.4 Concluding Remarks**

This chapter clearly defined what WLAN digital forensics entails. The definition pointed out that the tools (i.e. packet sniffers) and methodologies (i.e. digital forensic process models) remain the most important aspect of WLAN digital forensics. Various packet sniffers were identified and scrutinised to check if they possess any digital forensic capabilities. In addition, the chapter also presented several digital forensic challenges associated with packet sniffers.

Chapters 2, 3 and 4 introduced the reader to the necessary background concepts that will be dealt with in this dissertation. Chapter 3 pointed out that conducting a digital forensic investigation from beginning to end is a costly process. Digital forensic readiness was therefore introduced as a mechanism that can be used to reduce the cost and time involved in a possible digital forensic investigation, and that does not compromise the integrity of the digital information being examined.

Having introduced the reader to the background concepts required for this dissertation, the next chapter proposes a digital forensic readiness model that can be implemented in WLAN environments to address the problem as stated in the introduction.

## **PART III: Modelling**



## Chapter 5            **The Wireless Digital Forensic Readiness Model**

### **5.1 Introduction**

Part II of this dissertation provided the background knowledge necessary to proceed with the research on an appropriate model for digital forensic readiness. This background knowledge brings to the fore the problem that constitutes the focus of this research: the key issue in WLAN digital forensics is that it is an enormous challenge to intercept and preserve all the communications generated by communicating mobile devices and conduct a proper digital forensic investigation. WLANs as such are not digital forensically ready. In other words, without the model as proposed in this dissertation, it would currently be very difficult to gather enough digital evidence for a successful digital forensic investigation.

This problem is exacerbated by the fact that the devices participating in a WLAN environment are mobile, which means they can join and leave the network at any time. This makes it difficult to attribute a criminal activity on the network to a certain suspected mobile device because by the time the digital forensic investigation is warranted, the mobile device may have left the network a long time ago.

Prior work has been done on wireless forensics, especially on the mechanism and system design level (Ning et al., 2012; Cusack and Laurensen, 2011; Achi et al., 2009; Yim et al., 2008; Velasco et al., 2008; Turnbull and Slay, 2008; Endicott-Popovsky et al., 2007; Broadway et al., 2008, McGrath and Nelson, 2006). McGrath and Nelson (2006) designed and implemented a FLUX system that automates the collection of forensic data and identifies abnormal traffic and network weaknesses. Ning et al (2012) built an analytical framework that computes the likelihood of digital evidence existing with respect to transmissions, given a set of network parameters. Achi et al (2009) propose and implement techniques that can be used for wireless digital forensics. Turnbull and Slay (2008) studied the IEEE 802.11-based wireless networking environment from a forensic computing perspective to understand the current state of wireless misuses, and the current tools and techniques used in wireless digital forensics.

In summary, almost all of the above approaches study and propose techniques for solving specific network problems that require wireless digital forensics. However, none of the

studies or implements digital forensic readiness in a WLAN environment like we do in this dissertation.

In an attempt to address the above problem, this research proposes a Wireless Digital Forensic Readiness Model (WDFRM) with the capability of monitoring, logging and preserving wireless network traffic for subsequent digital forensic investigations. The proposed model builds on the work of Rowlingson (2004) with regard to traditional digital forensic investigations.

This chapter constitutes the contribution part of this dissertation. It starts off by presenting an overview of the proposed model in the form of a block diagram. The block diagram aims at providing the reader with a holistic view of the entire model before delving into details about the functions of each component. The components of the proposed model are then explained. These components are discussed in detail to show how they interact with one another. The focus then shifts to a discussion of the model as an integrated whole. Lastly, the chapter is concluded with a brief summary.

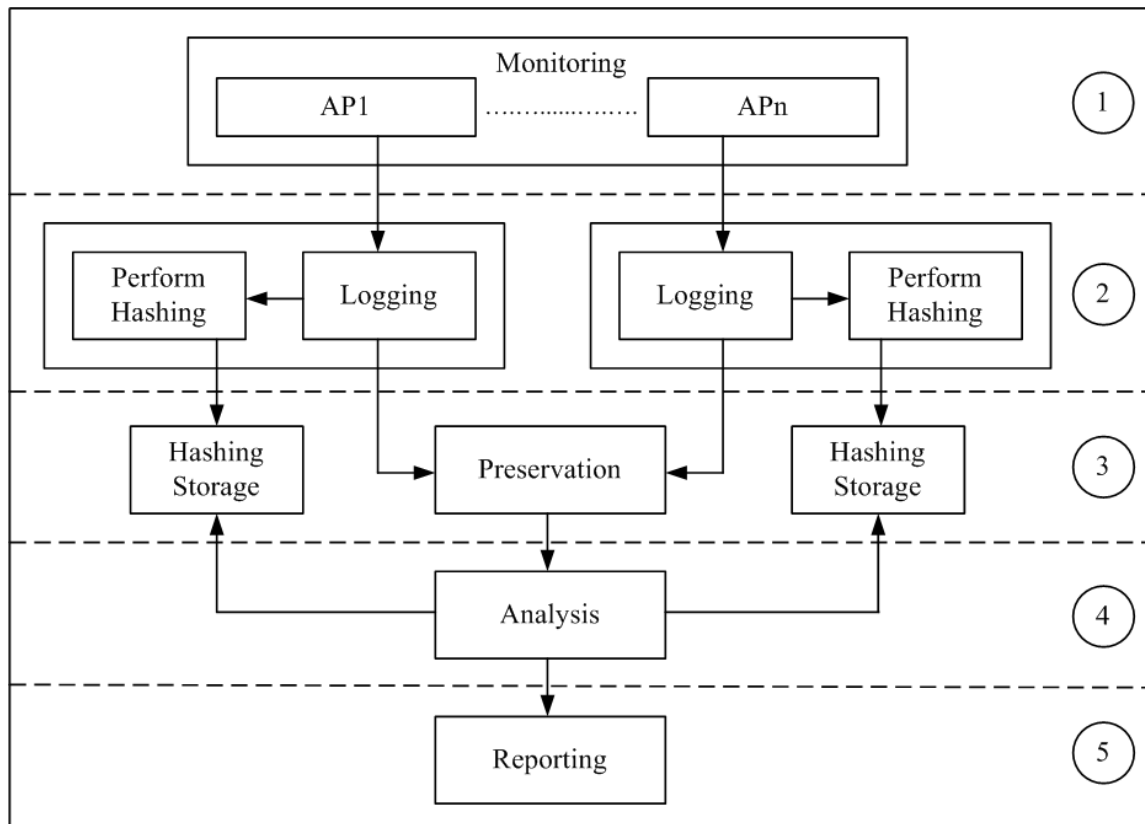
## 5.2 Block Diagram of the Wireless Digital Forensic Readiness Model

The principal concept addressed by the Wireless Digital Forensic Readiness (WDFRM) is that it monitors wireless network traffic from various access points (APs). The monitored traffic is logged in a log file and then preserved to maintain its integrity. The information needed by digital forensic experts is therefore rendered readily available, should it become necessary to conduct a digital forensic investigation.

The mere fact that this digital information is now available maximises the chances of it being used as evidence and reduces the cost of conducting an entire digital forensic investigation. This is simply because a large part of the digital forensic process (i.e. the monitoring, logging and preservation) would already have been conducted. Figure 5.1 indicates in a block diagram of how the components of the WDFRM interact with one another.

The encircled numbers 1 to 5 on the right-hand side of the block diagram in Figure 5.1 represent the phases or components of the digital forensic process of the WDFRM as indicated in Chapter 3, Table 3.1. Thus, 1 represents the monitoring phase, 2 represents the logging phase, 3 represents the preservation phase, 4 represents the analysis phase and 5

represents the reporting phase. These phases are described in detail from Section 5.2.1 to Section 5.2.5.



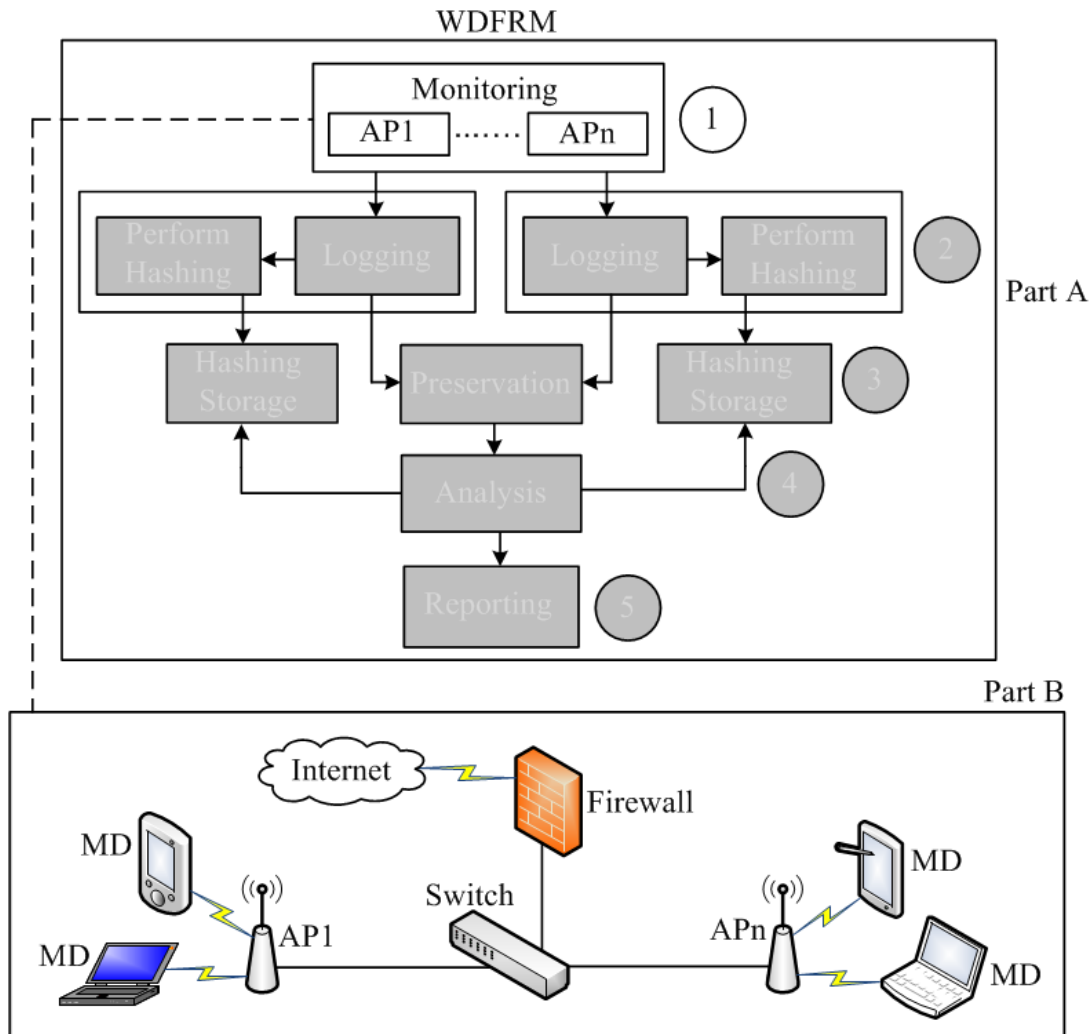
**Figure 5.1.** Block diagram of the WDFRM

### 5.2.1 Traffic Monitoring

This section presents the traffic monitoring component that is indicated in Figure 5.2. The reader should note that Figure 5.2 is similar to Figure 5.1. The main difference is that the unshaded area in Part A is expanded in Part B, with the latter being the key focus of this section. The reader should also note that Figure 5.3 – Figure 5.5 every time contain an expanded section.

In Part B of Figure 5.2, the monitoring component shows several Mobile Devices (MDs) that are connected to a WLAN through various Access Points (APs). This can be represented by  $AP_i = \{AP_1, AP_2, AP_3, \dots, AP_n\}$ ; where  $AP_i$  denotes a set of APs from  $AP_1$  to  $AP_n$ . In general, there can be many APs in a single WLAN environment. Each AP monitors all the traffic generated by the MDs that connect to it. For security purposes, the monitoring component uses a firewall to filter both inbound and outbound wireless traffic. Filtering is defined as the process of controlling access to the WLAN by examining all the packets based

on the content of their headers (Wiley, 2013). However, a firewall cannot detect all the misconduct of the WLAN since some MDs may obscure their identity and will appear to be legitimate users of the wireless network – therefore the proposed model employs another component called the Capture Unit (CU) that logs all the monitored traffic. The CU is discussed in detailed in the next section.



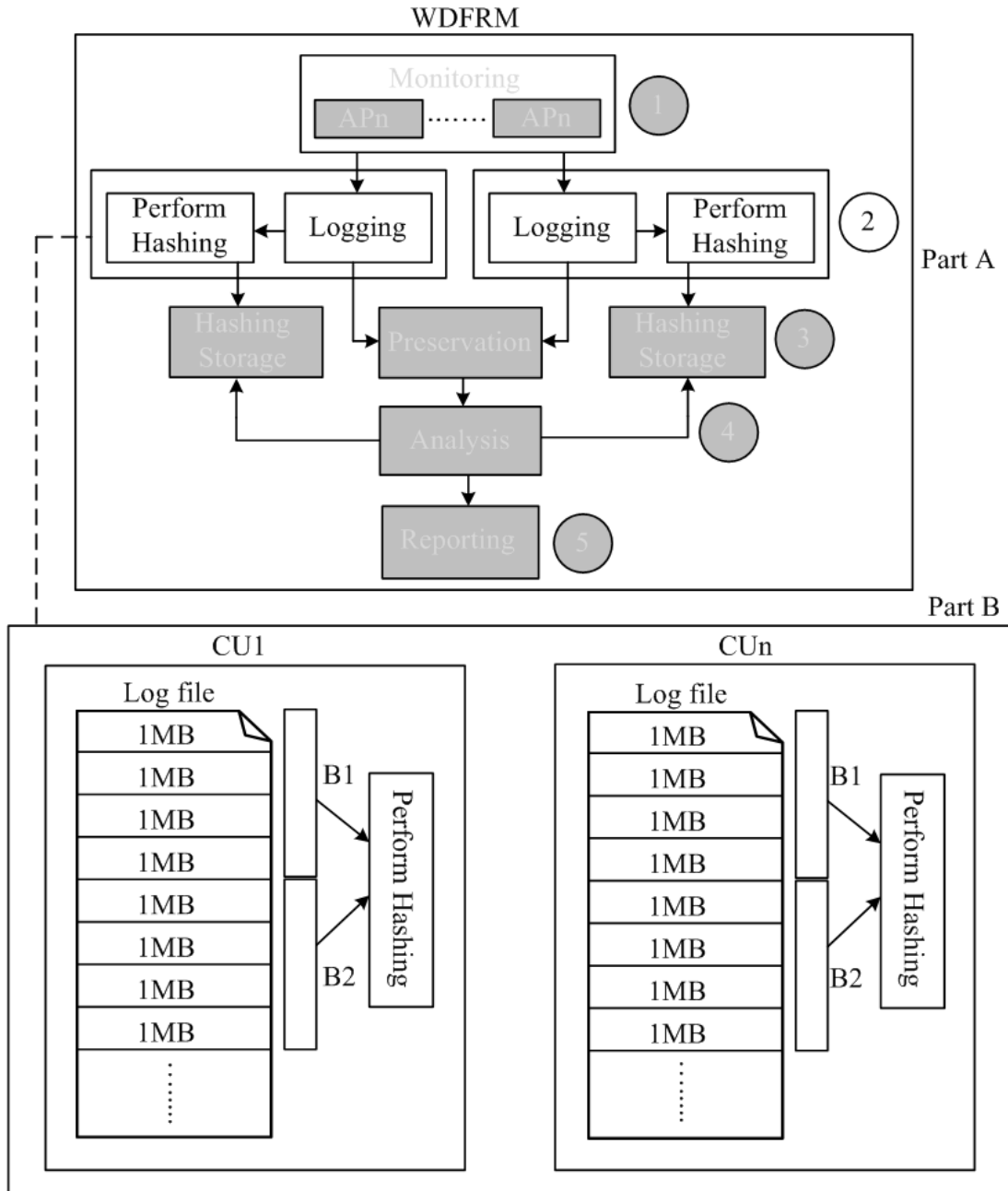
**Figure 5.2.** Traffic monitoring component

### 5.2.2 Logging

This section discusses the logging component in detail. In Part B, the CU component logs all the traffic monitored by the APs. Each AP has its own associated CU that logs the traffic passing through the AP. The CU logs the traffic in a log file as represented in Figure 5.3. The log file is divided into separate storage areas with each storage area consisting of, for example, 1 Megabyte (1MB) of data. As traffic is monitored from the AP and stored in a log



file, the storage area of the log file becomes limited. Therefore, this component creates a block of data per several MBs, i.e. B1 in Figure 5.3 represents a block of data consisting of 4MBs, for example.



**Figure 5.3.** Traffic logging component

A block is a fixed-size unit of data that is transferred together to a permanent storage space as described in the next section. For the purpose of this model and this study, the logged network traffic is the data packets. Therefore, whenever this study refers to ‘traffic’, it means all the data packets passing through the APs. Finally, the CU then sends the accumulated





blocks of data to the Evidence Storage (ES) for analysis purposes and creates a hash for each block of data that is sent to the hashing storage for preservation purposes, as will be explained in the next subsection. The reader should note that the CU is assumed to have enough processing power; otherwise it would struggle to capture and store all the data packets that flow through the network.

### 5.2.3 Preservation of Logs

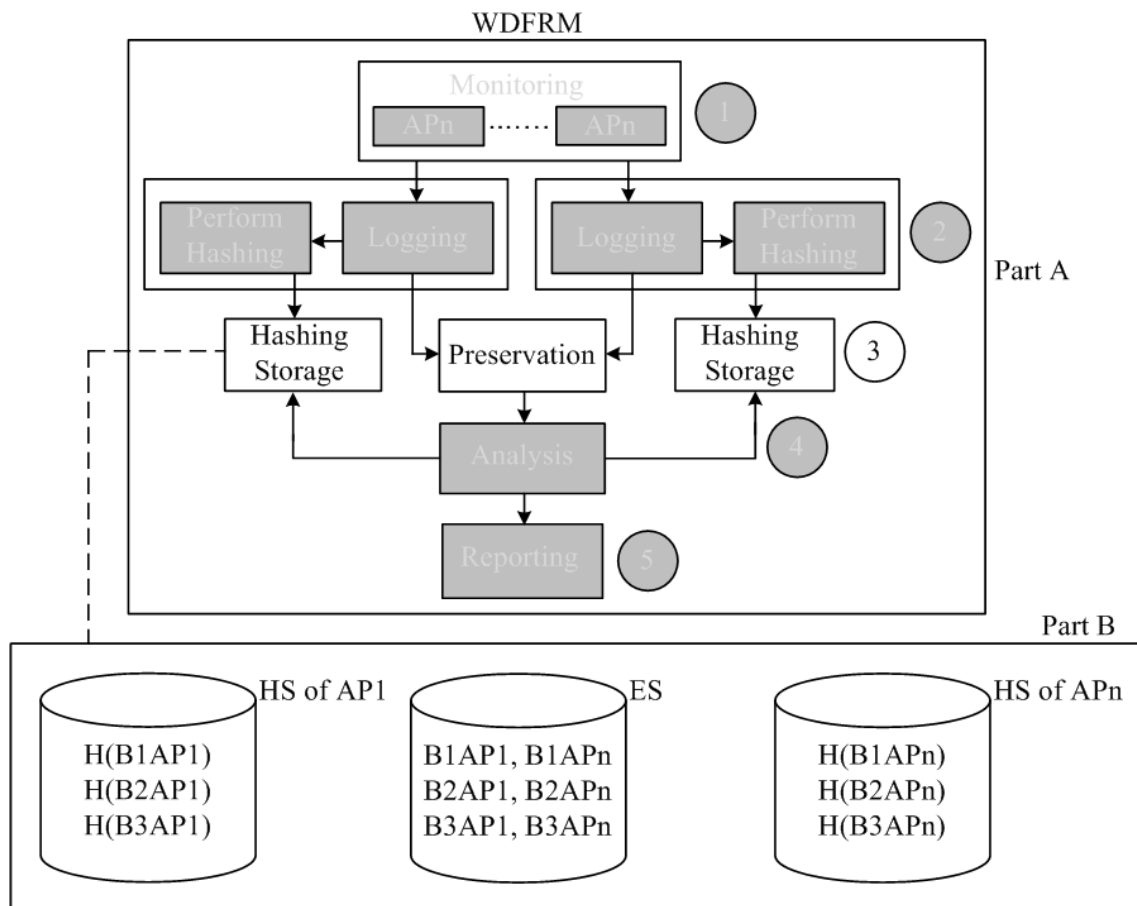
This section discusses the preservation component in detail. The primary goal of evidence preservation in WLANs is to ensure that absolutely no changes have been made to the logged data since it was collected (Solomon et al., 2005). Figure 5.4 demonstrates how the logs are being preserved in the proposed model. In Part B the Evidence Server (ES) stores all the blocks of data received from various CUs. In general, the ES acts as a central storage of all the data monitored from the APs. The ES logs the blocks of data in chronological order and store them according to the AP from which the traffic was monitored. For example, in the ES, B1AP1 represents the first block of traffic monitored from the first AP, whereas B1APn represents the first block of traffic monitored from the n<sup>th</sup> AP.

The reader should note that the data stored in the ES is needed only for analysis purposes. This data will only be analysed when a particular incident has been reported on the WLAN, which then needs to be investigated. The hash values of the blocks of data created in the “Perform Hashing” subcomponent within the CU are then transferred to the hashing storages represented as “HS of AP1” (Hashing Storage of AP1) and “HS of APn” (Hashing Storage of APn) as is represented in Part B of Figure 5.4.

The WDFRM implements a hashing storage for each AP. The H(B1AP1) in HS of AP1 represents the hash value of the first block from the first AP, and H(B1APn) in HS of APn represents the hash value of the first block from the nth AP (and so on). The WDFRM adopts both the MD5 and SHA-1 hashing techniques. Neither of these hashing techniques are addressed in detail in this dissertation since the focus is on implementing a digital forensic readiness in a WLAN. A detailed discussion of the MD5 and SHA-1 hashing techniques can nevertheless be found in Solomon et al (2005), who define hashing as a mathematical function that creates a unique fixed-length string from a message of any length. The result of a hash function is a hash value, sometimes called a message digest. The reader should note that the hashed blocks of data will only be used during a digital forensic investigation to

check whether the logged data on the ES was altered or not. This is a requirement of the digital forensic process (Casey, 2007).

Since the traffic has been captured on the network using a CU and preserved through the ES to maintain its integrity, the next section now proceeds to discuss the analysis and reporting components of the WDFRM.

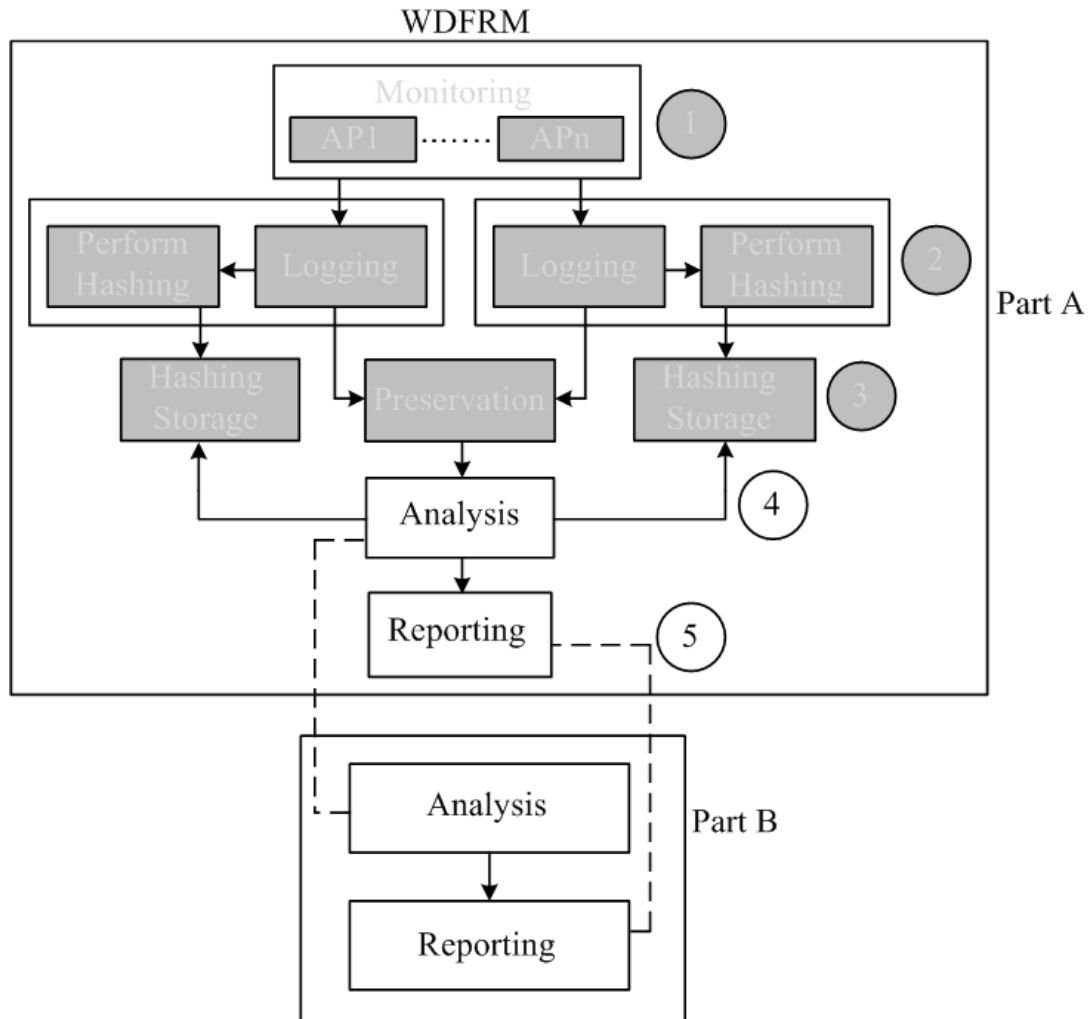


**Figure 5.4.** Preservation component

#### 5.2.4 Analysis and Reporting

The main purpose of the analysis and reporting component is to mine and extract the data from the ES to come up with digital evidence that can associate a particular adversary with a criminal activity committed on the WLAN. The analysis component is the one responsible for mining data from the ES. Although it is not within the scope of this study to discuss data mining in detail, the use of data-mining techniques should not be overlooked during the process of conducting a digital forensic investigation. The analysed data will then be passed to the reporting component.

The reporting component deals with the final evidence of the entire digital forensic investigation. It is used by the cyber forensic experts when they testify in a court of law that a suspect was found guilty due to the evidence they gathered from the investigation. It is then the decision of the judge/presiding officer in a court of law to decide whether the suspect is guilty or not, based on the evidence presented by the cyber forensic experts.



**Figure 5.5.** Analysis and reporting

The reader should note that the analysis and reporting components are not presented in detail – instead they are described with a view to seeing how they fit together in the context of the WDFRM. This is because monitoring, logging and preserving network traffic in a digital forensically sound manner are sufficient to demonstrate the viability of the WDFRM. The researcher nonetheless conducted an analysis of the data captured from the network and gives an example of how to report it in the later chapters of the dissertation. This will give the reader a sense of the actual digital evidence that can be used in a court of law.



The analysis phase is the most significant phase of the digital forensic investigation process since it is the one that should yield digital evidence that can be used in a court of law. According to Garfinkel (2010) and Casey et al (2011), organisations increasingly encounter digital data that would be difficult to analyse with today's digital forensic tools because of encryption, and not having a decryption key makes it challenging to find digital evidence (Spruill, 2012). Even when data is not encrypted, the sheer volume of it makes the search for evidence a difficult and time-consuming process.

Having introduced the reader to the different components of the proposed model, the chapter will now continue by putting the components together to create an integrated whole and provide a full picture of the model.

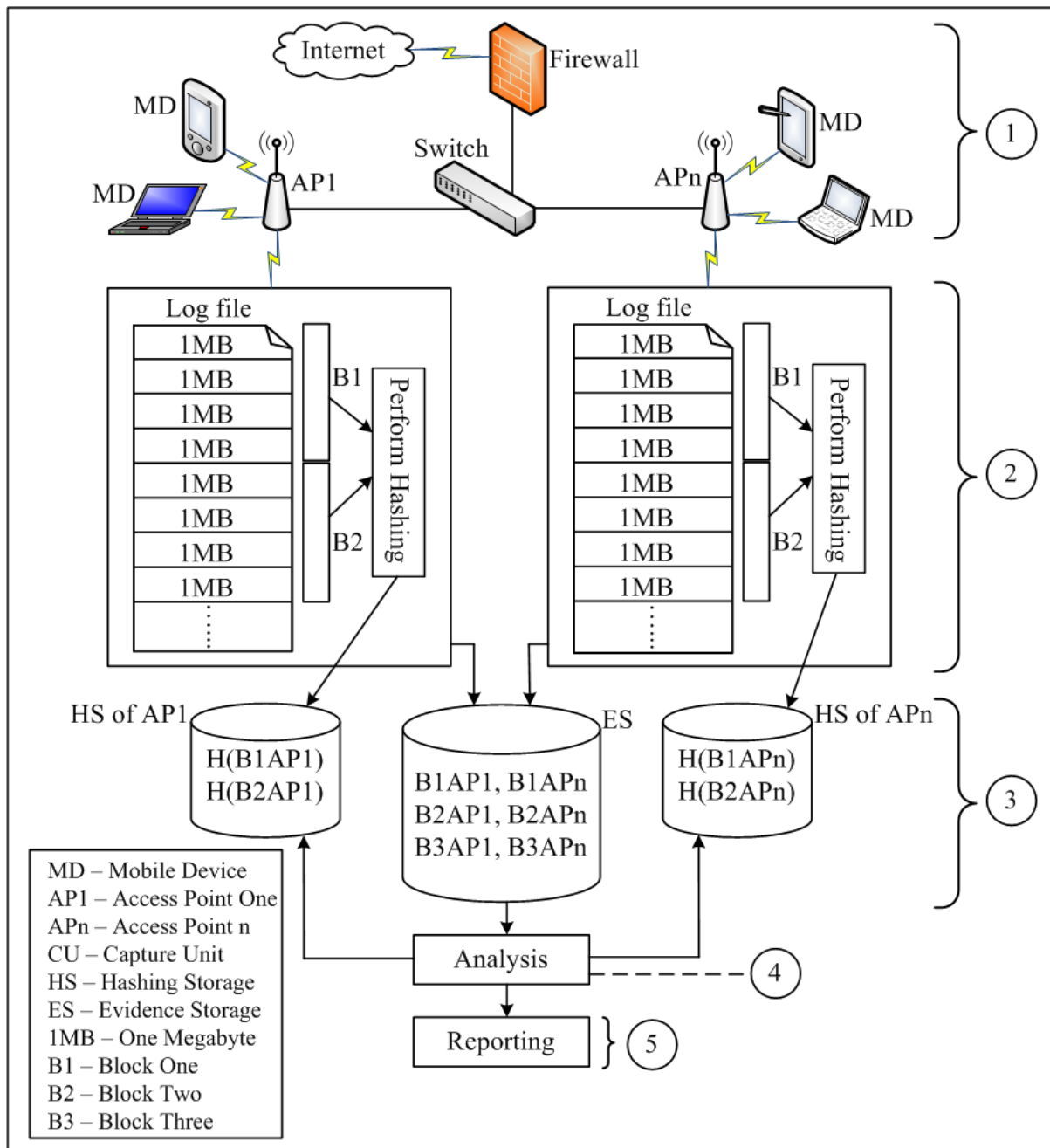
### 5.3 The WDFRM as an Integrated Whole

This section integrates the components discussed in the previous section and shows the WDFRM with all its components/phases. Figure 5.6 gives a graphical representation of the Wireless Digital Forensic Readiness Model (WDFRM). It shows how wireless traffic is monitored in the WLAN, how the monitored traffic is logged, and how the logged traffic is preserved to maintain its integrity. The analysis and reporting components, which render information that is forensically ready to be used by digital forensic experts, are also depicted.

The circled numbers 1 to 5 in the model represents the five phases of the digital forensic process which form the components of the WDRFM. In Figure 5.6, four mobile devices (MDs) and two access points (APs) are involved in the monitoring component. Two of the MDs are connected to each of the APs in a WLAN. It is assumed that these MDs have Internet access.

For the purposes of this dissertation, further assumptions are made, namely that the WDFRM is implemented in a device that is part of the WLAN, and that this device has a number of capabilities – i.e. monitoring wireless traffic, logging the monitored traffic, preserving the traffic, analysing the traffic and reporting the digital evidence. The component that does the logging receives all the monitored wireless network traffic from an AP and stores the data in a log file. The log file is divided into separate storage areas of, let's say, 4MB. The reason for choosing the 4MB capacity is that storing larger file sizes will reduce the number of records in the database (DB), which means during reconstruction, fewer records need to be extracted

from the DB. However, devices have a limited file storage space. Larger data files mean there will be less transmission to the server.



**Figure 5.6.** Wireless digital forensic readiness model

As the log file accumulates data, every fourth block (for example) is merged as a block of data. These blocks are then transferred to the Evidence Storage (ES), which constitutes the preservation component (Ngobeni and Venter, 2009). The WDFRM also assumes that the ES is a sufficiently large mass storage device. The hash values of each of these blocks are next

created and transferred to the hashing storage databases. In this way the integrity of the data that flows through the WLAN is preserved.

Let's assume that an incident is being reported on the WLAN. Responding to the reported incident will not require much effort because the digital data is already forensically stored. The cyber forensic experts will simply extract the data from the ES and do the analysis. The integrity of the analysed data can be shown beyond any doubt by creating hash values of each block from which the evidence was extracted, and matching those with the original hash values of each block as stored in the hashing storage. If the hash values match, it proves that the extracted digital evidence was in fact the original evidence, thus, it proves that the original evidence was not tampered with or manufactured.

#### **5.4 Concluding Remarks**

This chapter proposed a model for implementing digital forensic readiness in a Wireless Local Area Network environment. The model is based on the notion that the logging and preserving of network traffic before an incident occurs can minimise the cost and time needed to conduct a fully-fledged digital forensic investigation. This is because a part of the digital forensic investigation process – that is, the monitoring, logging and preserving of network traffic – has already been done.

The chapter introduced the model in the form of a black box at first (as shown in Figure 5.1), in order to provide the reader with a holistic view before delving into the functions of every component that constitutes the entire model. The components were subsequently explained in detail with a view to showing how they interact with one another to form the complete model. In addition to this, the components were put together to depict the model as an integrated whole. Having introduced the reader to the Wireless Digital Forensic Readiness Model proposed here, the chapter addressed the problem in principle as identified earlier in this dissertation. It next continues to discuss in more detail the prototype and experiments of the model as a proof of concept.

The next part, Part IV, will focus exclusively on the development of the prototype and an analysis thereof.

## **PART IV: Prototype and Experiment Tools**

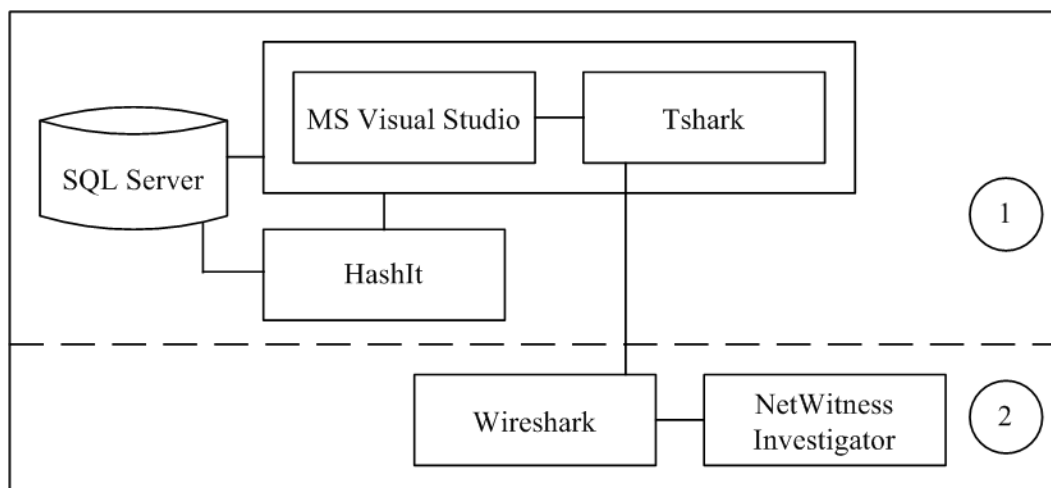
## Chapter 6      **Prototype Tools**

### 6.1 Introduction

Part III of this dissertation proposed a model that attempts to address the problem identified in this research. The WDFRM as a whole, as well as each component was explained in detail.

Part IV consists of three chapters – Chapters 6, 7 and 8 – which are devoted to the implementation of the model by means of a prototype. The set of tools used by the researcher to implement the prototype are indicated by the area containing a circle numbered 1 in Figure 6.1. After implementing the prototype, the researcher analyses the results of the prototype by conducting two experiments. The experiments are also conducted by using a set of tools that are indicated by the area containing a circle numbered 2 in Figure 6.1.

Chapter 6 is devoted to introducing the reader to both the tools used to develop the prototype and the tools used to conduct the experiments. The reader should note that the researcher does not discuss these tools in detail, but merely gives an overview of them. He shows how they fit together to develop the prototype and refers to the actual prototype experiments that will be presented in Chapter 8. The reader should also note that the researcher did not develop any of these tools but simply used them to perform specific functions in accordance with the requirements of the proposed model.



**Figure 6.1.** Prototype and experiment tools





Chapter 7 is devoted to the development of the prototype itself using the tools introduced in Chapter 6. The prototype demonstrates how traffic is captured from the wireless network and stored in a digital forensically sound manner. This is done so that when a digital forensic investigation is warranted, it can be shown beyond any reasonable doubt that the traffic captured from the wireless network was not tampered with.

Chapter 8 takes the network traffic captured and stored in a digital forensically sound manner (see Chapter 7) and analyses it by conducting two experiments. As in Chapter 7, the same set of tools introduced in Chapter 6 is again used to conduct the experiments.

The remainder of this chapter is structured as follows: Section 6.2 presents the set of tools used to *develop the prototype*. Section 6.3 presents the set of tools used to *conduct the experiments*. Section 6.4 concludes the chapter.

## 6.2 Tools Used to Develop the Prototype

This section introduces the reader to the tools that are used to develop the Wireless Digital Forensic Readiness prototype. The reader is first acquainted with the computer/ physical system requirements in which the prototype is developed and later receives an explanation of the tools.

### 6.2.1 Computer/ Physical System Requirements

The prototype that will be discussed in Chapter 7 and the experiments that are presented in Chapter 8 are conducted in a machine complying with the following system requirements:

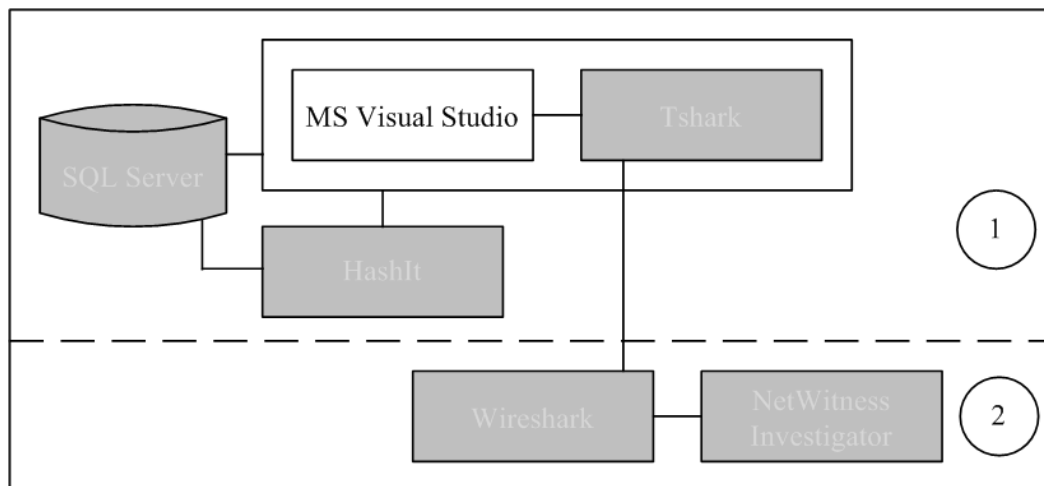
- System Type: 64-bit Operating System, Windows 7
- Processor: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2.99 GHz
- RAM: 4.00 GB
- Hard Disk Drive: 250 GB
- Network Adapter: Intel (R) 82567LM-3 Gigabit Network Connection

A computer system meeting the above requirements was chosen because it was sufficient to develop the prototype as a proof of concept.

Having introduced the reader to the system requirements for the prototype development, the next section presents the tools that will be used to develop the prototype and to conduct the experiments.

### 6.2.2 Microsoft Visual Studio Express 2012 for Windows Desktop

Figure 6.1 serves as the basis for all the figures in this section (6.2 – 6.8). In the case of Figure 6.2 – Figure 6.8 (except for Figure 6.6) the difference is that the unshaded tool represents the tool that is discussed in that section. In the case below, the unshaded tool in Figure 6.2 represents the Microsoft Visual Studio software, which is used to develop the prototype.



**Figure 6.2.** Microsoft Visual Studio

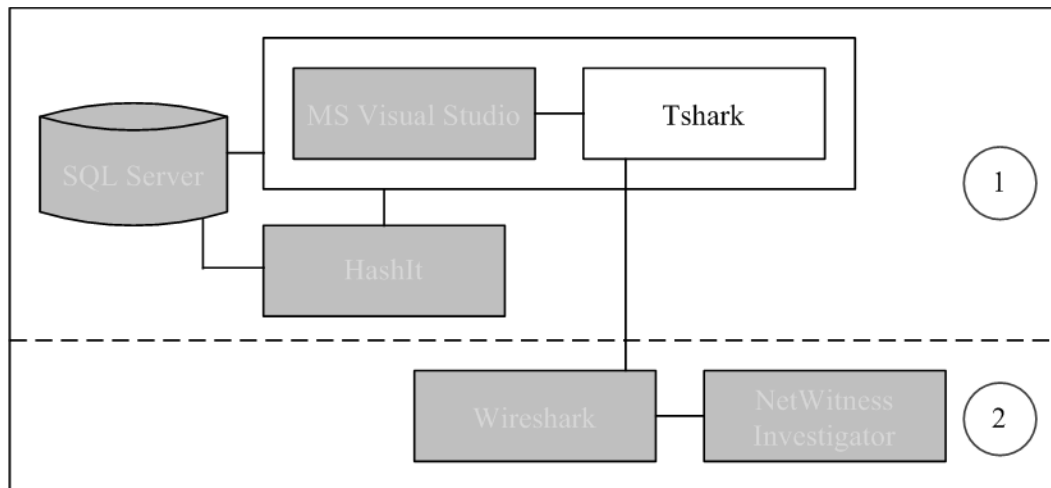
Microsoft Visual Studio Express 2012 for Windows Desktop is a software development environment, also known as an Integrated Development Environment (IDE) (Visual Studio, 2013). It is a free version of the popular MS Visual Studio 2010 IDE edition and is used primarily by software developers to build software products, websites and utilities (Visual Studio, 2013). This tool is used as an IDE to develop the prototype presented in Chapter 7. The IDE has a set of minimum system requirements on which it should be run, which are the same as those presented in Section 6.2.1.

In addition to the above, MS Visual Studio supports various native Windows languages such as C#, VB.NET, and C++ (Microsoft, 2013a). The C# programming language was used for the purposes of this research and proved to be useful in achieving the objective of the prototype.

One of the requirements of the WDFRM is that the prototype should be able to capture traffic from the network. This is achieved by using a tool called Tshark, which is discussed in the next section.

### 6.2.3 Tshark

This section is devoted to a brief explanation of the Tshark application.



**Figure 6.3.** Tshark

Tshark is an open-source command-line-oriented version of Wireshark (Wireshark, 2013). It is used to capture packets from a live network or to read packets from a previously saved capture file, either by printing a decoded form of those packets to a standard output or writing the packets to a file (Tshark, 2013). Packet capturing in Tshark is performed using the pcap library (Tshark, 2013).

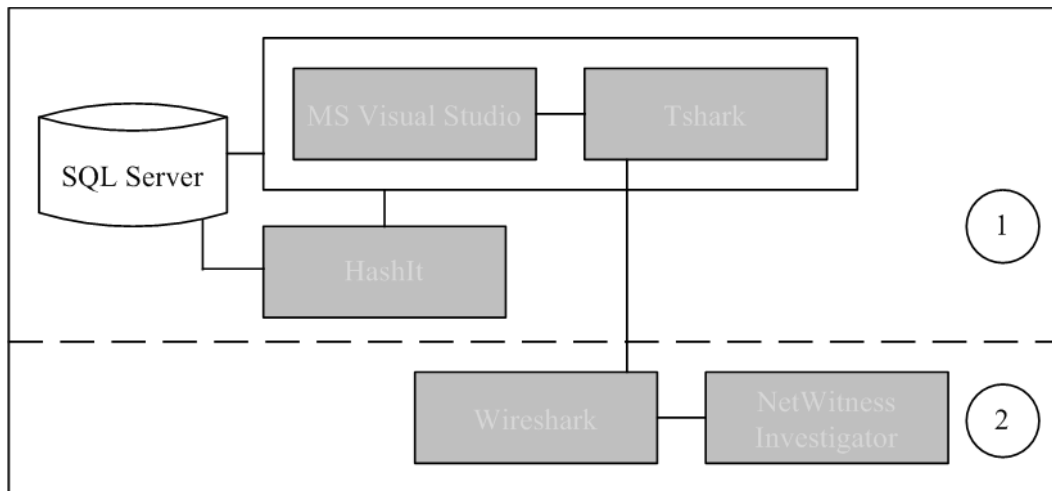
There are other tools similar to Tshark that can be used to capture traffic from the network, such as Wireshark, tcpdump, Ettercap, Kismet and Dsniff, to mention but a few. However, the main reason why the researcher chose to use Tshark was that it provides flexibility to pass flags on the command-line to achieve specific objectives of the prototype. For example, it can specify the network interface from which to listen to the traffic, the size of the packet, the packet file format, and the location in which the packets should be stored.

One of the requirements of the WDFRM is that the prototype should take the captured traffic and store it in a flat file, as well as hash the same traffic and store the resulting hash values in a database.

Now that the reader has been introduced to the tool used to capture the traffic, the next section discusses the type of database that is used to store the generated hash values.

#### 6.2.4 Microsoft SQL Server 2012 Management Studio

In this section the reader is introduced to the database used in the development of the prototype, which is the Microsoft SQL Server Management Studio.



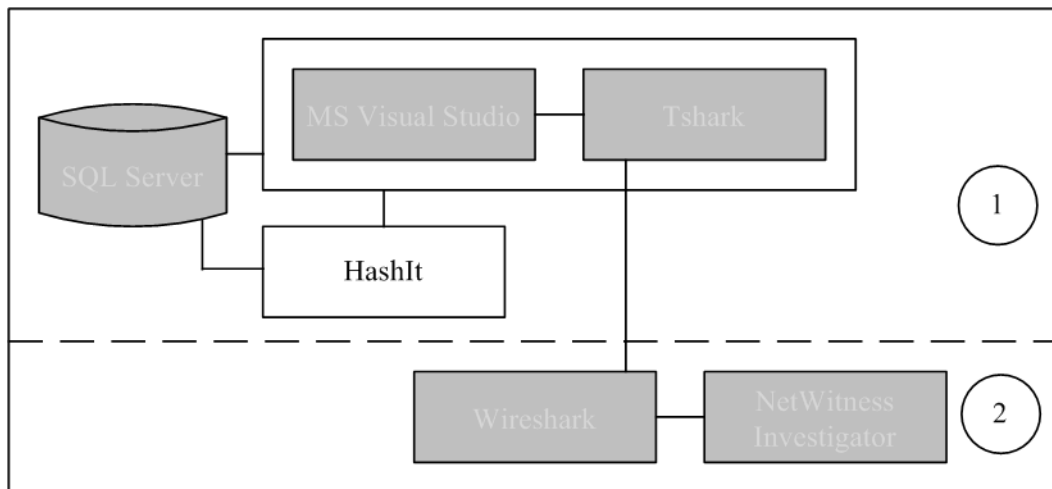
**Figure 6.4.** SQL server

Microsoft SQL Server 2012 Management Studio is an open-source, easy-to-use database management tool used to store and retrieve data as requested by other software applications (Microsoft, 2013b). For the purpose of the prototype, the MS Visual Studio calls the SQL server to store the hash values of the traffic captured from the network.

One of the requirements of the WDFRM is that the prototype should be able to prove beyond any reasonable doubt that the traffic captured from the network has not been compromised. To achieve this, the prototype uses a tool called HashIt, which is explained in the next section.

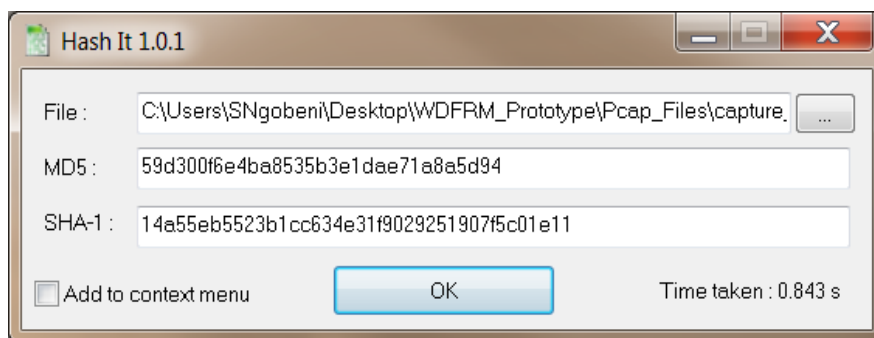
#### 6.2.5 Hash Utility - HashIt

This section describes the HashIt application, which aims at proving the integrity of the data captured from the WLAN. The researcher wishes to state upfront that the HashIt application is not directly involved in the development of the prototype, but merely a secondary tool used to generate hash values of the traffic captured from the network for integrity verification purposes.



**Figure 6.5.** HashIt

HashIt is an open-source and fast application that has been designed to generate both the MD5 and SHA-1 hash values of any given input file. It works on Windows platforms (TrishTech, 2013). Figure 6.6 shows the HashIt utility with a hashed4MB pcap file. Note that it took 0.843 seconds to generate both MD5 and SHA-1 hash values of the loaded file. The speed of the HashIt remains of paramount importance, because the digital forensic experts will need a bunch of traffic to be hashed as quickly as possible in a real digital forensic investigation.



**Figure 6.6.** HashIt utility

Should a digital forensic investigation be warranted, the digital forensic experts will need to prove beyond any reasonable doubt that the data captured by Tshark was not tampered with. To show this, the prototype takes the original traffic captured by Tshark and hashes it using the HashIt application as shown in Figure 6.6. The resulting MD5 and SHA-1 hash values from the HashIt application will then be compared with those stored in the SQL server

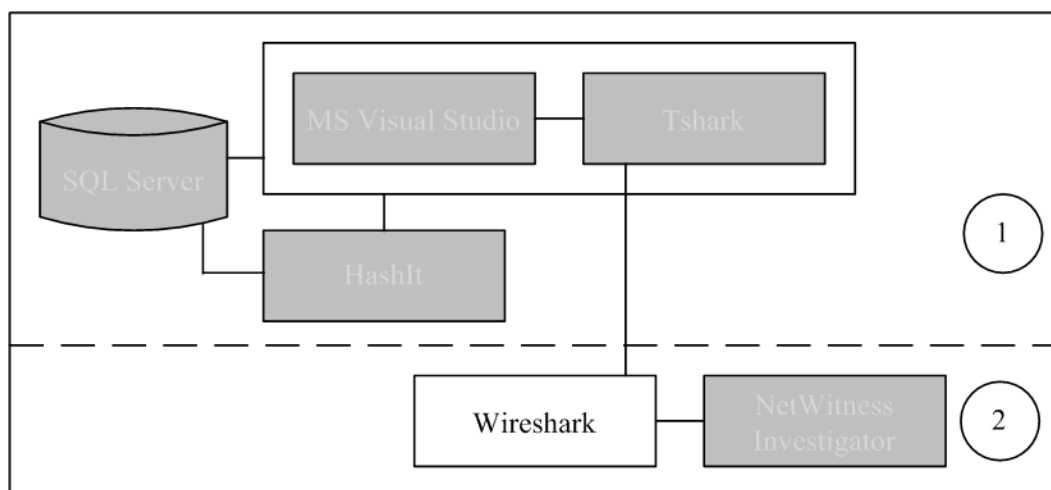
database. If the hash values match, then it will mean that the original data has not been compromised. Section 6.2 introduced the reader to all the tools that will be used to develop the prototype. In the next section, the researcher introduces the reader to the tools that will be used to conduct the actual experiments (explained in detail in Chapter 8).

### 6.3 Tools Used to Conduct the Experiments

After capturing and storing the traffic in a digital forensically sound manner, using the set of tools introduced in the previous section, the next step is to analyse this traffic in order to make sense of it. To achieve this, the researcher will conduct two experiments where this traffic gets reassembled in an attempt to determine if they contain any footprints that might constitute digital evidence. The application tools to be discussed in this section are Wireshark and NetWitness Investigator.

#### 6.3.1 Wireshark

This tool was defined in Section 4.3.1.1 above. It provides a rich set of features such as packet capturing, saving, opening, importing, exporting, filtering, searching, colouring, and creating various packet statistics.



**Figure 6.7.** Wireshark

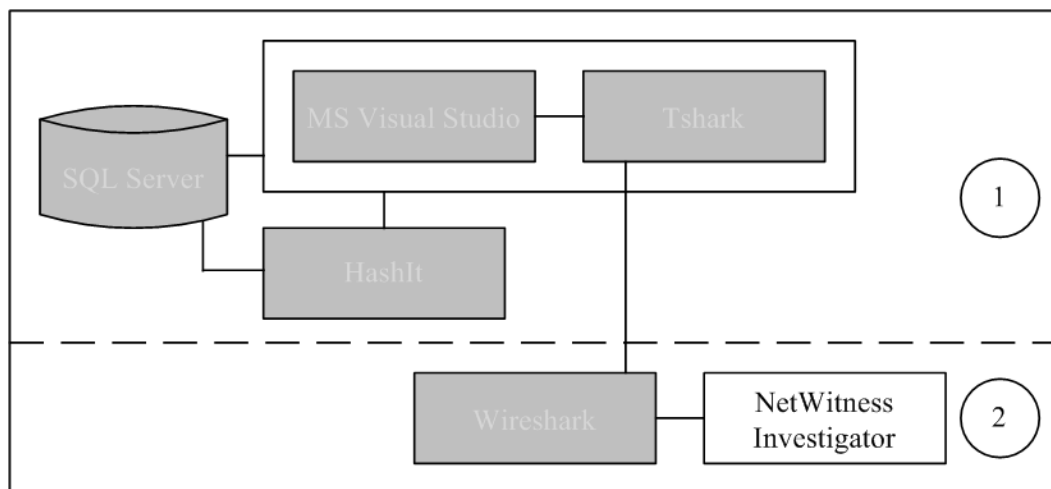
It should be noted that there are other tools similar to Wireshark that may be used to analyse traffic captured from a network, inter alia Tshark, tcpdump, Ettercap and Dsniff. However, since the traffic that flows through the network looks murky and difficult to understand, the researcher chose to use Wireshark. Wireshark provides a Graphical User Interface (GUI)

which is easy to navigate and which can view packets in a more readable format. For example, the user can view a capture of a whole session.

Once the packets have been viewed in a more readable and understandable way, a tool called NetWitness Investigator will be used to analyse the packets. In the next section, the researcher describes the NetWitness Investigator.

### 6.3.2 NetWitness Investigator

Figure 6.8 is again similar to Figure 6.1, but now the unshaded tool represents the NetWitness Investigator application, which is also used to conduct the experiment. A brief explanation of NetWitness Investigator follows in this section.



**Figure 6.8.** NetWitness Investigator

NetWitness Investigator is the proprietary software that effectively captures and analyses network traffic starting from application layer entities such as users, emails, addresses, files, and actions (Girardi, 2010). This software, however, has a free-ware version, which will be used in the experiments. The free-ware version can only support up to 25 users simultaneously with a data capture of up to 1GB. The reader should note that a data capture of 1GB was sufficient for the purpose of the experiment. The proprietary version of the software supports Linux-based network appliances and remote network monitoring, automated reporting, and data recording (Gross, 2008).

The features of NetWitness Investigator include its ability to do live capturing of raw packets from a wired or 802.11 wireless networks, importing and exporting of packets in the .pcap



file format, filtering, full content search, resolving IP addresses to city/country using integrated GeoIP, hashing, and SSL decryption (Girardi, 2010).

For the purpose of this research, NetWitness Investigator will be used in the experiments to analyse the traffic captured from the network and uncover the actual data that might be linked to the suspect and used as digital evidence during a digital forensic investigation. Though NetWitness Investigator provides the capability of capturing network traffic just like Tshark, the researcher chose to use Tshark because it is a command-line-oriented tool that enables the researcher to pass flags in it – something that could not be achieved by either NetWitness Investigator or Wireshark.

Having introduced the reader to the tools used to develop the prototype and to conduct the related experiments, the next section concludes this chapter with a brief summary.

#### **6.4 Concluding Remarks**

Chapter 6 presented the tools that will be used to develop the prototype in Chapter 7 and to conduct the experiments in Chapter 8 respectively. The chapter started off by introducing the reader to the computer/ physical system requirements on which the prototype will be developed and further explained the appropriate tools in detail.

Each tool was considered as a separate entity and discussed to show how it will be used in the development of the prototype and the associated experiments. Having introduced the reader to these tools, this dissertation will now continue to discuss how the prototype of the model presented in Chapter 5 was designed and developed using the tools presented in this chapter.



## Chapter 7      **Prototype Development**

### **7.1 Introduction**

Chapter 6 introduced the reader to the tools used to develop the prototype and to conduct the prototype experiments, with the latter discussed in detail in Chapter 8.

Chapter 7 presents the prototype as a means to validate the development of digital forensic readiness in a WLAN environment. The proposed model consists of five digital forensic phases marked by the five circled numbers on the right-hand side in Figure 7.1: Phase 1 (monitoring), Phase 2 (logging), Phase 3 (preservation), Phase 4 (analysis), and Phase 5 (reporting). For the sake of convenience, Figure 7.1 is a repetition of Figure 5.6 because the prototype implements these phases. Chapter 7 focuses only on the development of Phases 1, 2 and 3, which are all encircled in grey in Figure 7.1.

The three phases presented in this chapter are sufficient to show the viability of the proposed model. The phases demonstrate that capturing and storing network traffic in a digital forensically sound manner not only minimises the cost of conducting a digital forensic investigation from beginning to end, but also maintains the integrity of the network traffic that has been collected.

Phase 4 (reporting) and Phase 5 (analysis) are presented in Chapter 8 in the form of experiments. The researcher takes a step further in these phases and analyses the data captured and stored in phases 1, 2 and 3. The details of Phases 4 and 5 will be unpacked in Chapter 8.

Chapter 7 continues by presenting a high-level overview of the prototype setup and introduces the reader to the specific network components that were used for the prototype setup. Next, the researcher presents the monitoring phase (Phase 1) and explains the installation and configuration of the prototype in a WLAN environment. Next phase 2 (logging) is presented. This phase shows through demonstration how the prototype logs the bunch of traffic that flows through the WLAN. In Phase 3 (preservation), the researcher demonstrates how the logged traffic is stored in a way that will not compromise its integrity. The chapter as a whole is then concluded with a brief summary.

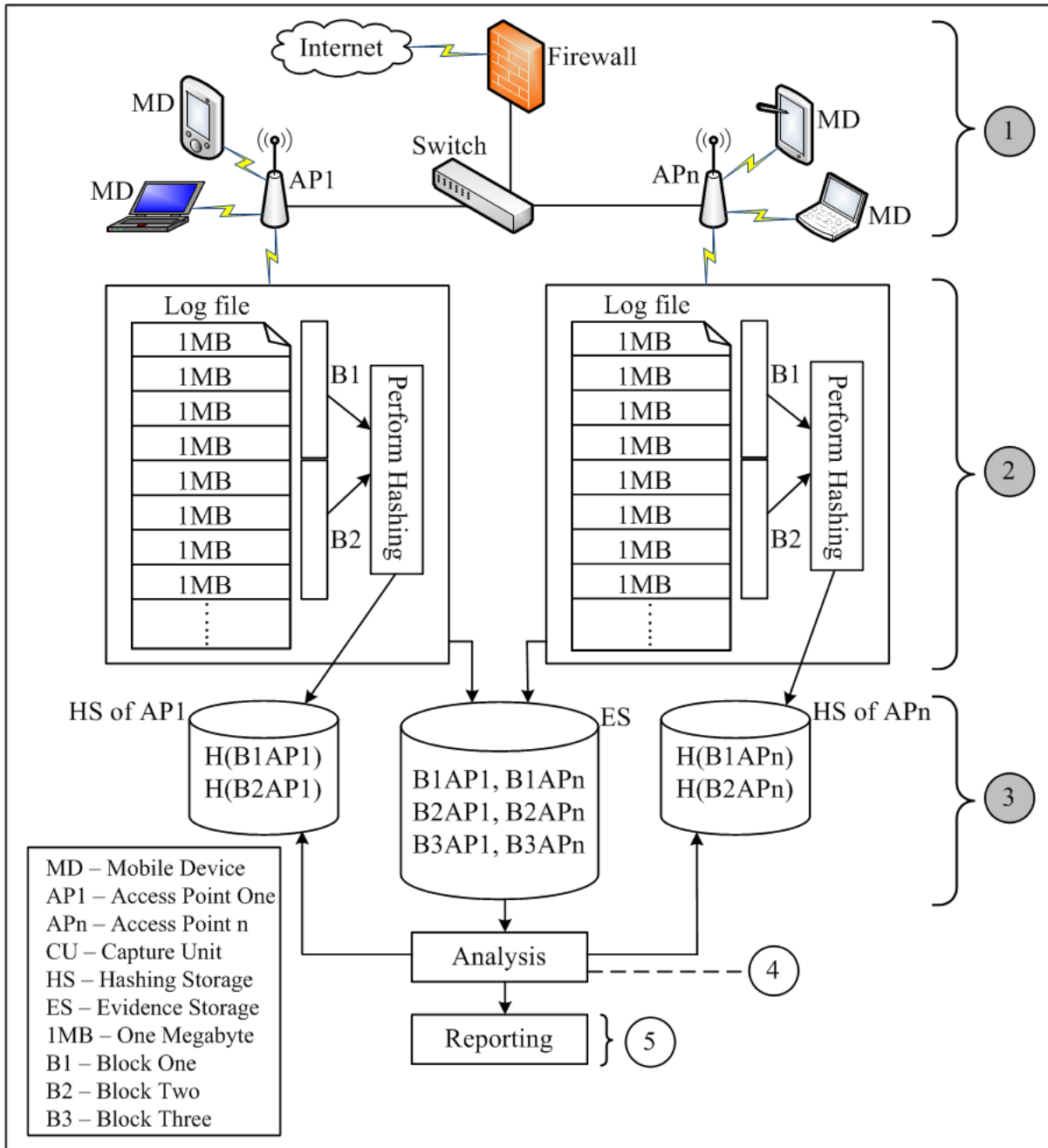


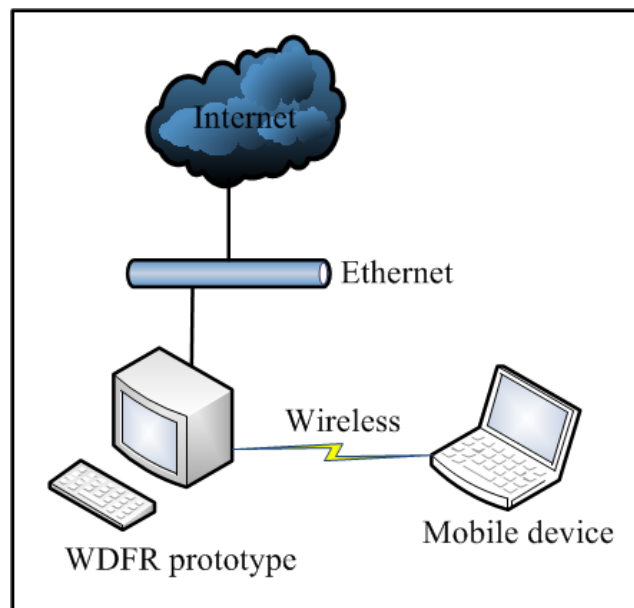
Figure 7.1. Wireless digital forensic readiness model (duplication of Figure 5.6)

## 7.2 Prototype Setup

This section acquaints the reader with the prototype setup. Figure 7.2 contains an overview of the prototype setup, which consists of the *Wireless Digital Forensic Readiness prototype*, *Mobile device*, *Ethernet* and *Internet*. In order for the mobile device to get internet connectivity from the WLAN, it should first connect to the WDFR prototype, which then connects it to the Internet through the Ethernet adapter. The connection between the WDFR prototype and the mobile device is wireless. In other words, the WDFR prototype can be seen

as an access point in a real-life WLAN setup, which performs the association function. It can also be viewed as a separate system that is linked directly to the access point. A detailed discussion on how a mobile device associates with the access point for Wi-Fi connectivity was presented in Chapter 2 of this dissertation.

The WDFR prototype implements the model proposed in Chapter 5. Phases 1, 2 and 3 of the proposed model are developed in the WDFR prototype in this chapter, while Phases 4 and 5 are developed in the next chapter. The WDFR prototype can be viewed as an access point with built-in functionalities of traffic monitoring, logging and preservation.



**Figure 7.2.** Overview of prototype setup

The dissertation next continues to present the first three phases, namely monitoring, logging and preservation.

### 7.3 Phase 1 (Monitoring)

This phase entails the preparation or setting up of the WDFR prototype. This includes the installation and configuration of all the tools introduced in Chapter 6. This phase can also be seen as the network management phase, because it allows the user of the prototype to configure the WDFR prototype in a way that meets the business requirements of the organisation that controls or owns the WLAN or hotspot.

For example, the user can configure the WDFR prototype to monitor specific types of traffic, due to suspicious behaviour detected in the network earlier.

After installing, configuring and getting the WDFRM prototype to monitor the wireless network traffic, the next step is to start the traffic-logging process (which is presented next).

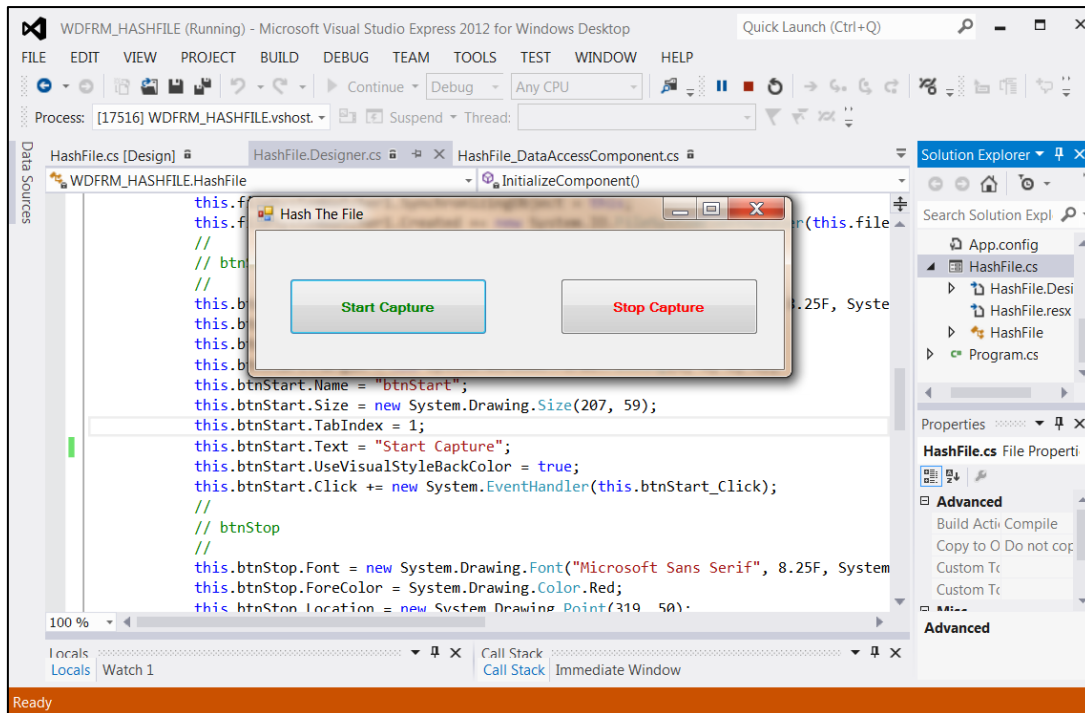
#### 7.4 Phase 2 (Logging)

The main essence of this section is to explain through demonstration how traffic is captured from the network and stored in a forensically sound manner.

To start the traffic-capturing process, the prototype presents the user with a dialog box as shown in Figure 7.3. The dialog box consists of two options, namely “Start Capture” and “Stop Capture”. The reader should note that the “Stop Capture” option is initially disabled because the prototype needs to start capturing traffic first before it can be halted. When the user clicks on the “Start Capture” button, the prototype invokes the Tshark application, which then starts capturing some of the raw packets as they traverse the WLAN. Once the traffic-capturing process has been launched, the “Stop Capture” option becomes enabled; therefore the traffic-capturing process can be halted.

One of the requirements of the proposed model is that, as the packets are captured from the WLAN, they should be stored in a flat file in the form of a standard output file called a pcap file. A pcap is a native file format of a dump capture of Ethernet sniffing software such as tcpdump, Wireshark and Tshark (Filetext, 2013). In this case, the Tshark application captures a bunch of packets from the network and writes them into the pcap file. The prototype then passes flags on the Tshark application, which determines the parameters such as location, size, interface, and when a new output file should be created. Table 7.1 shows a summary of the Tshark flags used in the prototype.

It can be noted from Table 7.1 that the prototype uses the `-i` flag to specify the network interface from which the traffic should be captured. After specifying the network interface, the prototype calls Tshark, which then invokes the `-a` flag. The `-a` flag specifies the output file size which is 4MB. This suggests that as the traffic is accumulated from the network, it gets written to an output file until it reaches a size of 4MB.



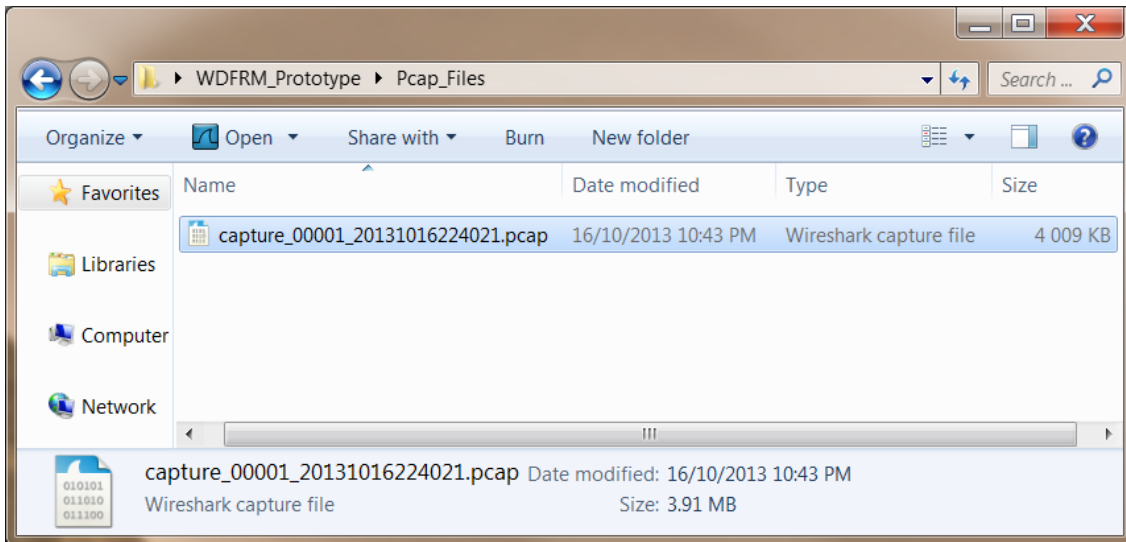
**Figure 7.3.** Start or stop capturing network traffic

When the first output file is written with 4MB of traffic, the Tshark invokes the `-b` flag, which then creates a new output file to be written with packets until it reaches the same file size as that of the `-a` flag. Lastly, the prototype calls the Tshark which invokes the `-w` flag. The `-w` flag specifies the location of the flat file within the WDFR prototype in which every written output file should be stored. The location or directory of the flat file in the WDFR Prototype is: “C:\Users\SNgobeni\Desktop\NAP\_Prototype\Pcap\_Files\capture.pcap”.

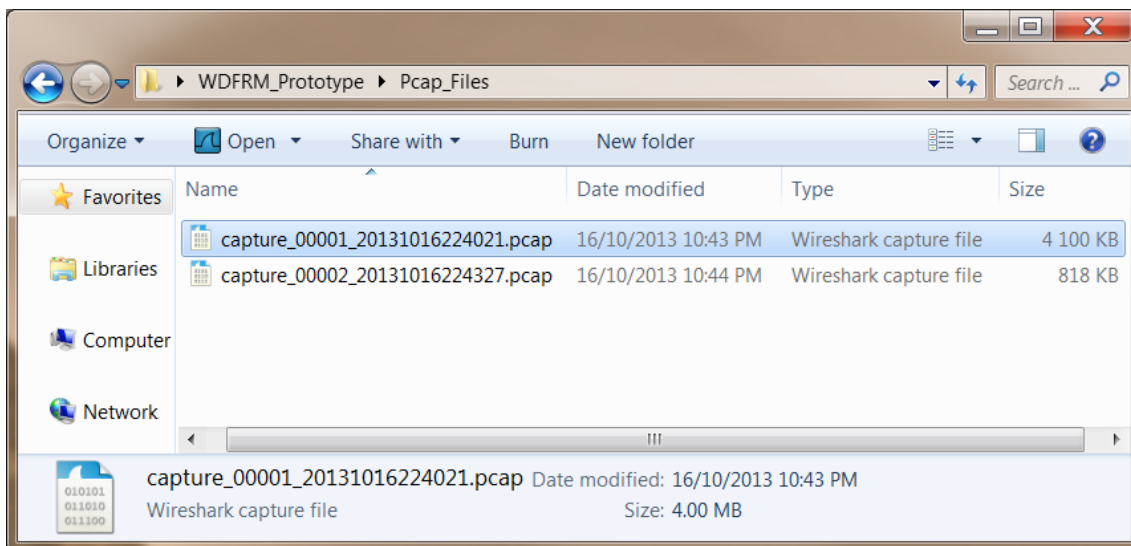
**Table 7.1.** Tshark flags

Tshark Flags	Description
<b>-a</b>	Specifies the file size of each Tshark output file. For the purpose of this prototype, an output file size of 4MB is used.
<b>-b</b>	Specifies that once the first output file is written with traffic of 4MB, the prototype should create a new output file to be written with packets of the same size as that of the <code>-a</code> flag.
<b>-i</b>	Specifies the network interface from which the prototype should capture traffic.
<b>-w</b>	Specifies the file location in which the Tshark output files should be stored.

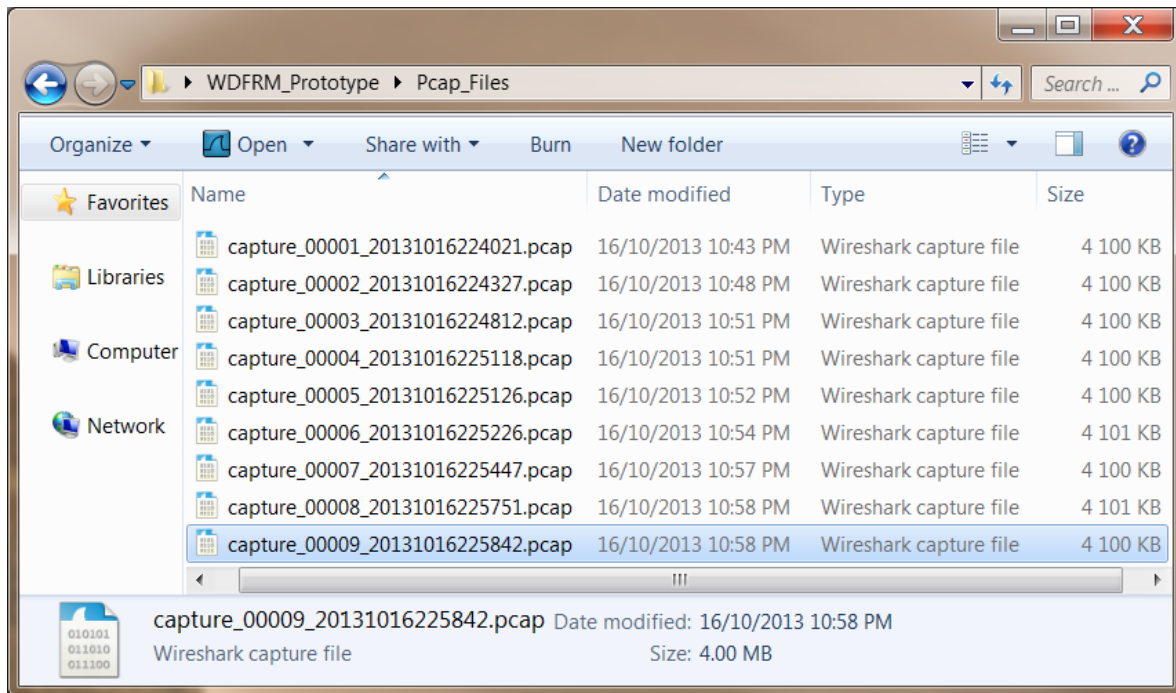
Figure 7.4 shows a flat file containing the first output file of Tshark. The reader should note that the size of the output file is 3.91MB at this stage. This suggests that Tshark is still capturing and writing traffic on this output file until it reaches 4MB. In Figure 7.5, the first output file is now written with 4MB of traffic, therefore a new output file is immediately created which should be written into. Figure 7.6 indicates nine output files with each output file consisting of 4MB of traffic.



**Figure 7.4.** One output file of Tshark



**Figure 7.5.** Two output files of Tshark



**Figure 7.6.** Ten output files of Tshark

Having demonstrated how the prototype captures network traffic by passing specific flags on the Tshark command-line, the next section shows how the prototype preserves the captured traffic to maintain its integrity.

## 7.5 Phase 3 (Preservation)

This phase is intended to introduce the reader to the way in which the prototype preserves the traffic captured in the preceding section to maintain its integrity. The prototype achieves this by encoding the traffic in Figure 7.6 using MD5 and SHA-1 and stores the resulting hash values in a database. The hash values are then verified to determine whether the original traffic was not perhaps compromised.

### 7.5.1 Hashing

To stop the traffic-capturing process, the user should click on the “Stop Capture” button (see Figure 7.3). The prototype then displays the message box indicated in Figure 7.7 to show that the traffic-capturing process has been stopped.

After stopping this process, the prototype immediately creates MD5 and SHA-1 hash values of every output file stored in Figure 7.6. The created hash values are then stored on the SQL server database with the corresponding file name of each output file.





**Figure 7.7.** Dialog box indicating that traffic capturing has been stopped

Table 7.2 indicates an SQL server database with both MD5 and SHA-1 hashes. Storing the hash values of the Tshark output files in the SQL server database is important for verifying the integrity of the output files, should a digital forensic investigation be warranted later. The UniqueNumber in Table 7.2 is the primary key that uniquely identifies each tuple in the table of the database.

**Table 7.2.** SQL server database with MD5 and SHA-1 hash values of Tshark output files

UniqueNumber	PcapFileName	MD5_HashValue	SHA1_HashValue
6002	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00001_20131016224021.pcap	6fef52b0903c954ecf98cb64be95f5fd	02f066682ee9264c9d4c4960c4260c793389c0b3
6003	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00002_20131016224327.pcap	51b8d2ecf1b5ac43ecf594cd67129088	1db6b2df31c3ca26d86d3248eadc5f7c36cb6bfd
6004	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00003_20131016224812.pcap	a4f4f0cb3f6389ec5a2bd16fc77cb4b4	9dc3b0b77e95895f84e32682fd9685dc3a8d467b
6005	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00004_20131016225118.pcap	ce05b15fa35d768ad27b522705407c9a	16a9f16816586a67ea6ebc70c9919b3c0adf451b
6006	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00005_20131016225126.pcap	fb4f306f7d579092b98700d9a78def2e	ae4c3aa44f6aa87e15db742d6a6e35c27ac588c8
6007	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00006_20131016225226.pcap	12bdba9518ec4b6d73e76cbb8f4e9f17	8710ee97666dfdb1e345fa27885c8795c586a93d
6008	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00007_20131016225447.pcap	9032da507572a5237791924c229f7d1c	dc8869cf02615e744de29d4237cdf3271f899fee
6009	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00008_20131016225751.pcap	afe118eb77719b176d8bf7c887f27d46	36247e1c1bad34aec39aab2428d63b8fb171c93a
6010	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00009_20131016225842.pcap	3b685a6dc3d3b7e863fcf6fa551d606	429cfe3d76e11295df6ea40a56e978ccc78265c2
NULL	NULL	NULL	NULL

The data in the SQL database is next exported to the Microsoft Excel application. The main reason for exporting the data to the Excel application is that the data in the Excel application can be easily read, while that in the SQL database might need the issuing of a command to read them. This will allow the forensic experts to easily extract the data in the Excel package and use it as part of the digital evidence when testifying in a court of law. Table 7.3 depicts the Excel Hash Table exported from the SQL server database.

**Table 7.3.** Excel Hash Table with MD5 and SHA-1 hash values of the Tshark output files

	UniqueNumber	PcapFileName	MD5_HashValue	SHA1_HashValue
1	6002	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00001_20131016224021.pcap	6fef52b0903c954ecf98cb64be95f5fd	02f066682ee9264c9d4c4960c4260c793389c0b3
2	6003	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00002_20131016224327.pcap	51b8d2ecf1b5ac43ecf594cd67129088	1db6b2df31c3ca26d86d3248eadc5f7c36cb6bfd
3	6004	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00003_20131016224812.pcap	a4f4f0cb3f6389ec5a2bd16fc77cb4b4	9dc3b0b77e95895f84e32682fd9685dc3a8d467b
4	6005	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00004_20131016225118.pcap	ce05b15fa35d768ad27b522705407c9a	16a9f16816586a67ea6ebc70c9919b3c0adf451b
5	6006	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00005_20131016225126.pcap	fb4f306f7d579092b98700d9a78def2e	ae4c3aa44f6aa87e15db742d6a6e35c27ac588c8
6	6007	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00006_20131016225226.pcap	12bdba9518ec4b6d73e76cbb8f4e9f17	8710ee97666dfdb1e345fa27885c8795c586a93d
7	6008	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00007_20131016225447.pcap	9032da507572a5237791924c229f7d1c	dc8869cf02615e744de29d4237cdf3271f899fee
8	6009	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00008_20131016225751.pcap	afe118eb77719b176d8bf7c887f27d46	36247e1c1bad34aec39aab2428d63b8fb171c93a
9	6010	C:\Users\SNgoben\Deskto\WDFRM_Prototype\Pcap_Files\capture_00009_20131016225842.pcap	3b685a6dc3d3b7e863fcf6fa551d606	429cfe3d76e11295df6ea40a56e978ccc78265c2



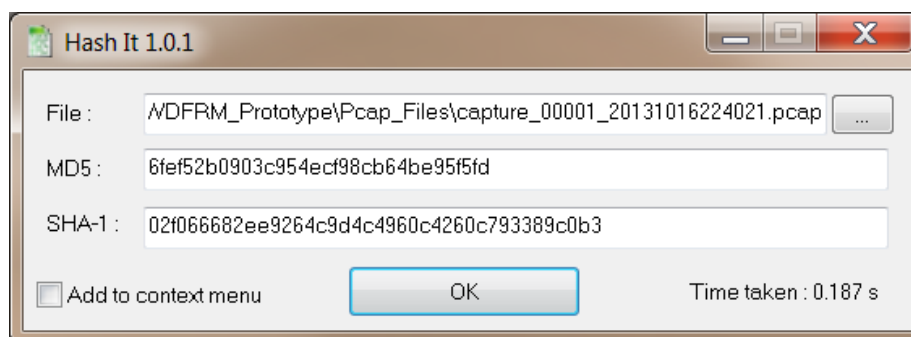
One should note that at this stage the researcher is not interested in what is inside the packets that were captured from the wireless network; instead the researcher is interested in capturing and storing the packets in a digital forensically sound manner. The next subsection shows how to verify the integrity of the hashes stored in the SQL database.

### 7.5.2 Hashing Verification

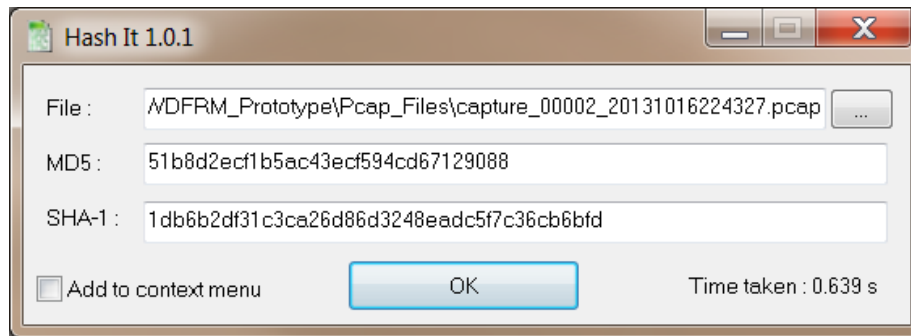
The researcher would like to state upfront that the hashing verification process is done manually after the prototype has logged the traffic from the WLAN. The reader should note that though this process is conducted to verify the integrity of the data produced by the prototype, it is independent of the prototype and should not be viewed as a process that was developed by the researcher.

The researcher verifies the integrity of the hash values stored in the SQL database by taking the original output files stored in the flat file in Figure 7.6, encoding them and generating both the MD5 and SHA-1 hash values. This process is conducted manually by using a tool called HashIt (see Chapter 6, Section 6.2.5) to perform the encoding. The resulting hash values of HashIt are then compared with those of the prototype stored in the SQL server database (see Table 7.4). If the hash values in the SQL server database and those of the HashIt are the same, it means the original output files were not tampered with. The reader should keep in mind that the HashIt application uses the same MD5 and SHA-1 hashing functions as the prototype.

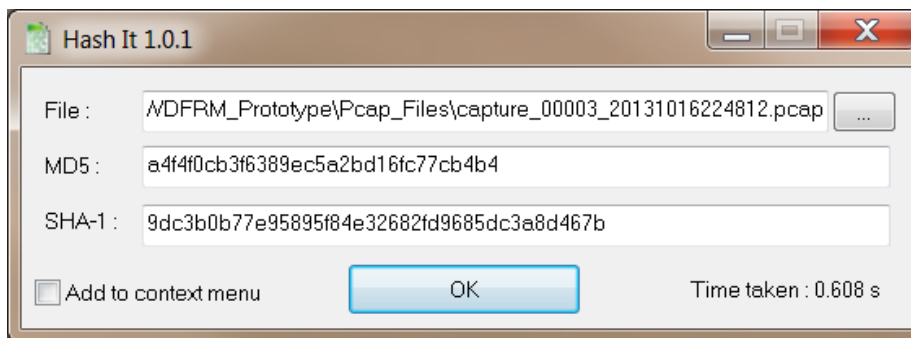
Figure 7.8, Figure 7.9 and Figure 7.10 respectively show the MD5 and SHA-1 hash values of the first, second and third output files in the flat file of Figure 7.6.



**Figure 7.8.** MD5 and SHA-1 of output file number 00001



**Figure 7.9.** MD5 and SHA-1 of output file number 00002



**Figure 7.10.** MD5 and SHA-1 of output file number 00003

Table 7.4 shows a comparison of the MD5 and SHA-1 hash values in the SQL server database generated by the prototype with those generated by the HashIt application. It is evident from Table 7.4 that encoding the output file number 00001 with HashIt generates the same MD5 and SHA-1 hash values as those of the prototype. Similarly, the HashIt MD5 and SHA-1 hash values of the output files 00002 and 00003 are the same as those of the prototype.

**Table 7.4.** Comparison of MD5 and SHA-1 hash table for the prototype and HashIt

Output File Number	Prototype MD5	Prototype SHA-1	HashIt MD5	HashIt SHA-1
00001	6fef52b0903c954ecf98c b64be95f5fd	02f066682ee9264c9d4c496 0c4260c793389c0b3	6fef52b0903c954ecf98c b64be95f5fd	02f066682ee9264c9d4c496 0c4260c793389c0b3
00002	51b8d2ecf1b5ac43ecf59 4cd67129088	1db6b2df31c3ca26d86d324 8eadc5f7c36cb6bfd	51b8d2ecf1b5ac43ecf5 94cd67129088	1db6b2df31c3ca26d86d324 8eadc5f7c36cb6bfd
00003	ce05b15fa35d768ad27b 522705407c9a	9dc3b0b77e95895f84e3268 2fd9685dc3a8d467b	ce05b15fa35d768ad27b 522705407c9a	9dc3b0b77e95895f84e3268 2fd9685dc3a8d467b

The fact that the hash values generated by the HashIt application are the same as those of the prototype suggests that the integrity of the original output files that contain traffic exactly as they were captured from the WLAN was preserved. However, if these hash values did not

correspond with each other, it would mean that the data inside the original output files have been compromised; thus, the output files would not qualify to be used as digital evidence.

Having discussed the hashing verification process, the chapter is concluded with a brief summary.

## 7.6 Concluding Remarks

This chapter demonstrated the development of the prototype as proof of concept. The setup environment in which the prototype was developed was also presented.

The researcher explained through demonstration the first three phases of the proposed model, namely Phase 1 (monitoring), Phase 2 (logging), and Phase 3 (preservation). Microsoft Visual Studio was a good choice as a platform for developing the prototype, as coding could be easily done in C# (a programming language with which the researcher was already familiar). The use of Tshark to capture traffic from the WLAN also proved to be a good decision because it provided a command-line interface that enabled the researcher to pass flags to determine the size of the output file, format, location, and when the next output file should be created.

The captured traffic was encoded using both the MD5 and SHA-1 hashing functions and the resulting hash values were stored in the SQL server database. The integrity of the original captured traffic was then proved by generating new MD5 and SHA-1 hash values. The hash values were compared with those of the prototype stored in the SQL server database. The hash values were found to be the same, meaning that the original traffic captured from the network had not been compromised.

The next chapter demonstrates through experiments how to analyse the traffic, should a digital forensic investigation be warranted. The chapter further provides the reporting component.

## Chapter 8                      **Prototype Experiments**

### **8.1 Introduction**

Chapter 7 discussed the prototype by demonstrating how traffic is captured from the wireless network and stored in a digital forensically sound manner.

This chapter is devoted to presenting a demonstration of Phase 4 (analysis) and Phase 5 (reporting) of the Wireless Digital Forensic Readiness Model. The analysis phase is conducted through experiments. The researcher takes the traffic captured from the WLAN (see Chapter 7) and analyses it to uncover any information that might be used as digital evidence. The chapter further provides a brief discussion on how to report the digital evidence from the analysis phase.

Three experiments are presented in this chapter. The first analyses network traffic in an attempt to identify illegal usage of the corporate resources. Experiment one focuses specifically on the downloading of music during office hours. The second experiment also analyses network traffic, but tries to identify a user who discloses the company's trade secrets by means of an email. Hence the emphasis in the second experiment is on the detection of an email message that might contain digital evidence. The third experiment discusses a man-in-the-middle attack scenario where captured wireless network traffic is analysed to determine illegal content accessed by the user of the WLAN. This experiment is independent from the first two experiments in a sense that it does not use the traffic captured in Chapter 7.

The remainder of this chapter is structured as follows: Section 8.2 presents the analysis phase of the proposed model based on the three experiments referred above. Section 8.3 presents the reporting phase. The chapter is subsequently concluded in Section 8.4.

### **8.2 Phase 4 (Analysis) – Prototype Experiments**

Phase 4 presents the three experiments that are discussed in detail in this section. The first experiment attempts to identify the illegal usage of corporate resources. The second experiment attempts to identify a sent email message that contains some of the company's trade secrets. The difference between the two experiments is that the first one involves a binary data analysis where the expected results should be in the form of audio files, while the



second experiment involves a text-based analysis and the expected results are in the form of an email message.

The third experiment provides a discussion on the man-in-the-middle attack using ARP spoofing. The expected results are illegal content in a form of images sniffed from the wireless network.

### **8.2.1 Experiment 1: Identifying Illegal Usage of Corporate Resources**

The following structure is followed in the discussion of this experiment: firstly, the purpose of the experiment is explained, followed by the test scenario, and lastly, the execution of the experiment.

#### **8.2.1.1 Purpose of the Experiment**

The main purpose of this experiment is to detect the illegal use of corporate resources. The experiment focuses on identifying a user who contravenes the company's ICT policy by downloading music during office hours.

#### **8.2.1.2 Test Scenario**

This experiment is conducted because there is a dispute between an employer and an employee. The employee is suspected of downloading music on his mobile device during office hours using the company's WiFi. The company has an ICT policy that prohibits the downloading of music using its resources and assumes that a digital forensic investigation is warranted. The researcher analyses the network traffic captured as explained in Chapter 7 (the data was captured and stored in a digital forensically sound manner) to show that the employee indeed breached the company's ICT policy by downloading music.

#### **8.2.1.3 Execution of the Experiment**

Before discussing the execution of the experiment, the researcher would like to remind the reader that this experiment will be executed using Wireshark and NetWitness Investigator, both of which were introduced in Chapter 6. Figure 8.1 is a duplication of Figure 7.6, because this experiment analyses the same network traffic that was captured in Chapter 7.



The experiment takes a Tshark output file (also called pcap file) depicted in Figure 8.1 and opens it with Wireshark in order to reproduce the raw packets to a more meaningful format. For example, Wireshark presents much information about each packet, such as the source and destination address, source and destination ports, protocol, packet length and message header.

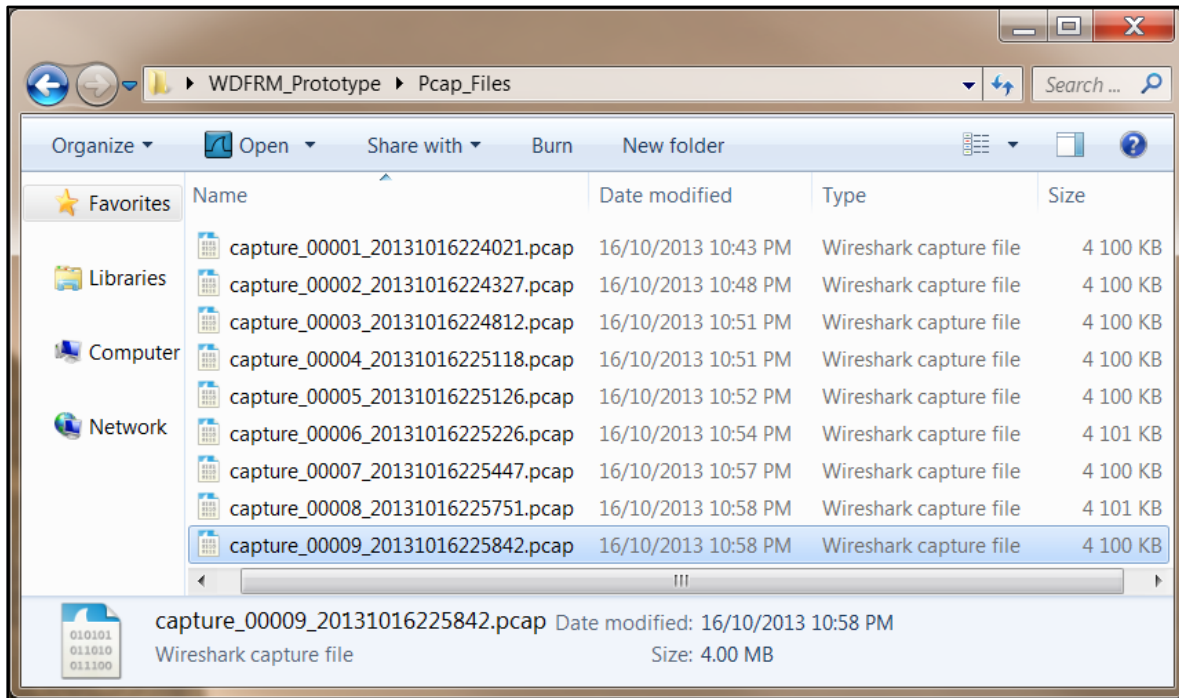


Figure 8.1. Ten output files of Tshark (duplication of Figure 7.6)

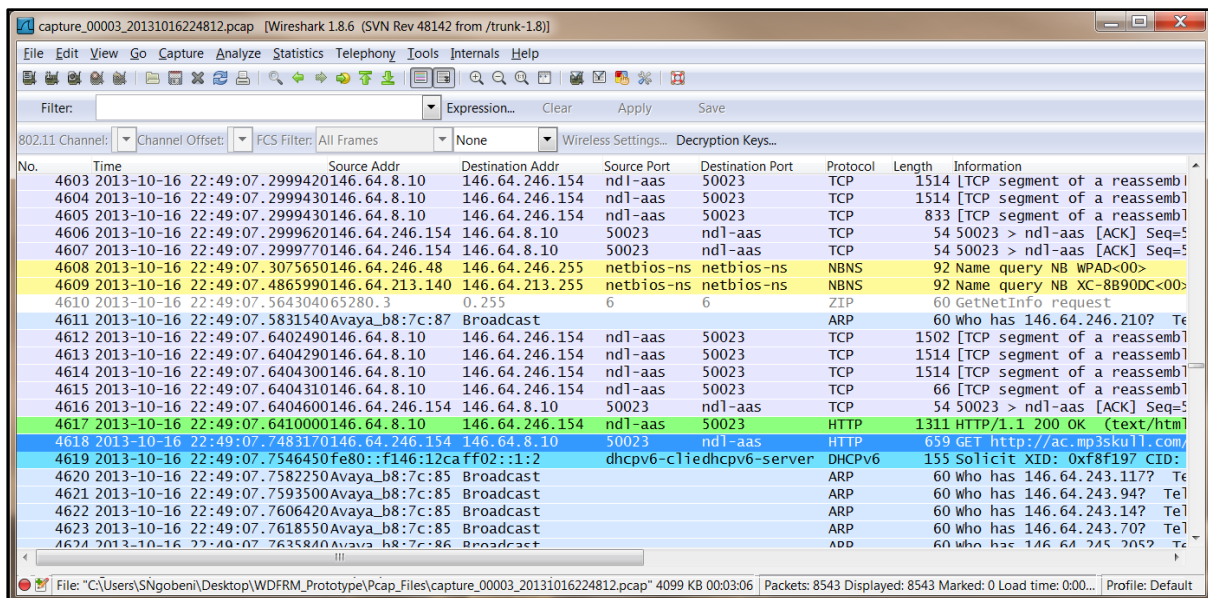


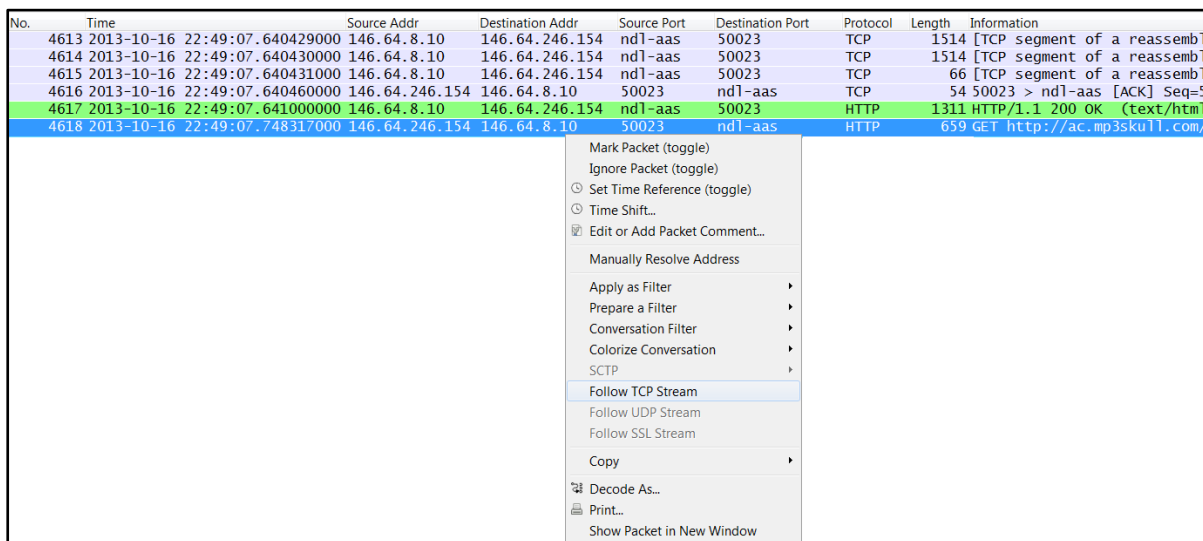
Figure 8.2. Output file replayed in Wireshark





Figure 8.2 depicts output file number 00003 (see Figure 8.1) opened in Wireshark. Each line in Figure 8.2 represents a packet of data as it was captured from the wireless network. The packet number “4618” highlighted in blue reveals the following information: [Date: 2013-10-16], [Time stamp: 22:49:07], [Source Address: 146.64.246.154], [Destination Address: 146.64.8.10], [Source Port: 50023], [Destination Port: ndl-aas], [Protocol: HTTP], [Packet Length: 659] and [TCP Message Header: GET <http://ac.mp3skull.com/autocomplete/add.php?q=lil+wayne+mirror+bruno+mars&rkey=4474bc2537f1fbbd690be0b6fe429ed3> HTTP/1.1].

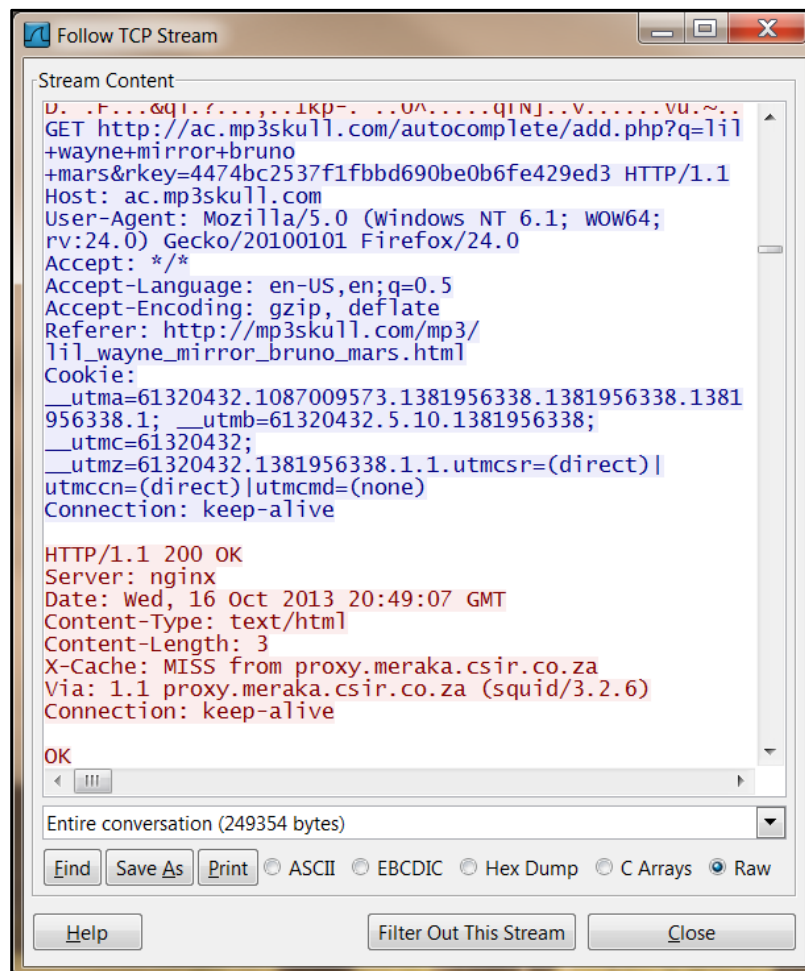
Without spending much effort analysing this packet, it is evident from the blue highlighted packet in Figure 8.2 that there was an “http” communication between two hosts, that is, IP address 146.64.246.154 and 146.64.8.10. By following the TCP stream of this packet, it can be envisaged that more information can be uncovered about this conversation. Figure 8.3 shows how to follow a TCP stream of the blue highlighted packet. This is done by right-clicking on the packet and selecting the option “Follow TCP Stream”.



**Figure 8.3.** Choosing the “Follow TCP Stream” option

After choosing the “Follow TCP Stream” option, Wireshark invokes and displays the “Follow TCP Stream” dialog box that is depicted in Figure 8.4. The red text in Figure 8.4 represents a client’s request to an “nginx server” indicated in the blue text. The client makes an “http GET” request to the nginx server located on the remote host “www.mp3skull.com”. The client uses a Firefox web browser as can be noticed from the user-agent string in the blue text. By observing the first line of the area marked in red in Figure 8.4, the reader can note

that the server sends an “http” acknowledgement with “200 OK”, meaning that it has received the client’s request.



**Figure 8.4.** The “Follow TCP Stream” dialog box

To delve into this packet and obtain more information about it, the researcher opened the “mp3skull.com” website in the browser and found that it was a website for downloading mp3 music. This simply means that a user with IP address 146.64.246.154 contacted a webserver with IP address 146.64.8.10 to download mp3 music. It is even clearer from the TCP message header: `http://ac.mp3skull.com/autocomplete/add.php?q=lil+wayne+mirror+bruno+mars&rkey=4474bc2537f1fbbd690be0b6fe429ed3` of Figure 8.2 that the user requested an mp3 song of “Lil Wayne featuring Bruno Mars, titled: Mirror”.

Despite the entire packet linking the suspected user to the downloaded music, it still remains important to determine the actual mp3 file. The mp3 file is the digital evidence that might increase the chances of this case being admissible in a court of law.

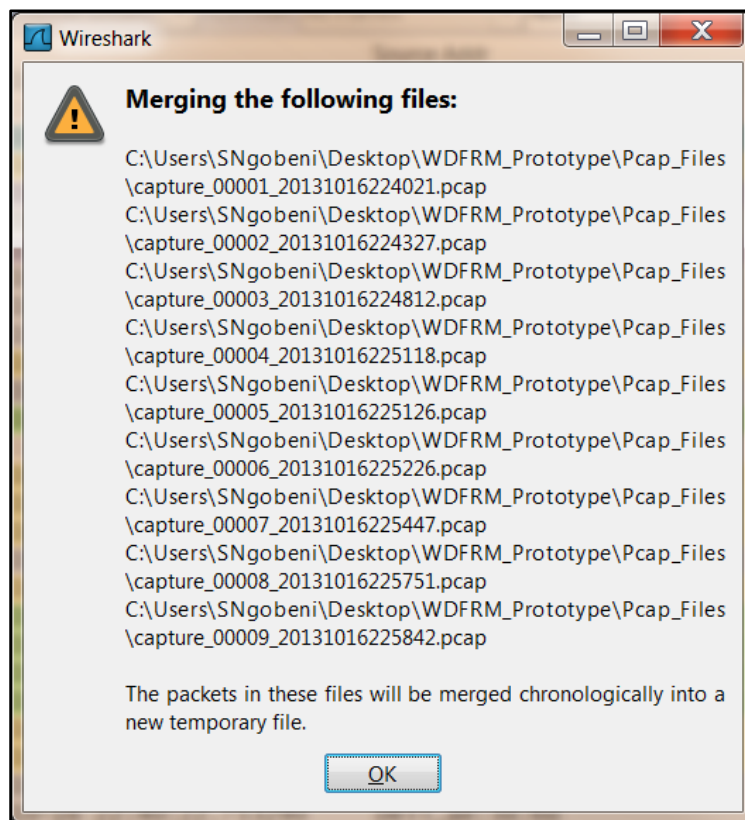




Before exploring the analysis process to determine the mp3 file in question, the reader should note that it remains important to merge the bunch of traffic captured from the network into a single output file. The reason for merging the traffic is that the packets that form a complete session may be fragmented into different output files. Hence, analysing one output file may result in missing digital evidence spread across multiple pcap files.

Next, the researcher merges the bunch of traffic captured from the network (see Figure 8.1) and preserves its integrity before the analysis process begins.

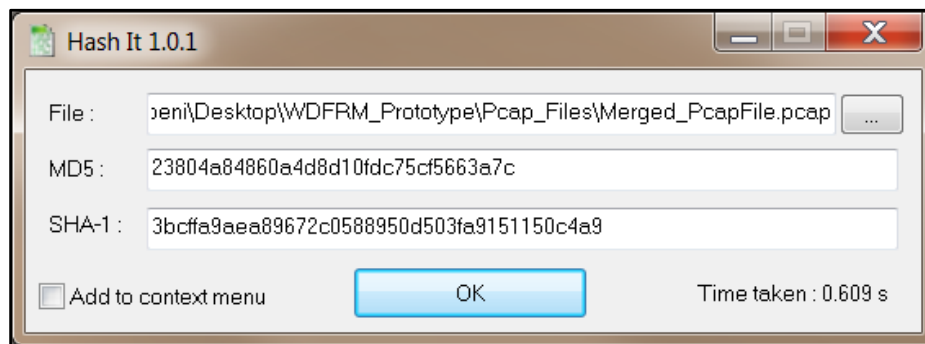
Figure 8.5 shows a dialog box that is displayed after dumping all the pcap files from Figure 8.1 into Wireshark. The dialog box also shows the directory where the original pcap files were stored. The reader should note that these directories are exactly the same as those of the original data captured from the network in Figure 8.1.



**Figure 8.5.** Merging pcap files with Wireshark

It is of paramount importance to preserve the integrity of the merged pcap files so that if the reliability of this data were to be questioned later, it can be shown that it was not tampered with. The researcher achieves this by simply invoking the same hashing techniques that were

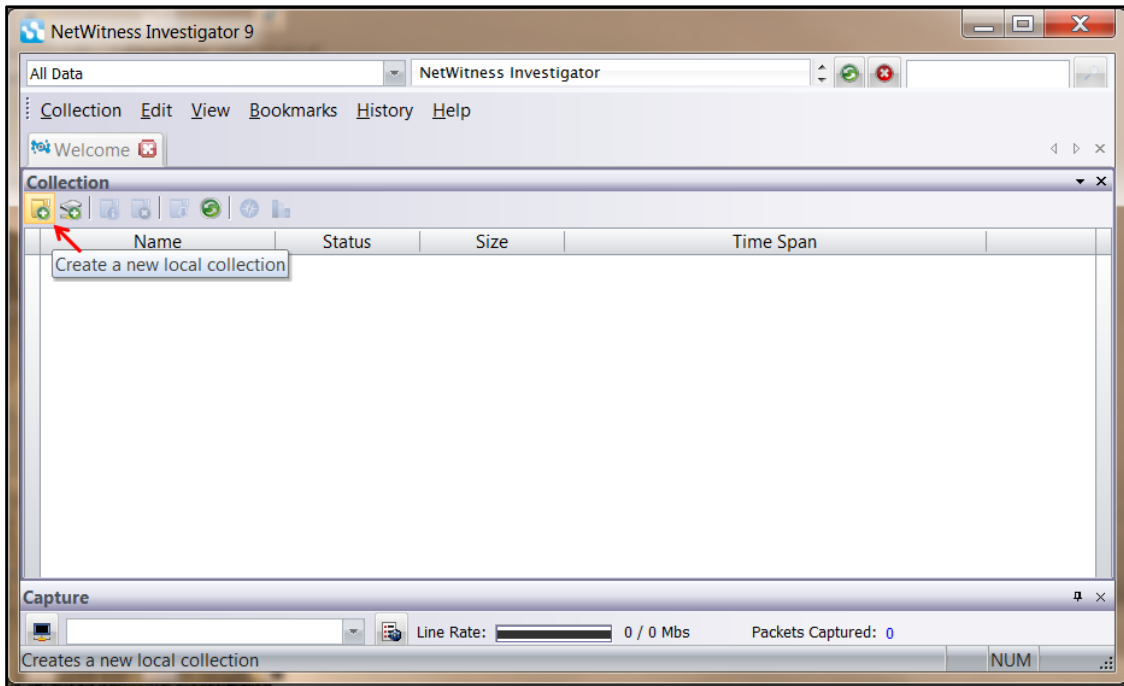
discussed in Chapter 7 – MD5 and SHA-1 – to hash the merged pcap file. Figure 8.6 depicts the resulting MD5 and SHA-1 hash values of the merged pcap file.



**Figure 8.6.** MD5 and SHA-1 hash values of the merged pcap file

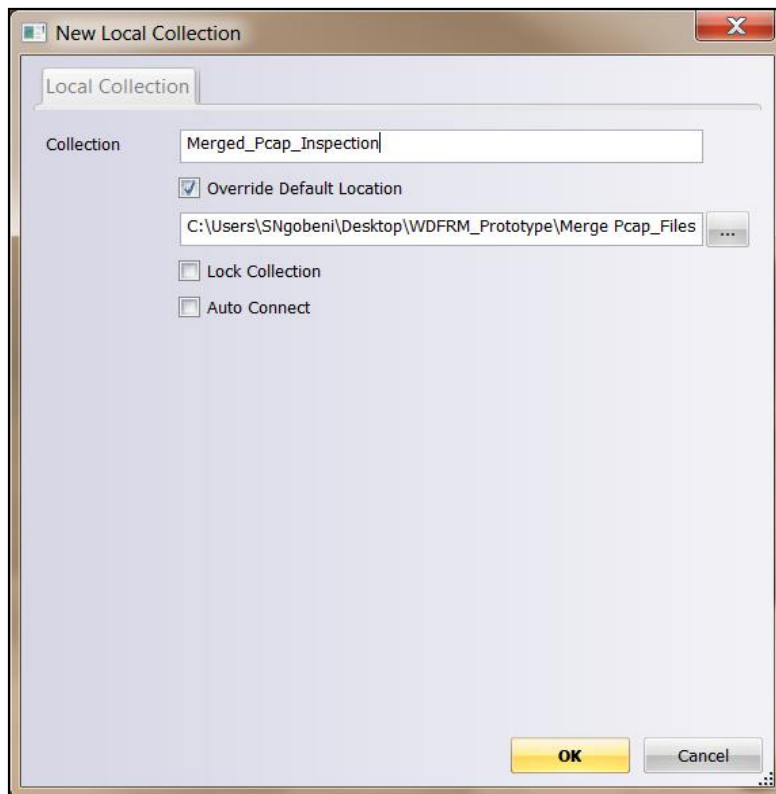
Next, the researcher uses the NetWitness Investigator to harvest the actual digital evidence in question, which in this case is the mp3 file.

The merged pcap file is then loaded in the NetWitness Investigator to start the traffic inspection process. The researcher creates a local collection to store the data extracted from the merged pcap file. When the user clicks on the icon indicated with the red arrow in Figure 8.7, NetWitness Investigator invokes the dialog box indicated in Figure 8.8 to allow the user to specify the directory for creating a local collection. For the purposes of this dissertation, a local collection is a directory into which the content of the merged pcap file is extracted.

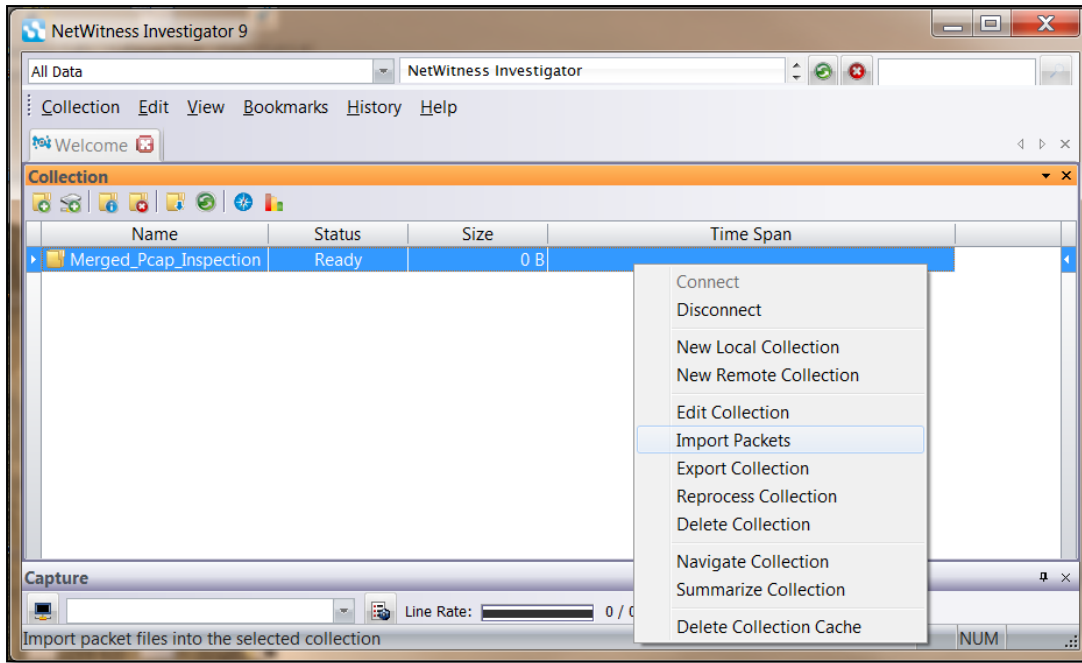


**Figure 8.7.** Creating a new local collection in NetWitness Investigator

Now that the local collection has been created, the next step is to import the merged pcap file into the created local collection.

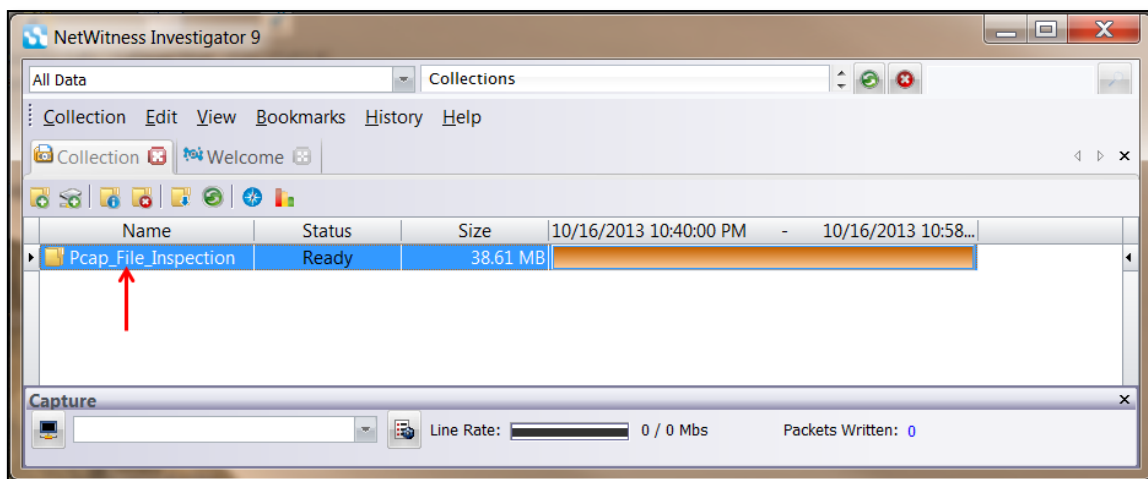


**Figure 8.8.** Specifying a directory for a local collection



**Figure 8.9.** Importing the merged pcap file

Figure 8.9 depicts the process of importing the merged pcap file. When the importing process has completed, the researcher double clicks on the folder icon of the “Merged\_Pcap\_Inspection” (indicated with the red arrow in Figure 8.10) to see a more detailed view of all the packets in the merged pcap file.



**Figure 8.10.** Viewing packets in the merged pcap file

Figure 8.11 gives a detailed view of all the packets in the merged pcap file.

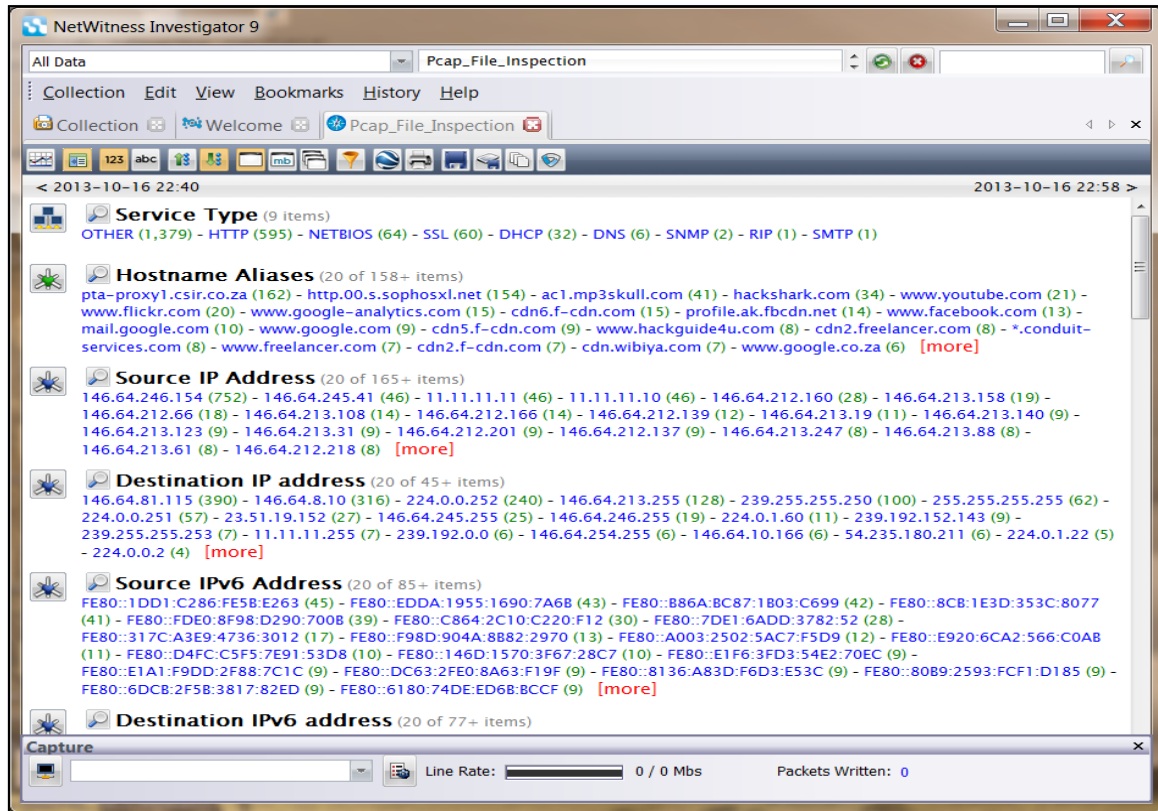


Figure 8.11. Detailed view of the packets in the merged pcap file

The next step is the extraction of the mp3 files in question, which should constitute the actual digital evidence. The researcher achieves this by extracting all information from common protocols as indicated by the red arrow in Figure 8.12.

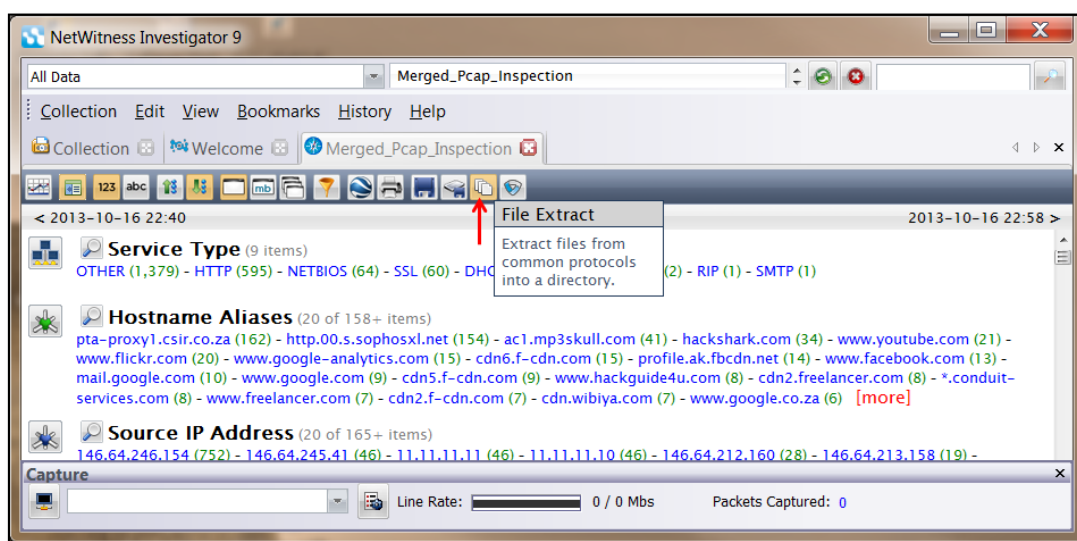


Figure 8.12. Extraction of files from common protocols into a directory



After performing this operation, NetWitness Investigator display a dialog box as given in Figure 8.13, which allows the user to select the type of files to be extracted from the merged pcap file. The reader should note that different categories of content can be extracted (see Figure 8.13) as is clear from the file types with their corresponding file extensions. However, for the purpose of this experiment, the researcher is only interested in the mp3 content, which is the audio files in this file. Furthermore, the researcher specifies the directory in which the mp3 content should be stored after extraction.

To extract only the audio files from the list of the different file extensions, the researcher selects the audio dialog box as shown in Figure 8.13. The process of extracting the audio files begins immediately after clicking the “OK” button in Figure 8.13, and the resulting mp3 audio files are extracted and stored in the specified folder as is shown in Figure 8.14.

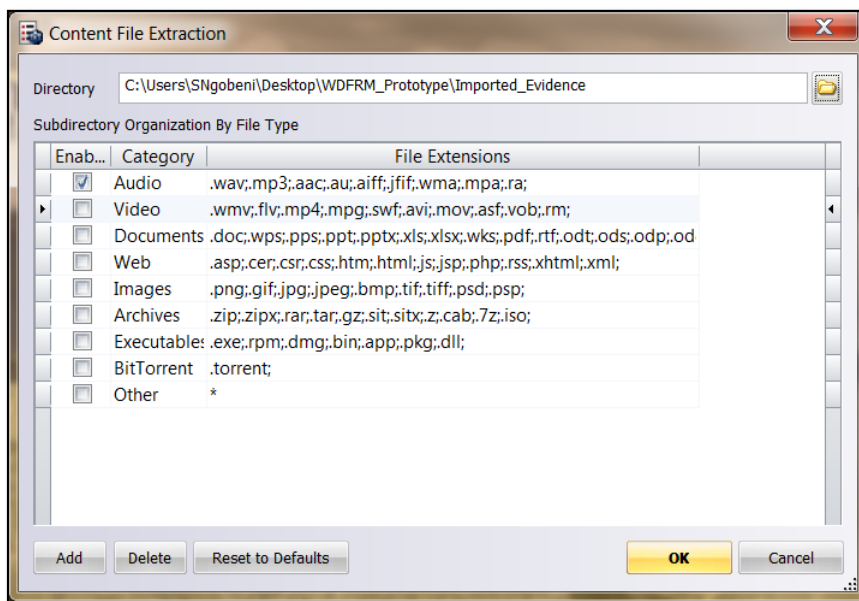
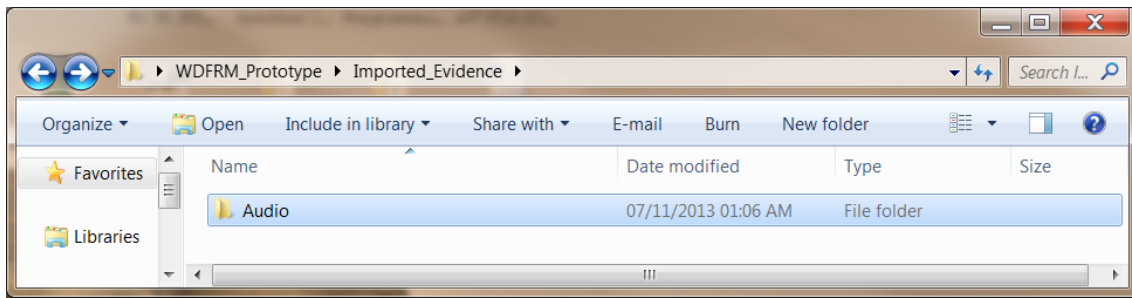


Figure 8.13. Specifying the type of files to be extracted from the merged pcap file

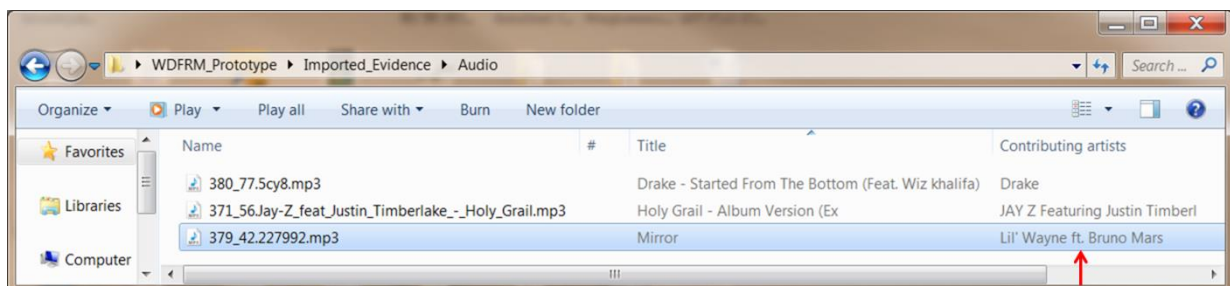


**Figure 8.14.** Files extracted from the merged pcap file

Figure 8.15 depicts the mp3 audio files that were found inside the audio folder in Figure 8.14.

After extracting the actual audio files, it remains important to link the individual suspected of misusing the company’s resources to the identified digital evidence. When reverting back to Figure 8.2 and Figure 8.4, it is clear that a machine with an IP address: 146.64.246.154 contacted a webserver with IP address: 146.64.8.10 to download mp3 audio music.

One of the songs that were downloaded was “Mirror”, by “Lil Wayne ft. Bruno Mars”. It is evident from Figure 8.15 that the machine with IP address 146.64.246.154 indeed downloaded the mp3 audio file in question. This is also true in the sense that this information was extracted from the same bunch of traffic that was captured from the network as discussed in Chapter 7.



**Figure 8.15.** Digital evidence – mp3 audio files

In summary, the reader can learn from this experiment that it is simply used to demonstrate a step-by-step process on how to attribute the illegal usage of corporate resources to the suspected employee through the use of various tools as introduced in Chapter 6 of this dissertation. Should a need arise for a digital forensic investigation to be launched; the employer could therefore use this data as digital evidence to show that the employee indeed infringed the company’s ICT policy on internet usage. Similarly, any other digital evidence of potential investigative value can be extracted in this way.





Having used Wireshark and NetWitness Investigator to analyse the traffic captured from the wireless network to identify an event that violates the company's ICT policy, the next experiment attempts to intercept an email message containing a company's trade secrets.

### **8.2.2 Experiment 2: Identification of Email Containing Company Trade Secrets**

Experiment 2 is conducted following the similar structure of Experiment 1, that is, firstly the purpose of the experiment, secondly the test scenario, thirdly the experiment setup (not part of experiment 1) and lastly the execution of the experiment (see Section 8.2.1).

#### **8.2.1.1 Purpose of the Experiment**

The main purpose of this experiment is to identify a user who has transmitted the company's trade secrets to a third party using the company's Wi-Fi. This experiment is aimed at analysing the transmitted Simple Mail Transfer Protocol (SMTP) traffic to identify the email message that could contain the necessary digital evidence that links the employee to the suspected event.

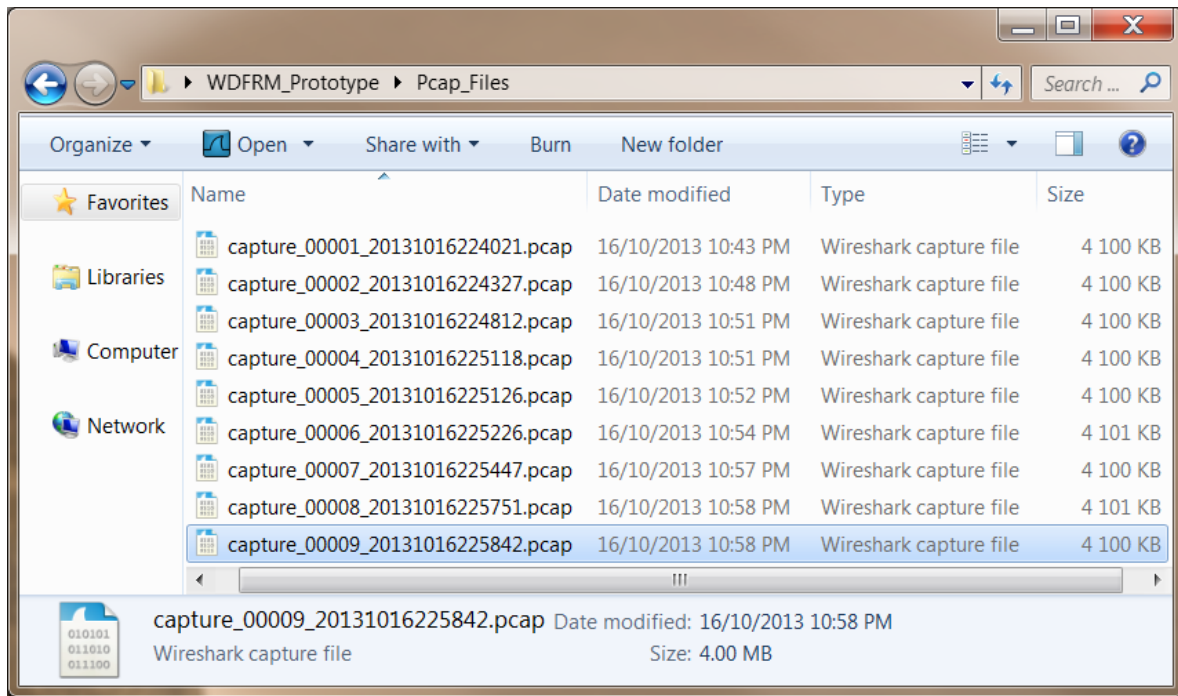
#### **8.2.1.2 Test Scenario**

As was the case with Experiment 1, Experiment 2 is also conducted because there is a dispute between the employer and employee. The employee is suspected of transmitting the company's trade secrets by email to a third party using the company's Wi-Fi. The company has an email policy that governs employees' use of its email system and that prohibits the disclosure of trade secrets to a third party or competitor. The employee denies having transmitted the company's trade secrets to a third party on the company's email system. The experiment analyses the network traffic captured as explained in Chapter 7 to show that the employee has indeed breached the company's email policy.

#### **8.2.1.3 Experiment Setup**

The researcher would like to state upfront that the setup of this experiment was conducted in conjunction with the prototype development presented in Chapter 7. This suggests that Experiment 2 will analyse the bunch of network traffic captured in Chapter 7, Figure 7.6. Figure 8.16 is a repetition of Figure 7.6, and it is again inserted here for the reader's convenience.

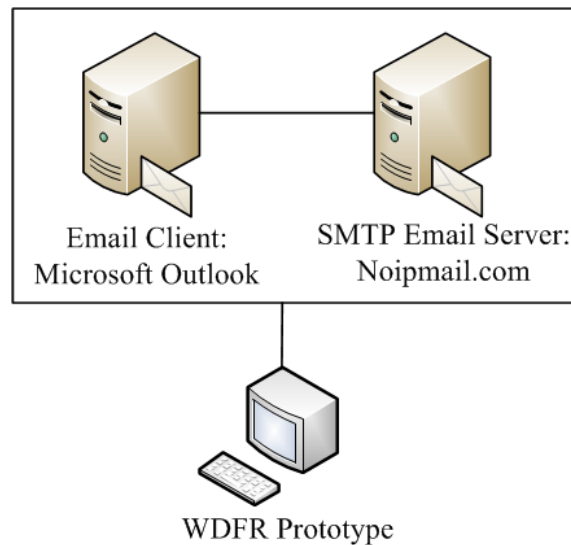




**Figure 8.16.** Ten output files of Tshark (duplication of Figure 7.6)

The reader should note that at this stage of the digital forensic investigation process the data has already been captured and stored in a digital forensically sound manner. However, the researcher would like to draw the reader's attention to the way in which the data is captured for this particular experiment. This will enable the reader to understand how the applications used to set up the experiment fit together before delving into the analysis part of the experiment.

The experiment setup consists of the email client, SMTP email server and the WDFR prototype. Note that the researcher does not provide a detailed discussion of the applications used in the experiment setup, but rather highlights them with a view to determining how they fit together. Below is a description of how they address the purpose of this experiment.



**Figure 8.17.** Setup and configuration of Experiment 2

**Email Client: Microsoft Outlook.** This is the email client that the experiment uses to send an email from. It is configured to read an email account that is created from the email server. The reader should note that there is no specific reason for choosing MS Outlook – other email clients like Thunderbird, Zimbra, etc. would also have sufficed for this experiment.

**SMTP Email Server: Noipmail.com.** This free anonymous Simple Mail Transfer Protocol email server is used in the experiment to deliver the email sent from the email client to the intended recipient. The name of this SMTP email server is noipmail.com and the name of the account that the researcher created is sjn03ngobeni@noipmail.com. The noipmail server was selected specifically because it disables TLS/SSL security (in contrast to other email servers like gmail and yahoo). The reader should note that the server is used only for experimental purposes and that any email server should implement TLS/SSL security in a real network environment.

**WDFR Prototype.** After setting up the email client and the email server, the researcher uses the WDFR prototype to intercept the SMTP traffic transmitted between the two email systems. The primary goal of the WDFR prototype is to capture and store the network traffic in a digital forensically sound manner. The exact details of how the WDFR prototype works are unpacked in Chapter 7.

Having introduced the reader to the experimental setup, Chapter 8 will now continue to explain how the entire experiment is executed.



#### 8.2.1.4 Execution of the Experiment

Before analysing the network traffic, the researcher would like to state upfront that the traffic for this experiment was not encrypted. If the WDFR prototype were to be placed in an environment where the network traffic was encrypted, the prototype would still capture the traffic and forensically store the data; however, encryption is still seen as the biggest enemy of forensic scientists (Casey et al., 2011).

The researcher would also like to remind the reader that this experiment uses Wireshark to merge and preserve the traffic captured from the network. (The details of how Wireshark works were introduced in Chapter 6).

Firstly, the network traffic captured from the network is merged using Wireshark. The details of why and how to merge the network traffic were explained in Experiment 1, and the same mechanism is used here. To preserve the integrity of the merged pcap file, the hashing techniques that were used in Experiment 1 are also used in this experiment. Figure 8.18 is a dump of the packets in Figure 8.16 to be merged with Wireshark.

After merging and preserving the integrity of the captured traffic, the researcher analyses the merged traffic with the intention to identify the suspected email message that may contain the company's trade secrets.

Since Figure 8.18 is just a bunch of traffic captured from the network, the traffic that forms a complete session might be fragmented into different packets. To address this issue, the researcher filters the traffic by specifically looking for any traffic that was intended to the SMTP "noipmail.com" email server. The noipmail.com email server is then queried (ping) to resolve the URL to an IP address that can easily be used to filter the specific email server's traffic on Wireshark. The same URL can also be resolved to an IP address by using the "nslookup" command.

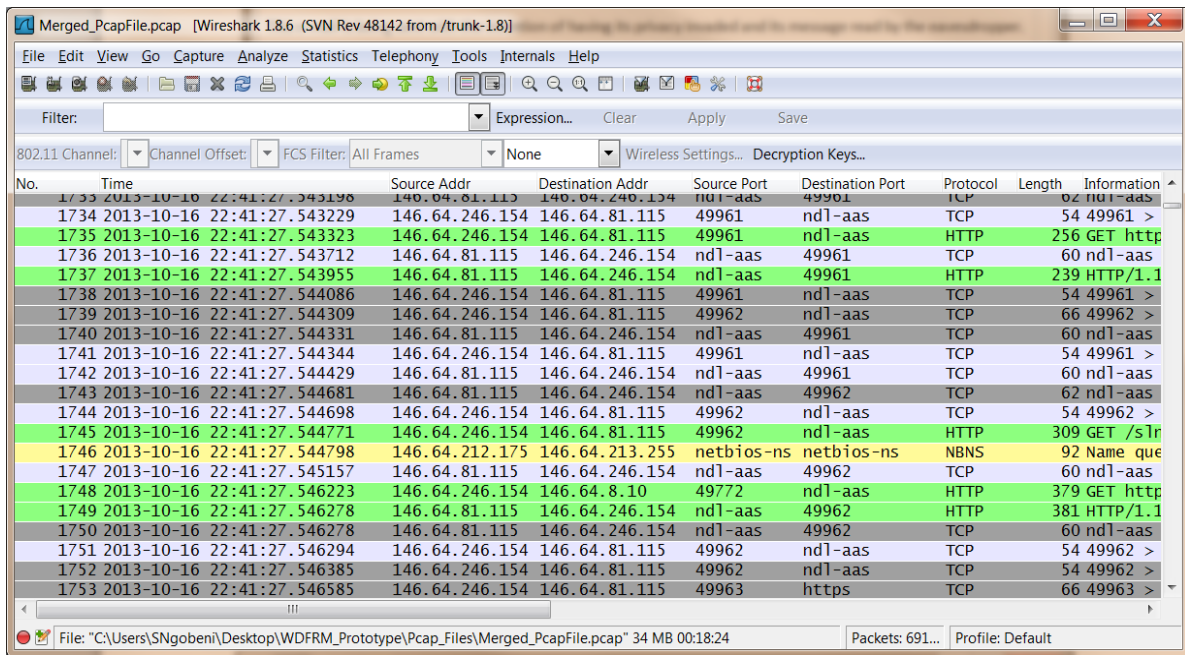


Figure 8.18. Merged pcap files of Figure 8.16

The noipmail.com email server was queried and resolved to “IP address: 192.117.115.28” as depicted in Figure 8.19. The traffic in Wireshark was then filtered with the IP address of the resolved email server.

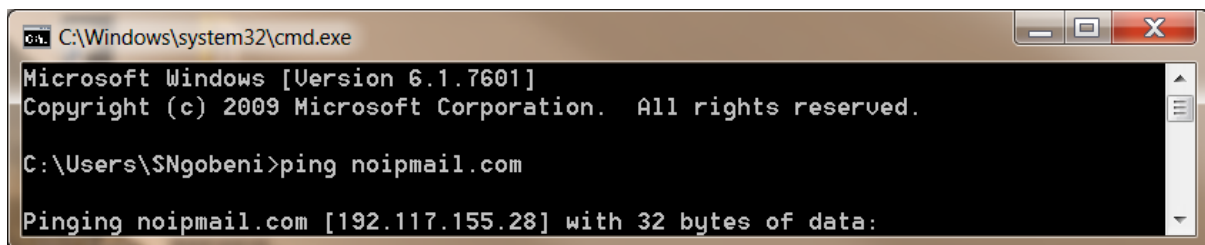


Figure 8.19. Resolving the noipmail.com email server to an IP address

Figure 8.20 depicts the resulting packets after filtering the traffic with the command “ip.addr == 192.117.155.28”. On taking a closer look at Figure 8.20, the reader can note from the “Protocol” field that it now shows SMTP traffic, following the issuing of the traffic-filtering command. The reader should remember that Experiment 2 is intended to examine the SMTP traffic that is believed to contain the suspected email event.

Having resolved the email server to an IP address and filtered the respective traffic accordingly, the next step is to follow the TCP stream of each packet in Figure 8.20 to identify and analyse the packet containing the suspected email event.

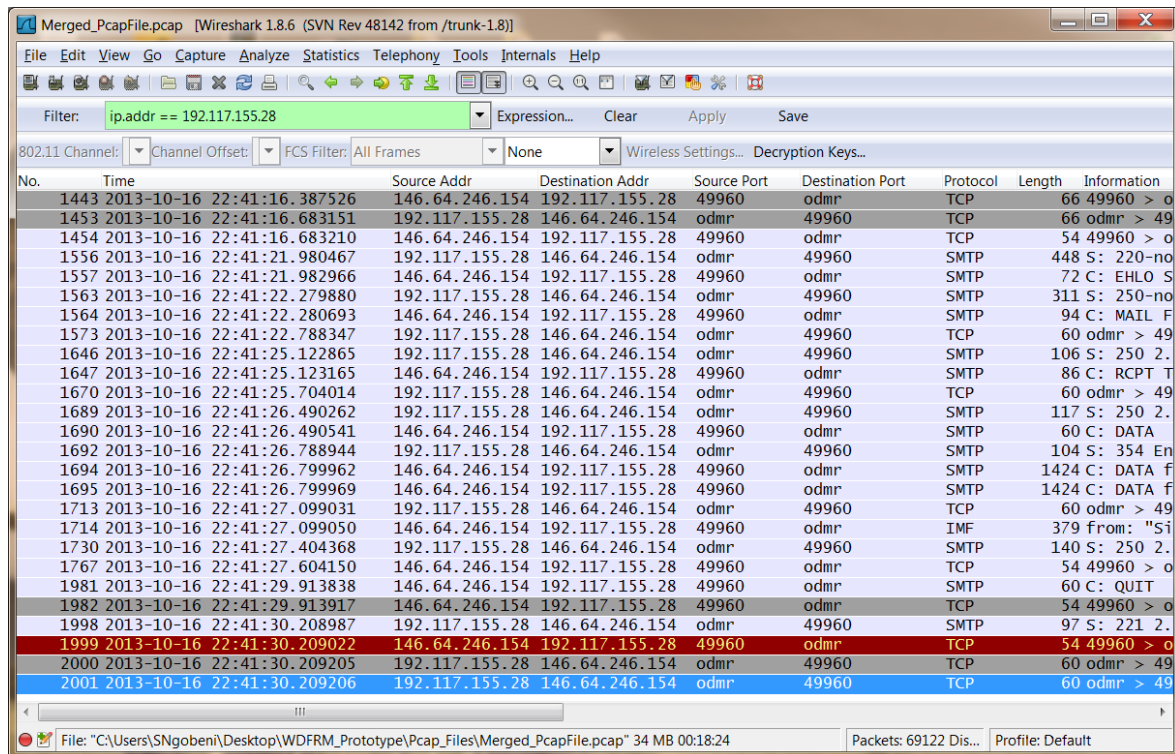
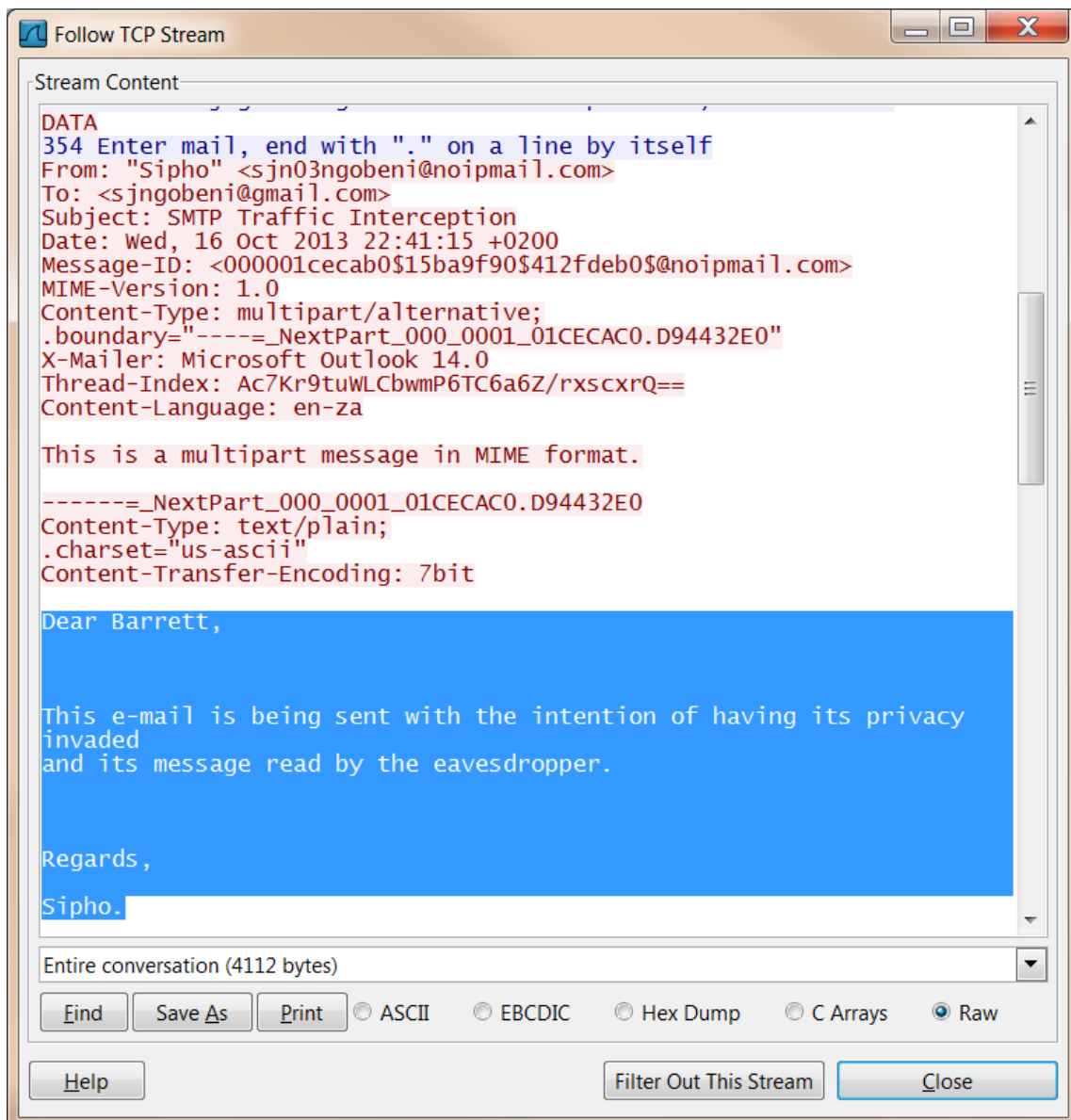


Figure 8.20. Filtered SMTP traffic

Packet number 2001, which is highlighted in blue in Figure 8.20, was selected and its TCP stream was followed. The same approach used in Figure 8.3 (Experiment 1) to follow a TCP stream in Wireshark is also used here. Figure 8.21 presents the dialog box displayed after following the TCP stream of packet number “2001” with all the data from the TCP stream displayed in order.

In general, email headers are known to provide additional information about the received message. The program that crafted the email usually provides information such as date and time, as well as in-depth properties such as the x-mailer and MIME-Version. The property Return Path is also provided in an event where the sent email cannot be delivered. Without making a tremendous effort to analyse the chosen packet number “2001” in Figure 8.20, the following packet header information about the transmitted email can be observed from Figure 8.21:



**Figure 8.21.** Following TCP stream of packet number 2001

Figure 8.21.**From:** “Sipho” <[sjn03ngobeni@noipmail.com](mailto:sjn03ngobeni@noipmail.com)>– The “From” email header property provides the email account from which the crafted suspected email was sent. The email is seen to be crafted from the email account [sjn03ngobeni@noipmail.com](mailto:sjn03ngobeni@noipmail.com). It is also evident from the “Source Address” field of packet number 2001 in Figure 8.20 that the sender’s IP address is 192.117.155.28.

- **To:** <[sjngobeni@gmail.com](mailto:sjngobeni@gmail.com)> – The email header “To” identifies the recipient to whom the suspected sent email is directed, namely [sjngobeni@gmail.com](mailto:sjngobeni@gmail.com). It is also evident from the “Destination Address” field of Figure 8.20 that the recipient’s IP address is “146.64.246.154”.





- **Subject:** SMTP Traffic Interception – The “Subject” email header property indicates the heading or subject of the suspicious sent email. In this case, the subject of the email is found to be “SMTP Traffic Interception”.
- **Date:** Wed, 16 Oct 2013 22:41:15 +0200. The “Date” property indicates the date and time at which the crafted email was sent. The packet reveals that the email was sent on Wednesday, 16 October 2013 at 22:41:15.
- **MIME-Version:** 1.0 – MIME stands for Multipurpose Internet Mail Extension. This email header field is an internet standard that was designed to extend the format of the email to support non-ASCII characters, attachments and other formats needed when writing an email. It can be observed from this field that the MIME-Version used is 1.0. Other fields represented by MIME are the Content-Type, Content-Transfer-Encoding, and Content Language.
- **X-Mailer:** Microsoft Outlook 14.0. This email header field provides information about the software that sends the suspected email. In this case, the email was found to be sent from a “Microsoft Outlook” version 14.0.

More interestingly, it can also be observed from Figure 8.21 that the blue highlighted text is the actual content that was transmitted in the email. Having collected all these pieces of information about the suspected email, the following facts can be concluded about this experiment:

- A user has sent an email from a Microsoft Outlook email client. The sender’s email address is [sjn03ngobeni@noipmail.com](mailto:sjn03ngobeni@noipmail.com). This suggests that the sender has an email account with the Noipmail email server as was mentioned earlier in this chapter. It was also found that the sender’s IP address is 192.117.155.28.
- The email was sent on Wednesday, 16 October 2013 at 22:41:15.
- The subject of the email is “SMTP Traffic Interception”.
- The email was sent to a destination email address [sjngobeni@gmail.com](mailto:sjngobeni@gmail.com). The destination IP address is 192.117.155.28.
- The actual content of the email reads as follows:



“Dear Barret,

This e-mail is being sent with the intention of having its privacy invaded and its message read by the eavesdropper.

Regards,

Sipho.”

An interesting observation is the fact that the email was successfully delivered to the recipient since Figure 8.21 shows that there is no indication of the “Return Path” field of the email header, which would indicate if the email was undelivered. It is therefore confirmed that a user sent an email containing a company trade secret to a third party, and this captured information can be used as digital evidence in a court of law. As was the case in Experiment 1, any other digital evidence of potential investigative value can be extracted in this way.

The two experiments discussed above show how the data captured from the network can be analysed without tremendous effort by using tools such as Wireshark and NetWitness Investigator. Both experiments could link the suspected individuals to the crime that was committed.

The next section presents the third experiment, that is, man-in-the-middle attack.

### **8.2.3 Experiment 3: Man-in-the-Middle Attack**

Experiment 3 is conducted following the similar structure of Experiment 2, that is, firstly the purpose of the experiment, secondly the test scenario, thirdly the experiment setup and lastly the execution of the experiment (see Section 8.2.2).

#### **8.2.3.1 Purpose of the Experiment**

The main purpose of this experiment is to demonstrate the concept of man-in-the middle attack. This experiment is aimed at capturing data from a suspected user who happens to connect to the WLAN and browse illegal content. The experiment shows the illegal content accessed by the suspected user can be harvested and may be used for digital forensic investigation.





### 8.2.3.2 Test Scenario

This experiment aims to test the scenario where the company's Wi-Fi has suspected that a specific IP address is accessing illegal content which has detrimental effects on the network bandwidth. The owner of the WiFi then setup a man-in-the-middle attack to harvest information accessed by the suspected IP address in order to see the actual content accessed by the suspected IP address. The reader should note that the suspected IP address is viewed as the legitimate user in this case as indicated in Figure 8.22. An assumption is made that the owner of the WiFi has obtained prior consent in writing to monitor activities on the WLAN.

### 8.2.3.3 Experiment Setup

This section is devoted to provide the reader with the tools used to setup this experiment. This will enable the reader to understand how the tools and applications used to set up the experiment fit together to address the above scenario before delving on the execution of the experiment itself.

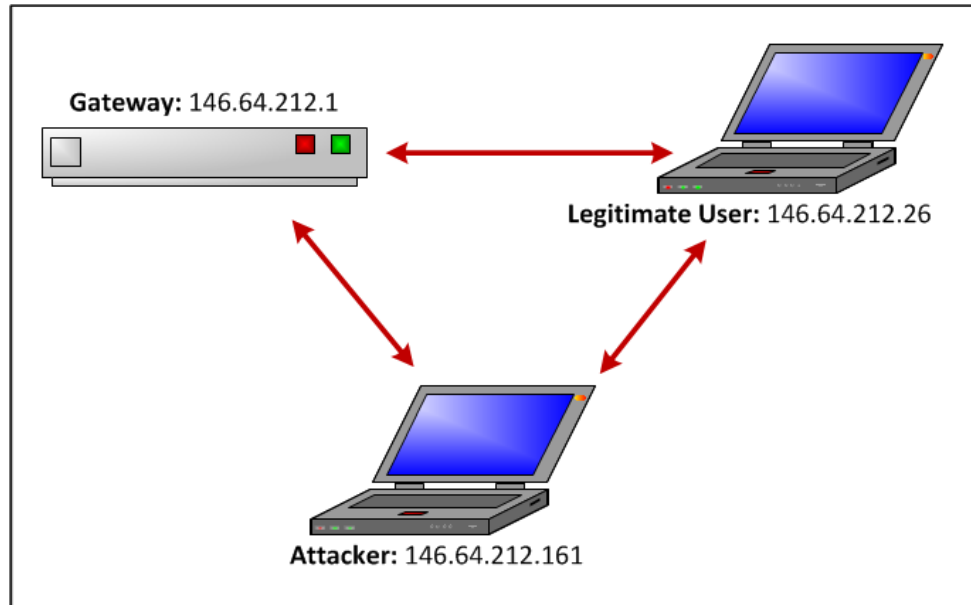
The experiment setup consists of three entities, that is, D-Link 3G WiFi Router (Gateway), Kali Linux Machine (Attacker), and a mobile device (legitimate user). Note that the researcher does not provide a detailed discussion of the applications used in the experiment setup, but merely provide highlights of the tools with a view to demonstrate how they fit together to address the test scenario. Below is a description of the tools.

**D-Link 3G WiFi Router (Gateway)** – The 3G D-Link WiFi is an 802.11b/g router which provides internet connectivity. Any wireless device within transmission range of the router will be able to connect and enjoy free internet connectivity. The router is used as a Gateway for this experiment, with an IP address of 146.64.212.1.

**Kali Linux Machine (Attacker)** – The attacker was setup on a Dell Latitude E5550 machine. Kali Linux was installed as a bootable USB to the Dell machine. Linux Kali is a free Debian-based distribution widely used for penetration testing. It consist of more than 600 tools aimed at penetration testing. The IP address of the attacker is 146.64.212.161.

**Mobile Device (legitimate user)** – This is a normal user who happens to connect to the WiFi network. This user was setup on a Dell Latitude E6530 machine with IP address 146.64.212.26. For the purpose of this experiment, this mobile device is treated as the suspected

user on the WiFi who happens to browse illegal content. The reader should note that all the three actors in this experiment, that is, the router, attacker and legitimate user are all in the same network address, that is, 146.64 with the remaining two numbers indicating the address of each host in the network.



**Figure 8.22.** Man-in-the-middle attack experiment setup

#### 8.2.3.4 Execution of the Experiment

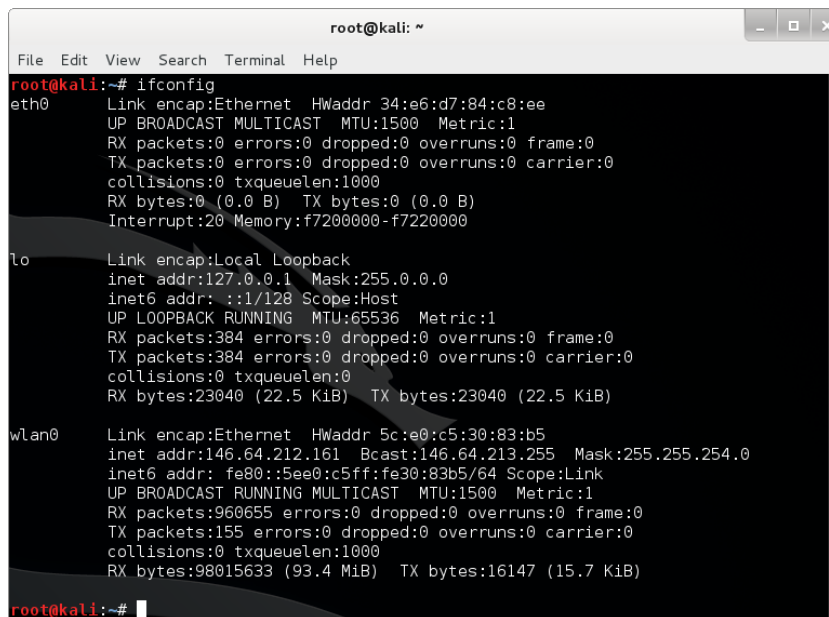
Similar to experiment 2, the researcher would like to state upfront that the traffic for this experiment was not encrypted too. The D-Link router was configured to be open, meaning no encryption keys such as WEP, WPA2, and WPS were configured. Despite this, the experiment would still be conducted successfully even if encryption was setup, though it would take a considerable significant amount of effort to crack the passwords first, however it should be noted that encryption is still seen as the biggest enemy for forensic Scientists (Casey et al., 2011).

The salient idea of this experiment is that, the attacker uses ARP spoofing mechanism to convince the legitimate user that it is the gateway. Upon reply of the legitimate user, the attacker then immediately convinces the gateway that it is the legitimate user. Both the legitimate user and the gateway would think that they have established connection with each other while they have both established connection with the attacker. Now this means that both the gateway and the legitimate user's traffic are routed to the attacker who can then intercept the communications between the two parties. For the purpose of this experiment, the

attacker is only interested in the traffic of the legitimate user whom is suspected to be browsing illegal content on the network. The experiment is executed following a sequence of steps, the steps are presented below:

### Step 1: Determine the IP address of the attacking machine.

The first step is to determine the IP address of the attacking machine. This is the IP address of the Kali Linux machine. Figure 8.23 depict the command that was issued to check the IP address of the attacker.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 34:e6:d7:84:c8:ee  
          UP BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
          Interrupt:20 Memory:f7200000-f7220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:384 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:384 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23040 (22.5 KiB)  TX bytes:23040 (22.5 KiB)  
  
wlan0     Link encap:Ethernet  HWaddr 5c:e0:c5:30:83:b5  
          inet addr:146.64.212.146  Bcast:146.64.213.255  Mask:255.255.254.0  
          inet6 addr: fe80::5ee0:c5ff:fe30:83b5/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:960655 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:98015633 (93.4 MiB)  TX bytes:16147 (15.7 KiB)  
root@kali:~#
```

Figure 8.23. Determining the IP address of the Kali Linux machine – attacker

The reader can note that that the IP address of the attacking machine is 146.64.212.146 which is configured on the wlan0 network interface. The next step is to check the address of the gateway.

### Step 2: Determine the gateway.

The second step of the experiment is to determine the address of the gateway. This is what gives access to the internet to all the devices connected to the D-Link router. Figure 8.24 presents the route command which is used to achieve this.

```
root@kali:~# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        146.64.212.1   0.0.0.0        UG    0     0     0 wlan0
146.64.212.0   *              255.255.254.0  U     0     0     0 wlan0
```

**Figure 8.24.** Determining the address of the gateway

After issuing the “route” command on the terminal, the gateway is displayed on the screen. The gateway is 146.64.212.1. Having determined the address of the gateway, the next step is to determine the IP address of the legitimate user.

### Step 3: Determine the IP address of the legitimate user.

The third step is to determine the IP address of the legitimate user. This can be achieved by issuing the “ipconfig” command on the terminal of the legitimate user’s mobile device, in this case is the Dell Latitude E6530. Figure 8.25 shows the IP address of the legitimate user.

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : csir.co.za
Link-local IPv6 Address . . . . . : fe80::31b2:3e6:5749:334f%11
IPv4 Address. . . . . : 146.64.212.26
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 146.64.212.1
```

**Figure 8.25.** Determining the IP address of the legitimate user

The reader can note that the IP address of the legitimate user is 146.64.212.26.

### Step 4. Test connection between legitimate user and the attacker.

This step is devoted to testing the connection between the attacker and the legitimate user. The “ping” command was issued from the terminal of the attacker’s machine. Figure 8.26 depicts the results of the ping command.

```
root@kali:~# ping 146.64.212.26
PING 146.64.212.26 (146.64.212.26) 56(84) bytes of data:
64 bytes from 146.64.212.26: icmp_req=1 ttl=128 time=2.25 ms
64 bytes from 146.64.212.26: icmp_req=2 ttl=128 time=2.71 ms
64 bytes from 146.64.212.26: icmp_req=3 ttl=128 time=3.01 ms
64 bytes from 146.64.212.26: icmp_req=4 ttl=128 time=2.71 ms
64 bytes from 146.64.212.26: icmp_req=5 ttl=128 time=4.32 ms
^Z
[2]+  Stopped                  ping 146.64.212.26
```

**Figure 8.26.** Pinging the legitimate user

The ICMP messages in Figure 8.26 show that the connection is established between the attacker and the legitimate user. The same command can be issued to test the connection between the attacker and the gateway. Having determined the connectivity between the



attacker and the legitimate user, the next step is to test if packet forwarding is established in the attacker's machine.

**Step 5. Test IP forwarding from the attackers' machine.**

By default many modern Linux Distribution will have IP forwarding disabled as depicted in Figure 8.27. The value in /proc system was checked whether it is currently set to "0" or "1". "0" means the IP forwarding is disabled and "1" means enabled. The initial test showed that the value in /proc system was set to "0" and it was then enabled by issuing the "echo 1" command.

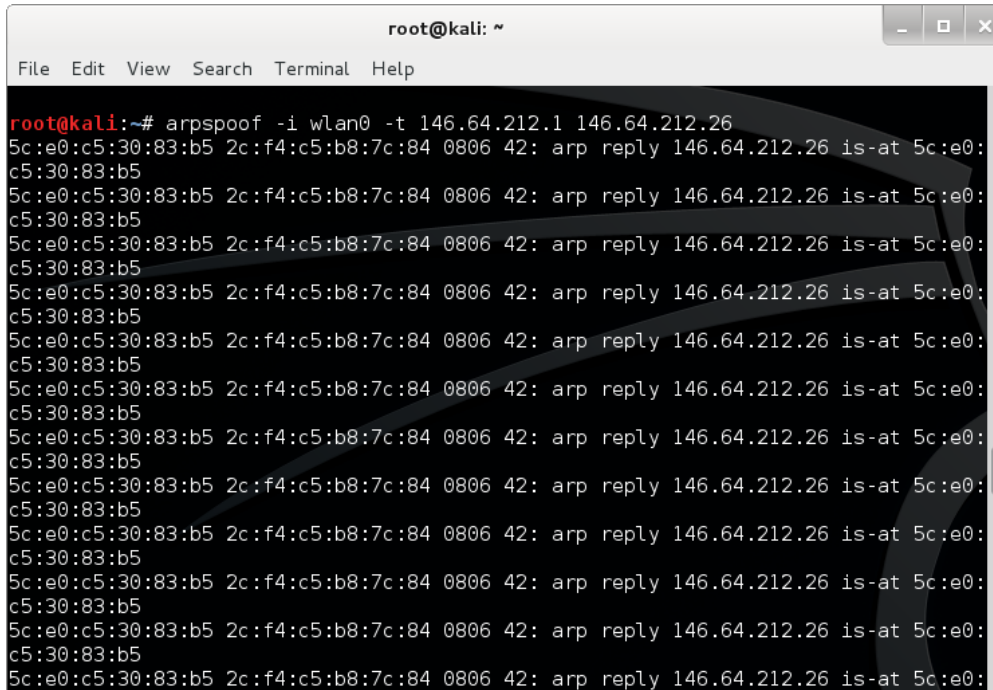
```
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
0
root@kali:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

**Figure 8.27.** Determine IP forwarding

In the next step, the attacker convinces the gateway that it is the legitimate user.

**Step 6. The attacker convinces the gateway that it is the legitimate user.**

The command "arp spoof" was issued from the attackers' machine where the attacker convinces the gateway that it is the legitimate user. The gateway sends "arp reply" messages indicating that a connection was established between the gateway and the attacker. Having established connection between the gateway and the attacker, the next step is for the attacker to convince the legitimate user that the attacker is the gateway.

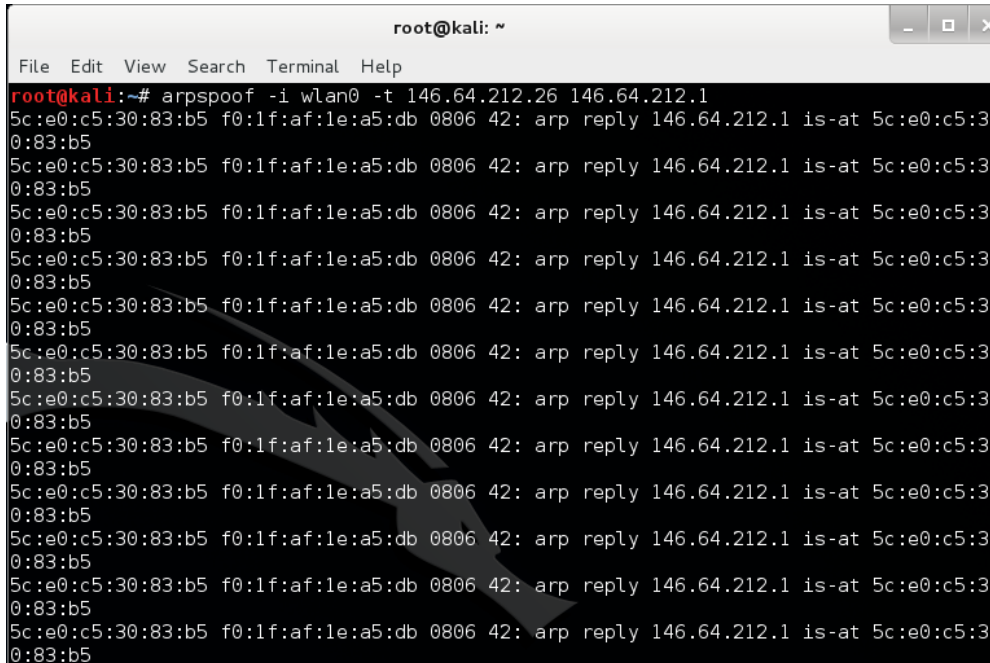


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof -i wlan0 -t 146.64.212.1 146.64.212.26  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5  
5c:e0:c5:30:83:b5 2c:f4:c5:b8:7c:84 0806 42: arp reply 146.64.212.26 is-at 5c:e0:  
c5:30:83:b5
```

**Figure 8.28.** The attacker convinces the gateway that it is the legitimate user

### Step 7. The attacker convinces the legitimate user that it is the gateway

The command “arpspoof” was issued again from the attackers’ machine where the attacker convinces the legitimate user that the attacker is the gateway. It can be noted in Figure 8.29 that the legitimate user sends “arp reply” messages indicating that a connection between the legitimate user and the attacker was established. Having established the connection between the legitimate user and the attacker, the next step is to determine the content accessed by the suspected legitimate user.

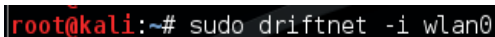


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof -i wlan0 -t 146.64.212.26 146.64.212.1  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5  
5c:e0:c5:30:83:b5 f0:1f:af:1e:a5:db 0806 42: arp reply 146.64.212.1 is-at 5c:e0:c5:30:83:b5
```

**Figure 8.29.** The attacker convinces the legitimate user that it is the gateway

### Step 8. Determine the content accessed by the legitimate user.

To determine the content accessed by the suspected legitimate user, a tool called Driftnet was used on the Kali Linux machine. Driftnet is used to watch the network traffic accessed by the legitimate user and picks out and display the JPEG and GIF images. The command “driftnet” was issued on the attackers’ machine as indicated in Figure 8.30 and all the content access by the legitimate user is displayed in Figure 8.31.



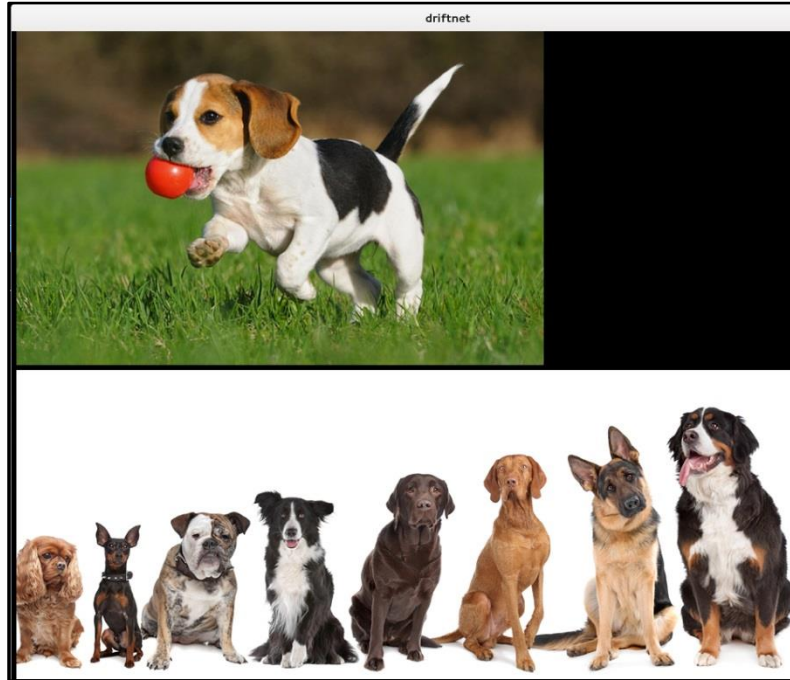
```
root@kali:~# sudo driftnet -i wlan0
```

**Figure 8.30.** Determine content accessed by the legitimate user

The researcher would like mention that sniffing network traffic as presented in this experiment is considered a horrific invasion of privacy and should not be done at all without obtaining prior consent in writing from law enforcement. However, as mentioned earlier, an assumption is made from this experiment that the owner of the Hotspot (the attacker) had prior obtained a permission from the law enforcement to monitor the network activities. Therefore, should a digital forensic investigation is warranted, the captured network traffic may be used for digital forensic investigations purposes. Similarly to the previous two experiments discussed above, this experiment shows how the data captured from the wireless



network can be analysed without tremendous effort by using a tool such as Driftnet. The data harvested from Drifted could link the suspected legitimate individual to the illegal activity suspected to be committed.



**Figure 8.31. Driftnet - digital evidence**

Having discussed the analysis phase, that is, Phase 4 of the WDFRM, the next section explains phase 5 (reporting).

### 8.3 Phase 5 (Reporting)

Reporting is a process used to present or communicate the results of a digital forensic investigation (Tanner et al., 2012). It is for this reason that this component forms an integral part of any digital forensic investigation (Lee et al., 2009). A digital forensic report typically contains information such as a case number, date, forensic examiner's information, a summary of the findings (Bunting and Wei, 2006; Nelson et al., 2010). This report can be supplemented by other detailed reports generated by forensic tools that were used during examination (Tanner et al., 2012). The report may include the findings of the digital forensic investigation and should also provide detailed steps that were taken during the analysis of the digital evidence.

Although there have been some work in the digital forensic community to create a common way of reporting digital evidence, a consensus is yet to be reached on a optimal way. Karie





and Venter proposed a framework for enhancing potential digital evidence presentation (Karie and Venter, 2013). Lee present a digital forensic search system architecture for efficiently presenting the searched results (Lee, 2008). Tanner et al presents a conceptual report management tool for graphically organising the facts of a case (Tanner et al., 2012). Lee et al. proposes a practical methodology for transforming the findings in a digital forensic report to a graphical representation using Bayesian Networks (BNs) (Lee et al., 2009). Garfinkel also mention that modern digital forensic tools assists with some aspects of report writing of digital evidence (Garfinkel, 2010). Farrell Jr presents a framework for automated digital forensic investigation (Farrell Jr. 2009). Casey provides reporting as the last stage of a digital forensic examination that integrate all findings and conclusions into a final report (Casey, 2010).

It should be noted that the reporting component was not implemented in the prototype and will therefore form part of future work.

#### **8.4 Concluding Remarks**

Chapter 8 presented and discussed Phase 4 – the analysis of the proposed model through demonstration by means of two experiments.

The first experiment was conducted to test the hypothesis of a dispute between an employer and an employee where the employee is being suspected of downloading music during office hours using the company's internet resources. The traffic captured from the network was analysed using Wireshark and NetWitness Investigator. Several interesting facts were identified from the analysis that could constitute digital evidence, such as, the IP address of the computer that the suspected user used to download music, the webserver's IP address in which the music was downloaded from, and the actual music content that the user downloaded.

The second experiment also aimed at testing a dispute between an employer and an employee. However, for this experiment, the employer was suspected of transmitting the company's trade secrets by an email to a third party. The experiment was conducted using Wireshark. Some of the results of the experiment includes the sender and recipient email addresses, the date and time in which the email was transmitted, and the actual email content which was transmitted.



The third experiment was conducted to test a scenario where a user is suspected of accessing illegal content on a WiFi network. The experiment used Driftnet to determine the suspected illegal content and could link the content to the suspected user.

The chapter also highlighted phase 5 (reporting) of the Wireless Digital Forensic Readiness Model. This chapter acknowledged the fact that reporting of digital evidence remains the important part in any digital forensic investigation because any inappropriate reporting could result in the inadmissibility of the digital evidence which is presented in the court of law. This phase was not explained into details; hence it will form part of future work.

The next part, part V concludes this dissertation by exclusively examining how the proposed model can be implemented in current WLAN environments.

## **PART V: Conclusion**



## Chapter 9                      **Critical Evaluation of the WDFRM**

### **9.1 Introduction**

This chapter highlights the two main contributions that this study has made by reflecting on the two main components of the study – the Wireless Digital Forensic Readiness Model and the WLAN digital forensic readiness prototype. It also explains why these items should be considered contributions to the field of WLAN digital forensics. The chapter further shows through an expert opinion that employing forensic readiness in a WLAN environment can minimise the cost and time needed to conduct a fully-fledged digital forensic investigation. The legal issues with regard to network traffic interception are also discussed in this chapter. The limitations of the model then follow, and the chapter is concluded with a brief summary of the entire dissertation.

### **9.2 Wireless Digital Forensic Readiness Model**

This dissertation proposed a Wireless Digital Forensics Readiness Model in Chapter 5. It was mentioned that the most salient issue addressed by the model is that it captures wireless network traffic and stores the traffic in a digital forensically sound manner. This was done so that should a full digital forensic investigation be warranted; the forensic team would simply extract the forensically stored data and conduct the required digital forensic investigation.

The benefit of the model is that it saves time and costs because the information needed for the digital forensic investigation has been made readily available. This implies that the first part of the digital forensic process (i.e. monitoring, logging and preservation) has been completed.

It was mentioned in Chapter 4 that a digital forensic investigation should adhere to the prescriptions of a proper digital forensic process. The model was designed in such a way that it adheres to this prescription because it consists of five phases, namely monitoring, logging, preservation, analysis and reporting. Since these phases were successfully followed as a proof of concept, other researchers who intend implementing digital forensic readiness in wireless networks can adhere to them and use them as a checklist, as they would have no negative effect on their existing wireless networks. After the model had been defined and designed, it was translated to a prototype in order to show the viability of implementing digital forensic



readiness in a WLAN environment. The next section explains the WLAN digital forensic readiness prototype.

### 9.3 WLAN Digital Forensic Readiness Prototype

The WLAN digital forensic readiness prototype was implemented in Chapter 7 using various tools that had been explained in Chapter 6. Only the first three phases of the WDFRM (i.e. monitoring, logging and preservation) were implemented since they are sufficient to show that capturing and logging network traffic in a digital forensic readiness manner can save cost and time when conducting a fully-fledged digital forensic investigation. The prototype presented in Chapter 7 has two benefits, namely the ability to implement digital forensic readiness in a WLAN environment and the ability to analyse the captured network traffic, should a digital forensic investigation be warranted. These benefits are explained next.

#### 9.3.1 Digital Forensic Readiness

The main goal of this dissertation was to implement digital forensic readiness in a WLAN environment. The dissertation claims that this goal was achieved successfully. Throughout Chapter 7, the prototype demonstrated that it captures network traffic using Tshark. The researcher implemented special flags within Tshark to determine the size of the Tshark output file, format, location, and when should the next output file be created.

One of the requirements of digital forensic readiness is to ensure that the traffic captured from the network was not compromised. The prototype adhered to this requirement by extracting the original captured traffic and hashed it using the MD5 and SHA-1 hashing function, after which it stored the resulting hash values in a database. The original traffic was then hashed again using the same hashing functions. The resulting hash values for both hashing were compared. It was found that they are the same, meaning that the original traffic captured from the network was not compromised.

The fact that the prototype can capture and store network traffic in a digital forensically sound manner and could prove beyond any reasonable doubt at a later stage that the original traffic was not compromised, suggests that the prototype fulfils the goal of implementing digital forensic readiness in WLAN. This is because, should a fully-fledged digital forensic investigation be warranted, the forensic expert's job is already reduced by half since the



capturing and preservation of network traffic has already been done for him. Assuming that a digital crime committed on the network is reported and a digital forensic investigation is warranted, the researcher explains in the next section how this dissertation analysed the network traffic that was captured from the network to check if it contains any data that can be used as digital evidence in a court of law.

### 9.3.2 Forensic Analysis of Network Traffic

In Chapter 7, the researcher explained how the prototype monitors, logs and preserves network traffic. In Chapter 8, the researcher explained two experiments that were used to analyse the digital forensically captured and stored network traffic. A third experiment was also conducted to tighten the argument wireless LAN forensics presented in this dissertation.

The first experiment was conducted to identify a user who was suspected of contravening the company's ICT policy by downloading music during office hours. The network traffic captured in the prototype was then analysed, using Wireshark and NetWitness Investigator (these tools were both introduced in Chapter 6). The results of the analysis successfully managed to identify the suspected illegal activity conducted on the network and could link it to the suspected user. That is, the IP address of the machine that downloaded the music was identified. Also, the actual binary data – in other words the mp3 files and the server to which the mp3 files were downloaded – were retrieved from the network traffic.

This experiment shows that storing network traffic in a digital forensically sound manner is very useful for digital forensic purposes. In this case, the researcher did not have to start the traffic capturing and preservation process from scratch; rather he could simply analyse the network traffic that had been captured and stored in a digital forensically sound manner. It is envisaged that by doing so, a lot of time and cost could be saved if a full digital forensic team were to be hired to conduct the digital forensic investigation from the beginning.

The second experiment was conducted to identify a user who was suspected of having transmitted the company's trade secrets to a third party using the company's Wi-Fi. This experiment was similar to the first one in that the first experiment focused on binary data analysis while the second one focused on plain text analysis. The focus here was on analysing the transmitted Simple Mail Transfer Protocol (SMTP) traffic to identify the email message that could contain the digital evidence to link the employee to the suspected event. The results of the second experiment revealed the following digital evidence, namely: the



sender's email address, the application used to send the email (Microsoft Outlook), the sender's IP address, the date and time at which the email had been sent, the subject of the email, the destination email and IP addresses, and even the actual email content that had been transmitted. Similarly to the first experiment, this experiment also showed that capturing and storing network traffic in a digital forensically sound manner was very useful in the sense that it can tremendously minimise the forensic expert's time and the cost needed to conduct a digital forensic investigation.

The third experiment was conducted to test a scenario where the owner on hotspot suspected that a specific user connected to the network is accessing illegal content which has detrimental effects on the network bandwidth. The owner of the WiFi then setup a man-in-the-middle attack to harvest information accessed by the suspected IP address in order to see the actual content accessed by the suspected IP address. Three entities were used in the experiment setup, that is, a 3G D-Link router acting as a gateway, a separate machine that access the illegal content and a Kali Linux machine that convinces both the gateway and the suspected machine that it is the other party. Driftnet was used on the Kali Linux machine to harvest the suspected illegal content. The results of the experiment show JPEG images that could be linked to the suspected IP address. Similarly to the two experiments above, this experiment proves the idea that capturing and storing network traffic before an incident occurs could greatly improve the amount of time needed to conduct a digital forensic investigation.

The fact that the model was tested with three different experiments shows that the model is scalable. If new wireless attacks happen other than the ones presented in chapter 8, the model would still be able to detect them due to its scalability.

The researcher would also like to mention that the proposed WDFRM would capture all the active wireless security attacks presented in Chapter 2. However, the passive attacks would be the most difficult one to be detected by the WDFRM due to the fact that they don't leave any digital footprint on the network to detect any vulnerability; rather they just sniff the transmitted traffic without altering or deleting it. The reader should also note that the WDFRM is encompassing in nature, hence it provides for many wireless digital footprint that might be useful for digital forensic investigations. For example, the mp3 files, the email content and the JPEG files presented in chapter 8 can act as digital evidence for this system.



It is also worth mentioning that Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS) and Intrusion Prevention (IPS) are all reactive management systems, which provide alerts when an event occurs. These systems collect logs and other security-related information which are then inspected and flag the anomalies. They are often after the fact and were not designed with forensic readiness capabilities. The Wireless Digital Forensic Readiness Systems presented in this dissertation is proactive in nature; it captures everything in the network in a forensic readiness manner which makes it a more viable solution when dealing with wireless network forensics.

The researcher explained the WDFRM and the prototype as two main contributions of this dissertation. Next, the researcher evaluates the WDFRM through obtaining the expert opinion of a company called Risk Diversion Pty (Ltd).

## 9.4 Evaluation of the Wireless Digital Forensic Readiness Model

This section reports on the evaluation of the WDFRM by an expert. The expert opinion also confirms that employing digital forensic readiness in a WLAN can greatly minimise the cost and time of conducting an entire digital forensic investigation. The section below firstly highlights the IEEE 802.11 a, b and g devices and further discusses the average data rate that can be produced by these devices in a given time.

### 9.4.1 IEEE 802.11 Performance and Characteristics

Table 9.1 (Geier, 2001) compares the maximum data rate, modulation, data rate and frequencies of different IEEE 802.11 specifications.

**Table 9.1.** IEEE 802.11 specification

Specifications	802.11a	802.11b	802.11g
Maximum data rate	54Mbps	11Mbps	54Mbps
Modulation	OFDM	DSSS	OFDM and DSSS
Data rate	6,9,12,18,24,36,48,54 Mbps	1,2,5.5,11 Mbps	DSSS:1,2,5.5, 11 OFDM:6,9,12, 18,24,36,48,54 Mbps
Frequencies	5GHz	2.4GHz	2.4GHz

Theoretically, the data rate of an 802.11g AP is 54Mbps. However, in practice an average data rate of 24Mbps is achievable due to factors such as interference and collision, as well as





the fact that the AP is not always utilised to capacity (100%) (WLAN, 2003). Of course, this data rate would be achievable if the AP's associated clients are also 802.11g products, taking into consideration the range between the AP and its associated clients.

#### 9.4.2 Average Data Rate of an IEEE 802.11g AP

Now that we know an 802.11g network will have an average data rate of 24 Megabytes per second (Mbps), we can calculate the average data rate it would produce in 8 hours to simulate a common business day. We first find the average data rate (ADR) that an AP would produce in one minute.

$$\begin{aligned}\text{ADR per minute} &= 24 \text{ Mbps} * 60'' \\ \text{ADR per minute} &= 1440 / 8 \text{ bits} \\ \text{ADR per minute} &= 180 \text{ Megabytes (MB)}\end{aligned}$$

The ADR of an AP per minute is 180 MB. Now that we know the ADR produced by the AP per minute, we can calculate the ADR of the AP per hour as follows:

$$\begin{aligned}\text{ADR per hour} &= 180 \text{ MB} * 60' \\ \text{ADR per hour} &= 10800 \text{ MB} \sim 10.8 \text{ Gigabytes (GB)}\end{aligned}$$

The ADR of an AP per hour is 10.8 GB. To calculate the ADR per day (which in our case is 8 hours), we multiply 10800 MB by 8, as shown below:

$$\begin{aligned}\text{ADR per day} &= 10800\text{MB} * 8\text{hr} \\ \text{ADR per day} &= 86400 \text{ MB} \sim 86.2 \text{ GB}\end{aligned}$$

If a particular public WLAN, e.g. a shopping mall, has five 802.11g APs where clients can connect to them, then the whole network would generate an average data rate of 431 GB per day. It should be noted that this value is very optimistic in the sense that we doubt that so much data will be generated over the said period, yet we need to cater for such scenarios. The average data rate may vary, depending on factors such as the number of clients associated with each AP, the range between an AP and its clients, and other factors.

#### 9.4.3 Expert Opinion

To show that a digital forensically ready organisation would minimise time and cost for conducting a fully-fledged digital forensic investigation as Tan (2001) suggests, the researcher requested a company called Risk Diversion (Risk Diversion, 2014) for a quotation as to how much it will cost to log such wireless network traffic in a public Wireless LAN environment with five 802.11g APs, assuming they have the necessary legal clearance to do



so. Risk Diversion is a (Pty) Ltd company specialising in information security audits as well as computer, cell phone and network forensic investigation and analysis. According to Risk Diversion, logging wireless traffic in an 802.11g network with five APs for 8 hours would cost about US\$2000 when hiring a full forensic team.

This shows that if an organisation were to log wireless traffic and store it in a forensically ready manner, say for five days, it would save them up to US\$10 000 compared to hiring a full forensic team. In fact, it would only cost the organisation approximately 2TB of storage to store all the data, which boils down to about US\$100 in cost. Even if data needs to be retained for a full year, the storage cost would amount to significantly less than hiring a forensic team. All that would be required would be to have a reliable RAID system with a few drives that would be able to accumulate data for about a week, after which the data can be written to tape drives and securely stored for periods as long as required by specific retention policies and laws. This confirms that the cost of logging and storing data is much cheaper than carrying out a fully-fledged digital forensic investigation. The point we want to make is simply that it would be cheaper and that acquiring storage space would be a once-off expenditure.

Organisations deploying WLANs that are at a high risk of cyber-attacks should be ready to collect digital evidence before an incident occurs. The model presented in this dissertation therefore addresses the concept of digital forensic readiness in WLANs.

The next section presents South African legal issues with regard to the interception of communication.

## **9.5 Legal Issues with Regard to Interception of Communication**

It was mentioned in Chapter 5 that one of the functions of the Wireless Digital Forensic Readiness Model is to monitor wireless network traffic. Traffic monitoring may also be referred to as interception of communication as provided for in the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) (RICA, 2003).

The legal requirements on interception of communication may vary across different jurisdictions all over the whole world. Examples of such legislation are the Electronic Communication Privacy Act (ECPA) of 1986 of the United Kingdom (UK) (Doyle, 2012),



the Electronic Communication and Transaction (ECT) Act of South Africa (ECT Act, 2002), Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) of South Africa (RICA, 2003), the Protection of Personal Information (POPI) Act of South Africa (POPI Act, 2013) and the Stored Communication Act (SCA) of United States of America (USA) (Kerr, 2004).

The ECPA states that it is a federal crime to intercept electronic communication of others without a court approval or consent. The SCA shares the same sentiments as the ECPA by stating that interception of communication without any consent is considered prohibited action. The ECT Act authorises cyber inspectors to monitor electronic communication systems in a public domain and report any unlawful activity to the appropriate authority. The RICA prohibits the interception of communication. However, it makes provision for a person intercepting communication only for the purpose of investigating or detecting unauthorised use of that communication system. It also states that the interception of communication may only take place if the entity whose information is intercepted has given prior consent in writing to the applicable law enforcement authorities. The POPI Act prohibits interference of privacy information especially if the matters are of national interest. However, a provision is made when the information is needed for law enforcement purposes and the party that is being monitored has consented to it.

Since the Wireless Digital Forensic Readiness Model provides a traffic monitoring functionality, it requires that all organisations deploying the model should adhere to these legal requirements on interception of communication – especially the South African ones. Since the legal requirements may vary on different jurisdictions of different countries, the system may be affected when deployed in another country since it has to first comply with legal requirements on interception of communications of that particular country. Despite all the functionalities provided by the WDFRM, it still has limitations. The next section presents the limitations of the WDFRM.

## 9.6 Limitations of the WDFRM

This section highlights the limitations of the proposed Wireless Digital Forensic Readiness Model. The limitations are discussed below.

- Physical attack on the access point – The first limitation is that the physical attack on the Access Point would not be detectable by the system.

- Storage constraint of the log file – The second limitation is that of the storage constraint of the log files. For demonstration purposes, the prototype output file size of the log file was set to 4 Megabytes. In larger organisation that generates a lot of traffic, this storage space might not be a feasible and can result to slow processing of the Tshark – a flag due to the large volume of traffic passing through the network.
- Difficult to detect passive attacks – The current system is designed in such a way that it would detect most of the active attacks presented in Chapter 2. However, it would not be able to detect most of the passive attacks since their purpose is just to listen to the network traffic without injecting, altering or deleting any packets on the networks.

Having discussed the limitations of the proposed WDFRM, the next section provides concluding remarks of the entire chapter.

## 9.7 Concluding Remarks

This chapter was devoted to a discussion of the two main contributions of this dissertation, namely the Wireless Digital Forensic Readiness Model and the Wireless Digital Forensic Readiness prototype. Each of these items showed that it can make a viable contribution to the WLAN digital forensic readiness domain.

The WDFRM was envisaged as a viable solution for minimising the cost and time needed to conduct a fully-fledged digital forensic investigation. This is true in the sense that network traffic is captured and stored in a digital forensic readiness manner. In an event where a crime is reported later on and a digital forensic investigation is warranted, the digital forensic experts would simply have to extract the digital forensically stored data and analyse it, rather than to conduct the entire investigation from the beginning. Moreover, it was evident that the model adheres to the prescripts of the digital forensic processes because it was designed based on five phases, namely monitoring, logging, preservation, analysis and reporting. These phases could be used by other researchers as a checklist when implementing digital forensic readiness in wireless networks.

The model was then translated to a prototype to prove the viability of implementing digital forensic readiness in a Wireless LAN. Two experiments were conducted to analyse the captured and digital forensically stored traffic. A third experiment was also conducted to



identify potential evidence from network traffic. All the three experiments were viable since they could identify information that might be used as digital evidence in a court of law.

The focus subsequently shifted to evaluating the model through obtaining an expert opinion. The expert opinion showed that an organisation employing digital forensic readiness would incur minimal cost compared to hiring a full digital forensic team. The legal issues with regard to the interception of communication were also looked at from a South African perspective.

Following the critical evaluation of the WDFRM, the next chapter constitutes a conclusion to this dissertation.



## Chapter 10 Conclusion

### Final Remarks

This study focused on developing a digital forensic readiness model that can be implemented in a Wireless Local Area Network environment. To accomplish this, several factors were considered.

The researcher started by studying the WLAN in general, which is the underlying network environment on which the entire dissertation is based. This was important because it provided an understanding of how WLANs function, for example, how a mobile station gets associated to the AP, and how network traffic is transmitted from the source to the destination address. It was pointed out that a WLAN allows mobile clients to join and leave the network at any time, in other words a WLAN is an open environment. This renders the WLAN vulnerable to a number of security attacks that were explained in this dissertation.

Next, the researcher looked at how an organisation can put itself in a position of being ready to respond to security attacks, should they occur. Digital forensics readiness was subsequently provided as a mechanism that can be implemented in a WLAN to help organisations to respond to these security attacks. Admittedly, there is no security protocol that is 100% secure, as even a strong encryption can be cracked given enough time to do so. It is for this reason that this research proposed a digital forensic readiness model that can be implemented in a WLAN environment. The model consists of five digital forensic phases, namely monitoring, logging, preservation, analysis and reporting. These phases were formulated from other digital forensic process models within the digital forensics domain. This model was then translated into a prototype to prove its viability.

All the research above was conducted to answer one question: *Is it possible to intercept and preserve all the communications generated by the mobile devices in a WLAN and conduct a digital forensic investigation?* The situation was exacerbated by the fact that a WLAN is an open environment that enables mobile devices to join and leave the network at any time, making it a real challenge to monitor and/or seize and investigate such mobile devices. The problem is that, by the time the investigation is required, the devices have long since left the network and communications have long been lost. The research question was answered by



providing a digital forensic readiness prototype that can be successfully implemented in a WLAN environment.

The problem was further answered by conducting three experiments to analyse the results of the prototype. The experiments were found to increase the usefulness of the forensically captured network traffic. The three experiments showed that organisations that use WLANs can greatly benefit from deploying the digital forensic readiness model and if an incident were to be reported later on and a digital forensic investigation would be warranted, the organisation would simply extract the forensically captured and stored data and conduct an analysis – rather than having to conduct the investigation from the beginning.

The researcher further evaluated the model by obtaining an expert opinion. A comparison was made on how much it would cost an organisation to hire a full forensic team, as compared to deploying the forensic readiness model. The findings by the expert suggested that it would be far cheaper to conduct a digital forensic investigation in a forensically ready organisation than to hire a full forensic team. The only cost that would be incurred in the latter case would be that of the storage space, since a lot of network traffic would need to be logged in one day. However, with the ever-declining prices of storage on the market, it would still be cheaper to buy a reliable RAID system compared to hiring a full forensic team.

Based on all the research conducted in this dissertation, a number of conclusions can be drawn:

- The Wireless Digital Forensic Readiness Model proved to be a viable contribution to the field of wireless digital forensics since it provides for five digital forensic phases that can be used as a checklist for other scholars when implementing digital forensic readiness in a wireless network environment.
- The implementation of digital forensic readiness in a WLAN environment was a viable solution because the prototype was able to capture and store network traffic without compromising the integrity of the traffic.
- The prototype experiments showed that the network traffic that was forensically captured and stored by the prototype could easily be analysed using off-the-shelf tools and without making a tremendous effort, seeing that the data would be forensically stored.

When all these factors are taken into consideration, it is clear that a feasible way is proposed for implementing digital forensic readiness in any Wireless Local Area Network environment. Despite the fact that this is in itself a contribution to the wireless digital forensics domain, there are more areas that can benefit from this research through future research.

Future research can be conducted by exploring the reporting component of the Wireless Digital Forensic Readiness Model. It should be noted that this component was not implemented in the prototype in Chapter 7. However, reporting remains an integral part of any digital forensic investigation. Future research can focus on coming up with an optimal way of reporting digital evidence.

Another area of proposed future research involves that of handling the huge amount of network traffic that flows through the WLAN. The prototype currently uses Tshark to capture network traffic with specific flags parsed in it to specify the network interface from which network traffic should be captured, the Tshark output file size, and to create a new output file to be written to. For demonstration purposes, the output file size was set to 4Megabytes. However, increasing the output file size to cater for a network within a larger organisation might cause this flag to experience slow processing due to the large volume of traffic passing through the network. It is therefore proposed that an efficient mechanism or an algorithm be developed to help improve this flag.

From the research reported on in this dissertation, several research outputs were produced and published at conferences. The papers that were published include Ngobeni and Venter (2009), Ngobeni et al. (2010), and Ngobeni et al. (2012) and they are included in Appendix B.



## Bibliography

M. Ergen. I-WLAN: Intelligent Wireless Local Area Networking, PhD Thesis, Engineering-Electrical Engineering and Computer Sciences, University of California, Berkeley, 2004.

ITU-T Recommendation Y.2012. *Functional requirements and architecture of the NGN*, September 2006.

F. Mouton. Digital Forensic Readiness for Wireless Sensor Networks, MSc Thesis, Computer Science, University of Pretoria, Pretoria, 2012.

A. Adamczyk, M. Denny, X. Gao, N. Huslak, A. Modaresi, H. Nguyen, G. Patterson, M. Pickett and S. Stillman. *Application Services Infrastructure for Next Generation Networks Including One or More IP Multimedia Subsystem Elements and Methods of Providing the same*, US Patent US20070100981 A1, 2007.

ITU-T Recommendation Y.2001. *General overview of NGN*, October 2004.

M. Wu. Fighting Phishing at the User Interface, PhD Thesis, Massachusetts Institute of Technology, 2006.

H. Huang, J. Tan and L. Liu. Countermeasures Techniques for Deceptive Phishing Attack, *International Conference on New Trends in Information and Service Science*, 2009.

M. Jakobsson and S. Myers. *Phishing and Countermeasures, Understanding the Increasing Problem of Electronic Identity theft*, John Wiley & Sons, Inc Publication, Indiana University, Bloomington, Indiana, 2007.

Independent Communications Authority of South Africa (ICASA). A Notice Regarding the Frequency Spectrum Regulations, Government Gazette, Act No. 38641, Vol 597, 2015.

M. Souppaya and K. Scarfone. Guidelines for Securing Wireless Local Area Networks (WLAN), *Recommendations of the National Institute of Standards and Technology*, 2012.

N.B. Salem, J.P. Hubaux and M. Jakobsson. Reputation-based Wi-Fi Deployment, *ACM Journal of Mobile Computing and Communications Review*, Vol.9(3), Pp. 69-81, 2005.

G. Lackner, U. Payer and P. Teufl. Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods, *International Journal of Network Security*, Vol.9(2), Pp. 164-172, 2009.

L. Arockiam, B. Vani, S. Sivagowry and A. Persia. A Solution to Prevent Resource Flooding Attacks in 802.11 WLAN, *4<sup>th</sup> International Conference on obCom*, 2011.

B. Humble and E. Sundholm. Denial of Service Attacks Against 802.11b Wireless Networks, *ECE 478: Final Project*, 2004.

A. Gupta and M. Garg (2010). DoS Attacks on IEEE 802.11 Wireless Networks and Its Proposed Solutions, Available at: <http://ssrn.com/abstract=1645757>, [Accessed: 15 July 2012].

E. Velasco, W. Chen, P. Ji, and R. Hsieh. Wireless forensics: A new radio frequency based location system, *Proceedings of the Pacific Asia Workshop on Cybercrime and Computer Forensics*, pp. 1361-1368, 2008.

T.D. Nguyen, D.H.M. Nguyen, B.N. Tran, H. Vu, and N. Mittal. A Lightweight solution for defending against deauthentication/ disassociation attacks on 802.11 networks, *International Conference on Computer Communications and Networks (ICCCN)*, 2008.

E. Casey (Ed). *Handbook of Computer Crime Investigation, Forensic Tools and Technology*. San Diego, USA: Elsevier Academic Press, 2007.

D.A. Dripps. “Dearest Property”: Digital Evidence and the History of Private “Papers” as Special Objects of Search and Seizure, *Journal of Criminal Law and Criminology*, Vol.103(1), Pp. 49-110. 2013.

J. Broadway, B. Turnbull, and J. Slay. Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis, *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES)*, Pp. 1335-1360, 2008.

E. Casey. Network traffic as a source of evidence: tool strengths, weaknesses, and future needs, *Journal of Digital Investigation*, Vol.1 (1), Pp. 28-43, 2004.

S.S. Al-Wakeel. A Planning Methodology and Cost Models for Designing A Wide Area Network, *Proceedings of the World Congress on Engineering and Computer Sciences (WCECS)*, 2009.

T. Karyagiannis and L. Owens. Wireless Network Security, 802.11, Bluetooth and Handheld devices, *NIST Special Publication 800-48, National Institute of Standards and Technology, Gaithersburg, Maryland*, 2008.

K.J. Negus and A.L. Petrick. History of Wireless Local Area networks (WLANs) in the Unlicensed Bands, *Info*, Vol. 11(5), Pp. 36-56, 2008.

A. Rahman, (2009). Wireless Local Area Network: Background and Functions, Available online at: [http://www.bukisa.com/articles/153981\\_wireless-local-area-network-background-and-functions](http://www.bukisa.com/articles/153981_wireless-local-area-network-background-and-functions), [Accessed: 02 July 2011].

K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs. Guide to Securing Legacy IEEE 802.11 Wireless Networks, *NIST Special Publication 800-48, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland*, 2008.

L. Yang, P. Zerfos, and E. Sadot, (2005). Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP). Available at: <http://tools.ietf.org/html/rfc4118>, [Accessed: 13 July 2011].

M. Ergen, (2002). IEEE 802.11 Tutorials, Available at: <http://wow.eecs.Berkeley.edu/ergen/docs/ieee.pdf>, [Accessed: 02 July 2011].

M. Ilyas and S. Ahson (Ed). *Handbook of Wireless Local Area Networks, Applications, Technology, Security, and Standards*. Florida, USA: Taylor and Francis Publication, 2005.

I. Sherman. *Apparatus for and Method of Low Power Wireless Local Area Network Independent Basic Service Set Mode Operation*, US Patent, US20080181154 A1, 2007.

B. O'Hara and A. Petrick. *IEEE 802.11 Handbook, A Designer's Companion*, 2<sup>nd</sup> Edition. Park Avenue, New York: IEEE Press, 2005.

G.J. Mullet. *Wireless Telecommunications and Networks*. Springfield, MA: Thomson, 2006.

D. Bansal and S. Lalar. Authentication in Wireless Networks, *2<sup>nd</sup> National Conference on Challenges & Opportunities in Information Technology*, 2007.

M.S. Gast. *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, California: O'Reilly, 2002.

R. Wood. Programming Wireless Security, *SANS Institute*, 2008.

Privacy, (2006). Confidentiality, Integrity, Availability (CIA), Available at: **Error! Hyperlink reference not valid.**, [Accessed: 28 July 2011].

M.S. Gast. *802.11 Wireless Networks: The Definitive Guide, Second Edition*. Sebastopol, California: O'Reilly, 2005.

Computer networking notes, (2010). Available at: <http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html>, [Accessed, 25 March 2012].

A.R. Alkhawaja and H. Sheibani. Security Issues with Mobile IP, MSc. Thesis, School of Information Science, Computer and Electrical Engineering, Halmstad University, Sweden, 2011.

K. Bicakci and B. Tavli. Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks, *Journal of Computer Standards & Interfaces*, Vol. 31(5), Pp. 931-941, 2009.

C.A. Henk van Tilborg and S. Jajodia (Ed). *Man-In-the-Middle Attack*, Encyclopedia of Cryptography and Security, Second Edition, 2011.

V. Moen, H. Raddum, and K.J. Hole. Weaknesses in the Temporal Key Hash of WPA, *Journal of Mobile Computing and Communication, ACM*, Vol.8(2), Pp. 76-83, April 2004.

DFRW, (2001). Report from the First Digital Forensic Research Workshop (DFRW), Available at: <http://www.dfrws.org/2001/dfrws-rm-final.pdf>, [Accessed: 18 July 2011].

S.Y. Willassen and S.F. Mjøl̄snes. Digital Forensic Research, *Teletronikk*, 2005.

B. Carrier. *File System Forensic Analysis*. Crawfordsville, USA: Addison Wesley Professional, 2005.

Network Security,(2010).Available at:[http://computernetworkingnotes.com/ccna\\_certifications/types\\_of\\_attack.htm](http://computernetworkingnotes.com/ccna_certifications/types_of_attack.htm), [Accessed: 10 October 2011].

R. Leigland and A.W. Krings. A Formalization of Digital Forensics, *International Journal of Digital Evidence*, Vol. 3(2), Pp. 1-32, 2004.

K. Kent, S. Chevalier, T. Grance and H. Dang. Special Publication 800-86: *Guide to Integrating Forensic Techniques into Incident Response* – Recommendations of the National Institute of Standards and Technology, Gaithersburg, Maryland, USA, 2006.

D. Farmer and W. Venema, (1999). Computer Forensics Analysis Class Hand-outs, Available at: <http://www.bio-guru.com/forensics.htm>, [Accessed: 28 July 2010].

D. Farmer and W. Venema, (2004). The Coroner's Toolkit (TCT), Available at: **Error! Hyperlink reference not valid.**, [Accessed: 28 July 2010].

M. Reith, C. Carr and G. Gunsch. An Examination of Digital Forensic Models, *International Journal of Digital Evidence*, Vol. 1(3), Pp.1-12, 2002.

USDOJ,(2001).Electronic Crime Scene Investigation - A Guide for First Responders, Available at: [www.nwfiia.org/NIJGuideforFirstResponders.pdf](http://www.nwfiia.org/NIJGuideforFirstResponders.pdf), [Accessed: 23 October 2011].

K. Mandia, C. Prosise and M. Pepe. *Incident Response and Computer Forensics*, 2nd Edition New York, USA: McGraw-Hill, 2003.

*The American Heritage Dictionary of the English Language*, 4<sup>th</sup> Edition, Boston, USA: Houghton Mifflin Company, 2001.

S.S. James and J.J. Nordby (Ed).*Forensic Science: An Introduction to Scientific and Investigative Techniques*, 2<sup>nd</sup> Edition, Boca Raton, FL: Taylor and Francis Publishers, 2005.

J. Tan. Forensic Readiness, *The CanSecWest Computer Security Conference*, 2001.

G. Mohay. Technical Challenges and Directions for Digital Forensics, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2007.

C. Seifert, B. Endicott-Popovsky, D. Frincke, P. Komisarczuk, R. Muschevici and I. Welch. Justifying the need for forensically ready protocols, A case study of identifying malicious web servers using client honeypots, *4th Annual IFIP WG 11.9 International Conference on Digital forensics*, 2008.

Honeynet, (2011). Honeynet Project, Available at: <http://www.project.honeynet.org/>, [Accessed: 20June 2011].

S. Quinn. Examining the State of Preparedness of Information Technology Management in New Zealand for Events that May Require Forensic Analysis, *Journal of Digital Investigation*, Vol. 2(4), Pp. 276-280, 2005.

R. Rowlingson. A Ten Step Process for Forensic Readiness, *International Journal Of Digital Evidence*, Vol. 2(3), Pp. 1-27. 2004.

S. Mocas. Building Theoretical Underpinnings for Digital Forensics Research, *International Journal of Digital Forensics & Incident Response*, Vol. 1(1), Pp. 61-68, 2004.

A. Ahmad. The Forensic Chain-of-Evidence Model: Improving the Process of Evidence Collection in Incident Handling Procedures, *Proceedings of the 6th Pacific Asia Conference on Information Systems*, 2002.

B. Cusack and T. Laurenson. System Architecture for the Acquisition and Preservation of Wireless Network Traffic, *The proceedings of the 9th Australian Digital Forensics Conference*, 2011.

B. Turnbull and J. Slay. Wi-Fi network Signals as a Source of Digital Evidence: Wireless Network Forensics, *The Third International Conference on Availability, Reliability and Security*, 2008.

W.A. Arbaugh. Wireless Security is Different, *IEEE Information Technology Library*, Vol. 36(8), Pp. 99-101, 2003.

R. Siles, (2010). Wireless Forensics: Tapping the Air – Part One, Available at: **Error! Hyperlink reference not valid.**, [Accessed: 25 March 2011].

D. Yim, J.Y. Lim, S. Yun, S.H. Lim, O. Yi and J. Lim. The Evidence Collection of DoS Attack in WLAN by Using WLAN Forensic Profiling System, *International Conference on Information Science and Security*, 2008.

C.Y. Cho, S.Y. Lee, C.P. Tan and Y.T. Tan. Network Forensics on Packet Fingerprint, *In 21<sup>st</sup> IFIP Information Security Conference (SEC 2006)*, 2006.

J. Yeo, M. Youssef and A. Agrawala. A Framework for Wireless LAN Monitoring and Its Applications, *Proceedings of the 3rd ACM workshop on Wireless Security (Wise '04)*, 2004.

S. Ansari, S.G. Rajeev and H.S. Chandrashekar. Packet Sniffing: A Brief Introduction, *IEEE Potentials*, Vol. 21(5), Pp. 17-19, 2003.

M.A. Qadeer, A. Iqbal, M. Zahid and M.R. Siddiqui. Network Traffic Analysis and Intrusion Detection Using Packet Sniffers, *Second international Conference on Communication Software and Networks*, 2010.

A. Meehan, G. Manes, L. Davis, J. Hale and S. Sheno. Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation, *Proceedings of the IEEE Workshop on Information Assurance and Security*, 2001.

S. Northcutt. *Network Intrusion Detection, An Analyst's Handbook*. Indianapolis, Indiana: New Riders, 2000.

WireShark, (2012), Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?Arnumber=5496372>, [Accessed: 18 July 2012].

E. Seagren and W.J. Noonan. *Secure Your Network for Free: Using NMAP, Wireshark, Snort, Nesusand MRTG*. Rockland, MA,USA: Syngress Publishing, 2007.

S. Wang, D.S. Xu, and S.L. Yan. Analysis of Wireshark in TCP/IP Protocol Training, *International Conference on E-Health Networking, Digital Ecosystems and Technologies*, 2010.

R. R. Mohammad, F. Mohsen, (2009). Project: Network Analyser Software, Available at: <http://www.slideshare.net/sourav894/wireshark>, [Accessed: 15 April 2012].



F. Fuentes and D.C. Kar. Ethereal Vs. Tcpdump: A Comparative Study on Packet Sniffing for Educational Purpose, *Journal of Computing Science in College*, Vol. 20(4), Pp. 169-176, 2005.

S. McClure, J. Scambray and G. Kurtz. *Hacking Exposed, Network Security Secretes & Solutions*, Fourth Edition. Ney York, USA: McGraw-Hill/Osborne, 2003.

B. Turnbull and J. Slay. Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection Process, *Proceedings of the 40<sup>th</sup> Hawaii International Conference on System Sciences (HICSS)*, 2007.

J. Ning, S. Singh, K. Pelechrinis, B. Liu, S.V. Krishnamurthy and R. Govindan. Forensic Analysis of Packet Losses in Wireless Networks, *20<sup>th</sup> IEEE International Conference on Network Protocols (ICNP)*, 2012.

H. Achi, A. Hellany and M. Nagrial. Digital Forensics of Wireless Systems and Devices: Technical and Legal Challenges, *6<sup>th</sup> International Symposium on High-Capacity Optical Networks and Enabling Technologies (HONET)*, 2009.

B. Endicott-Popovsky, D.A. Frincke, C.A Taylor. A Theoretical Framework for Organizational Network Forensic Readiness, *Journal of Computers*, Vol.2(3), Pp. 1-11, 2007.

K.P. Mc Grath and J. Nelson. A Wireless Network Forensic System, Irish Signal and Systems Conference (ISSC), 2006.

B. Wiley,(2013). Dust: A Blocking-Resistant Internet Transport Protocol, Available at: <http://blanu.net/Dust.pdf>, [Accessed: 18 November 2013].

M.G. Solomon, D. Barrett, and N. Broom. *Computer forensics, The Best First Step towards a Career in Computer Forensics*. San Francisco, London: SYBEX Inc, 2005.

S.L. Garfinkel. Digital Forensic Research: The next 10 years, *The Proceedings of the Tenth Annual Digital Forensic Research Workshop (DFRW) Conference*, 2010.

E. Casey, G. Fellows, M. Geiger, G. Stellatos. The Growing Impact of Full Disk Encryption on Digital Forensics. *Journal of Digital Investigation*, Vol.8(2), Pp. 129-134, 2011.



A. Spruill (2012). Digital Forensics and Encryption, Available at: [Accessed: 15 October 2013].

S.J. Ngobeni and H.S. Venter. The design of a Wireless Forensic Readiness Model (WFRM). *Proceeding of 8th Information Security South Africa (ISSA) Conference*, pp 1-18, 2009.

Visual Studio, (2013a). What is Visual Studio? Available at: <http://whatisvisualstudio.com/>, [Accessed: 22 February 2013].

Microsoft, (2013a). Microsoft Visual Studio Express 2012 for Windows Desktop, Available at: <http://www.microsoft.com/visualstudio/eng/products/visual-studio-express-for-windows-desktop#product-express-desktop>, [Accessed: 22 February 2013].

Wireshark, (2013). Terminal-based-Wireshark, Available at: [http://www.wireshark.org/docs/wsug\\_html\\_chunked/AppToolstshark.html](http://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html), [Accessed: 25 February 2013].

Tshark, (2013). Tshark, Available at: [www.wireshark.org/docs/man-pages/tshark.html](http://www.wireshark.org/docs/man-pages/tshark.html), [Accessed: 25 February 2013].

Microsoft, (2013b). Microsoft SQL Server, Available at: <http://www.microsoft.com/en-us/download/details.aspx?id=29062>, [Accessed: 22 February 2013].

A. Orebaugh, G. Ramirez, J. Burke and L. Pesce. *Wireshark & Ethereal Networks Protocol Analyzer Toolkit: Jay Beale's Open Source Security*. Rockland, MA, USA: Syngress Publishing, 2006.

B. Girardi. NetWitness Investigator Freeware, Network Intelligence, Threat Indicators and Session Exploitation, NetWitness Corporation, 2010.

G. Gross, (2008). NetWitness Releases Free Version of Security Software, Available at: <http://www.infoworld.com/d/security-central/netwitness-releases-free-version-security-software-888>, [Accessed: 15 March 2013].

Filetext, (2013), Available at: <http://filext.com/file-extension/PCAP>, [Accessed: 17 May 2013].

A. Tanner, D. Dampier and J. Thompson. On Developing a Conceptual Modeling Report Management Tool for Digital Forensic Investigation, *IEEE Conference on Homeland Security Technologies (HST)*, 2012.

R. Lee, S.D. Lang and K. Stenger. From Digital Report to Bayesian Network Representation, *IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2009.

S. Bunting and W. Wei. *EnCase Computer Forensics: The official EnCE: EnCase Certified Examiner Study Guide*. Crosspoint Blvd, Indianapolis: Wiley Publishing, 2006.

B. Nelson, A. Phillips, and C. Steuart. *Guide to Computer Forensics and investigation, 4th Edition*, Boston, USA: Cengage Learning, 2009.

N.M. Karie and H.S. Venter. Towards a Framework for Enhancing Potential Digital Evidence Presentation, *Information Security South Africa (ISSA)*, 2013.

J. Lee. Proposal for Efficient Searching and Presentation in Digital Forensics, *The Third International Conference on Availability, Reliability and Security (ARES)*, 2008.

P.F. Farrel Jr. A Framework for Automated Digital Forensic Reporting. MSc. Thesis, Naval Postgraduate School, California, USA, 2009.

E. Casey (Ed). *Handbook of Digital Forensics and Investigation*. Burlington, USA: Elsevier Inc, 2010.

WLAN, (2003). The New Mainstream Wireless LAN Standard, White Paper, IEEE 802.11g, Available at: [http://www.dell.com/downloads /global/shared/broadcom\\_8\\_02\\_11\\_g.pdf](http://www.dell.com/downloads/global/shared/broadcom_8_02_11_g.pdf), [Accessed: 02 April 2012].

Risk Diversion, (2014). Available at: <http://www.pretoria-south-africa.com/risk-diversion-forensic-services.html>, [Accessed: 10 October 2014].

RICA. Regulation of Interception of Communications and Provision of Communication-Related Information Act, act No. 122 of 2003, Vol. 45, 2003.

C. Doyle. Privacy: An Overview of the Electronic Communication Privacy Act, *Congressional Research Service, CRS Report for Congress*, 2009.

ECT Act. Electronic Communication and Transaction Act, act No 25 of 2002, Vol. 446, 2002.

POPI Act. Protection of Personal Information Act, Act No. 912 of 2013, Vol. 58, 2013.

O.S Kerr. A User's Guide to the Stored Communications Act – And a Legislator's Guide to Amending it, *George Washington Law Review*, Vol.72(6), 2004.

A.W Tsui, W.C, Lin and W.J Chen. War Driving and War Waling in Metropolitan Wi-Fi Localization, *IEEE Transactions on Mobile Computing*, Vol.9 (11), 2010.

K.P McGraw (Ed). *Animal Communication Networks*, United Kingdom, Cambridge: Cambridge University Press, 2005

Y. Song, C. Yang, and G. Gu. Who is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point. *IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 2010.

A. Bianchi, I. Oakley, V. Kostakos, and D.S Kwon. The Phone Lock: Audio and Haptic Shoulder-Surfing Resistance PIN entry Methods for Mobile Devices, *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction*, 2011.

P. Chumchu, T. Saelim and C. Sriklauy. A new MAC address Spoofing Detection Algorithm Using PLCP Header, *International Conference on Information Networking (ICOIN)*, 2011.

Technopedia, (2015). Address Resolution Protocol Spoofing (ARP Spoofing), Available at: <http://www.techopedia.com/definition/25409/address-resolution-protocol-spoofing-arpspoofing>, [Accessed, 03 May 2015].

R. McKemmish. What is Forensic Computing? *Australian Institute of Criminology Trends and Issues*, No. 118, 1999.

M.G Noblett, M. Pollit and L.A Presley. Recovering and Examining Computer Forensic Evidence, *Journal of Forensic Science Communication*, Vol 2(4), 2000.

K. Kent, S. Chevalier, T. Grance and H. Dang. Guide to Integrating Forensic Techniques into Incident Response. *National Institute of Standards and Technology, Special Publication 800-86*, 2006.

A. Mouhtaropoulos, C.T Li and M. Grobler. Digital Forensic Readiness: Are We There Yet? *Journal of International Commercial Law and Technology*, Vol. 9(3), 2014.

E. Casey. Investigating Sophisticated Security Breaches, *Communication of the ACM*, Vol. 49(2), 2006.

M. Schwartz (Eds) and N. Abramson. The ALOHAnet-Surfing for Data, History of Communications, *IEEE Communications Magazine*, 2009.

Y. Zhang, J. Zheng and H. Hu (Eds). *Security in Wireless Mesh Networks*, USA, Florida: CRC Press, 2008.

J. Geier. Wireless LANs, *Implementing High Performance IEEE 802.11 Networks*, 2<sup>nd</sup> Edition: Sams Publication, 2001.

E. Perahia and R. Stacey. *Next Generation Wireless LANs: 802.11n and 802.11ac*, United Kingdom, Cambridge: Cambridge University Press, (2013).

H.H Chen and M. Guizani. *Next generation wireless systems and networks*, England, West Sussex: John Wiley & Sons, 2006.

## Appendix A: Source Code

### A.1 Hash File

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using DataAccessComponent;
using DataAccessLayer;
using System.Security.Cryptography;
using System.IO;
using System.Security.Permissions;
using System.Diagnostics;

namespace WDFRM_HASHFILE
{
public partial class HashFile : Form
{
//Initializing the data access component so that we are able to use
//it to access the database
```



```
        HashFile_DataAccessComponent DAC =new
HashFile_DataAccessComponent ();
string[] filenameNames =newstring[10];
int j =0;
int l =0;

        Process p1 =newProcess ();

public HashFile ()
{
InitializeComponent ();
}

privatevoid fileSystemWatcher1_Created(object sender,FileSystemEventArgs e)
{
filenameNames[j]=e.FullPath.ToString ();
        j = j +1;

if(filenameNames[l]!=null)
{
stringtowrite= filenameNames[l];
WriteToDatabase(towrite);
        l = l +1;
}
else
{
}
}

privatevoidWriteToDatabase ()
{
        List<HashTable>newList=new List<HashTable> ();
newList=DAC.SelectPcapFileName ();
bool found =false;

for(int k =0; k <filenameNames.Length; k++)
{
for(int m =0; m <newList.Count; m++)
{
if(filenameNames[k]==newList[m].PcapFileName)
{
found=true;
}
}
if(filenameNames[k]!=null&& found ==false)
{
//creates an instance of the MD5 cryptography
        MD5 md5=System.Security.Cryptography.MD5.Create ();
        SHA1 sha1=System.Security.Cryptography.SHA1.Create ();

//reads the bytes of the file
byte[] b =File.ReadAllBytes (filenameNames[k].ToString ());
//creates the hash value but its not in hex
byte[] md5Hash = md5.ComputeHash(b);
byte[]shaHash= sha1.ComputeHash(b);

//converts the hash value to hex
StringBuilder md5String =newStringBuilder ();
StringBuilder sha1String =newStringBuilder ();

for(int i =0; i < md5Hash.Length; i++)
```

```

{
md5String.Append(md5Hash[i].ToString("x2"));
}

for(int i =0; i <shaHash.Length; i++)
{
sha1String.Append(shaHash[i].ToString("x2"));
}
//Pass the filename and the hash value to the data access component to be
inserted into the database
DAC.InsertIntoDumpLogTable(new HashTable(filenameNames[k].ToString(),
md5String.ToString(), sha1String.ToString()));
}
found=false;
}

        j =0;
        l =0;
}

privatevoidWriteToDatabase(string filename)
{
        List<HashTable>newList=new List<HashTable>();
newList=DAC.SelectPcapFileName();
bool found =false;

for(int m =0; m <newList.Count; m++)
{
if(filename ==newList[m].PcapFileName)
{
found=true;
}
}
if(found ==false)
{
//creates an instance of the MD5 cryptography
        MD5 md5=System.Security.Cryptography.MD5.Create();
        SHA1 sha1=System.Security.Cryptography.SHA1.Create();

//reads the bytes of the file
byte[] b =File.ReadAllBytes(filename.ToString());
//creates the hash value but its not in hex
byte[] md5Hash = md5.ComputeHash(b);
byte[] shaHash= sha1.ComputeHash(b);

//converts the hash value to hex
StringBuilder md5String =newStringBuilder();
StringBuilder sha1String =newStringBuilder();

for(int i =0; i < md5Hash.Length; i++)
{
md5String.Append(md5Hash[i].ToString("x2"));
}

for(int i =0; i <shaHash.Length; i++)
{
sha1String.Append(shaHash[i].ToString("x2"));
}
//Pass the filename and the hash value to the data access component to be
inserted into the database

```

```
DAC.InsertIntoDumpLogTable(new HashTable(filename, md5String.ToString(),
shalString.ToString()));
}

}

private void btnStart_Click(object sender, EventArgs e)
{
    p1.StartInfo.UseShellExecute = false;
    p1.StartInfo.RedirectStandardInput = true;
    p1.StartInfo.RedirectStandardOutput = true;
    p1.StartInfo.RedirectStandardError = true;
    p1.StartInfo.FileName = @"cmd.exe";
    p1.StartInfo.CreateNoWindow = true;
    p1.Start();

    p1.StandardInput.WriteLine(@"cd C:\Program Files\Wireshark");
    p1.StandardInput.WriteLine(@"tshark -a filesize:6000 -b filesize:4000 -i 2
-n -q -w C:\Users\AShozi\Documents\Demo\Capture.pcap");

    string name = p1.ProcessName;
}

private void btnStop_Click(object sender, EventArgs e)
{
    Process[] proc;
    proc = Process.GetProcesses();

    for (int i = 0; i < proc.Length; i++)
    {
        string name = proc[i].ProcessName;

        if (name == "dumpcap")
        {
            proc[i].Kill();
        }
    }

    WriteToDatabase();
    filenameNames = new string[10];

    MessageBox.Show("Files have been hashed and saved to the database", "Files
saved", MessageBoxButtons.OK);
}

private void HashFile_Load(object sender, EventArgs e)
{
}

}

}
```

## A.2 Data Access Component

```
using System;
using System.Collections.Generic;
using System.Linq;
```



```
using System.Text;
using System.Configuration;
using System.Data.SqlClient;
using System.Data;
using System.Security.Cryptography;
using DataAccessLayer;

namespace DataAccessComponent
{
    public class HashFile_DataAccessComponent
    {
        private string connectionString;

        public string ConnectionString
        {
            get { return connectionString; }
            set { connectionString = value; }
        }

        public HashFile_DataAccessComponent ()
        {
            connectionString = ConfigurationManager.AppSettings["connectionString"];
        }

        public void InsertIntoDumpLogTable (HashTable hashtable)
        {
            using (SqlConnection conn = new SqlConnection(connectionString))
            {
                SqlCommand cmdInsertIntoDumpLogTable
                = new SqlCommand("InsertIntoHashTable", conn);
                cmdInsertIntoDumpLogTable.CommandType =
                CommandType.StoredProcedure;

                cmdInsertIntoDumpLogTable.Parameters.Add(new SqlParameter("@UniqueNumber",
                SqlDbType.Int));

                cmdInsertIntoDumpLogTable.Parameters["@UniqueNumber"].Direction =
                ParameterDirection.Output;

                cmdInsertIntoDumpLogTable.Parameters.Add(new SqlParameter("@PcapFileName",
                SqlDbType.NVarChar, 100));
                cmdInsertIntoDumpLogTable.Parameters["@PcapFileName"].Value
                = hashtable.PcapFileName;

                cmdInsertIntoDumpLogTable.Parameters.Add(new SqlParameter("@MD5_HashValue",
                SqlDbType.NVarChar, 50));

                cmdInsertIntoDumpLogTable.Parameters["@MD5_HashValue"].Value =
                hashtable.Md5HashValue;

                cmdInsertIntoDumpLogTable.Parameters.Add(new
                SqlParameter("@SHA1_HashValue", SqlDbType.NVarChar, 50));

                cmdInsertIntoDumpLogTable.Parameters["@SHA1_HashValue"].Value =
                hashtable.Sha1HashValue;

            }

            try
            {
                conn.Open ();
                cmdInsertIntoDumpLogTable.ExecuteNonQuery ();
            }
        }
    }
}
```



```

catch (SQLException)
{
throw new ApplicationException("An error was encountered");
}
}

public List<HashTable>SelectPcapFileName ()
{
    List<HashTable>newList=new List<HashTable> ();

using (SqlConnection conn =new SqlConnection(connectionString))
{
    SqlCommand
cmdSelectPcapFileName=new SqlCommand("SelectPcapFileName", conn);

cmdSelectPcapFileName.CommandType= CommandType.StoredProcedure;

try
{
conn.Open ();

using (SqlDataReader reader =cmdSelectPcapFileName.ExecuteReader ())
{
while (reader.Read ())
{
    HashTable hash =new HashTable ()

{
        PcapFileName
=reader.GetString (reader.GetOrdinal ("PcapFileName"))
};
newList.Add (hash);
}
}

//    newList.Add (new
HashTable (cmdSelectPcapFileName.ExecuteNonQuery ().ToString ());
}
catch (SQLException)
{
throw new ApplicationException("An error was encountered");
}
conn.Close ();
}

return newList;
}
}
}

```

### A.3 Hash Table

```

public class HashTable
{
private int uniqueNumber;
private string pcapFileName;
private string md5HashValue;
private string sha1HashValue;
}

```



```
public HashTable(string filename,string md5Value,string sha1Value)
{
    pcapFileName= filename;
        md5HashValue = md5Value;
        sha1HashValue = sha1Value;
}

public HashTable(string filename)
{
    pcapFileName= filename;
}

public HashTable()
{
}

public HashTable(int number,string filename,string md5Value,string
sha1Value)
{
    uniqueNumber= number;
    pcapFileName= filename;
        md5HashValue = md5Value;
        sha1HashValue = sha1Value;
}

public int UniqueNumber
{
    get{return uniqueNumber;}
    set{ uniqueNumber = value;}
}

public string PcapFileName
{
    get{return pcapFileName;}
    set{ pcapFileName = value;}
}

public string Md5HashValue
{
    get{return md5HashValue;}
    set{ md5HashValue = value;}
}

public string Sha1HashValue
{
    get{return sha1HashValue;}
    set{ sha1HashValue = value;}
}
}
}
```

## A.4 Design

```
namespace WDFRM_HASHFILE
{
    partialclass HashFile
    {
        /// <summary>
        /// Required designer variable.
    }
}
```



```
/// </summary>
private System.ComponentModel.IContainer components =null;

/// <summary>
/// Clean up any resources being used.
/// </summary>
/// <param name="disposing">>true if managed resources should be disposed;
otherwise, false.</param>
protectedoverride void Dispose(bool disposing)
{
if(disposing &&(components !=null))
{
components.Dispose();
}
base.Dispose(disposing);
}

#region Windows Form Designer generated code

/// <summary>
/// Required method for Designer support - do not modify
/// the contents of this method with the code editor.
/// </summary>
private void InitializeComponent()
{
this.components=new System.ComponentModel.Container();
this.fileSystemWatcher1 =new System.IO.FileSystemWatcher();
this.timer1 =new System.Windows.Forms.Timer(this.components);
this.btnStart=new System.Windows.Forms.Button();
this.btnStop=new System.Windows.Forms.Button();
((System.ComponentModel.ISupportInitialize)(this.fileSystemWatcher1)).BeginInit();
this.SuspendLayout();
//
// fileSystemWatcher1
//
this.fileSystemWatcher1.EnableRaisingEvents =true;
this.fileSystemWatcher1.NotifyFilter
=((System.IO.NotifyFilters)(((System.IO.NotifyFilters.FileName|System.IO.N
otifyFilters.DirectoryName)
|System.IO.NotifyFilters.Size)
|System.IO.NotifyFilters.LastWrite));
this.fileSystemWatcher1.Path ="C:\\Users\\AShozi\\Documents\\Demo";
this.fileSystemWatcher1.SynchronizingObject =this;
this.fileSystemWatcher1.Created
+=new System.IO.FileSystemEventHandler(this.fileSystemWatcher1_Created);
//
// btnStart
//
this.btnStart.Font=new System.Drawing.Font("Microsoft Sans
Serif",8.25F, System.Drawing.FontStyle.Bold, System.Drawing.GraphicsUnit.Poin
t, ((byte)(0)));
this.btnStart.ForeColor=System.Drawing.Color.Green;
this.btnStart.Location=new System.Drawing.Point(26,41);
this.btnStart.Name="btnStart";
this.btnStart.Size=new System.Drawing.Size(155,48);
this.btnStart.TabIndex=1;
this.btnStart.Text="START CAPTURE";
this.btnStart.UseVisualStyleBackColor=true;
this.btnStart.Click+=new System.EventHandler(this.btnStart_Click);
//
```

```
// btnStop
//
this.btnStop.Font=newSystem.Drawing.Font("Microsoft Sans
Serif",8.25F,System.Drawing.FontStyle.Bold,System.Drawing.GraphicsUnit.Poin
t,((byte)(0)));
this.btnStop.ForeColor=System.Drawing.Color.Red;
this.btnStop.Location=newSystem.Drawing.Point(239,41);
this.btnStop.Name="btnStop";
this.btnStop.Size=newSystem.Drawing.Size(155,48);
this.btnStop.TabIndex=2;
this.btnStop.Text="STOP CAPTURE";
this.btnStop.UseVisualStyleBackColor=true;
this.btnStop.Click+=newSystem.EventHandler(this.btnStop_Click);
//
// HashFile
//
this.AutoSizeDimensions=newSystem.Drawing.SizeF(6F,13F);
this.AutoSizeMode=System.Windows.Forms.AutoSizeMode.Font;
this.ClientSize=newSystem.Drawing.Size(422,134);
this.Controls.Add(this.btnStop);
this.Controls.Add(this.btnStart);
this.Name="HashFile";
this.Text="Hash The File";
this.Load+=newSystem.EventHandler(this.HashFile_Load);
((System.ComponentModel.ISupportInitialize)(this.fileSystemWatcher1)).EndIn
it();
this.ResumeLayout(false);

}

#endregion

privateSystem.IO.FileSystemWatcher fileSystemWatcher1;
privateSystem.Windows.Forms.Timer timer1;
privateSystem.Windows.Forms.ButtonbtnStop;
privateSystem.Windows.Forms.ButtonbtnStart;
}
}
```

## A.5 Application Configuration

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<appSettings>
<add key="connectionString" value="Data Source=ASHOZI-NB1;Initial
Catalog=WDFRM_DB;Integrated Security=SSPI;"/>
</appSettings>
</configuration>
```

## Appendix B: Published Papers

During the process of conducting this research, three research outputs were produced, namely two peer-reviewed conference papers and a peer-reviewed international journal. These research outputs are inserted in this appendix in an ‘as is’ format, which includes retaining the original paper formatting such as font, page numbering and other formatting styles that were prescribed by the specific conference.

The three documents appear in chronological order according to the date on which they were presented/ published. The first paper presents the model proposed in this dissertation and is entitled “The design of a Wireless Forensic Readiness Model (WFRM)”. The second paper entitled “A Forensic Readiness Model for Wireless Local Area networks” is also concerned with the model proposed in this dissertation but with a specific focus on the components of the model as an integrated whole. The third document is a journal article entitled “The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks”. This article focuses on the implementation of the proposed model to show the viability of implementing digital forensic readiness in a WLAN environment.

The papers start on the next page.

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/220803199>

# A Framework for the Rapid Development of Anomaly Detection Algorithms in Network Intrusion Detection Systems.

Conference Paper · January 2009

Source: DBLP

---

READS

27

2 authors, including:



[Barry Irwin](#)

Rhodes University

97 PUBLICATIONS 207 CITATIONS

[SEE PROFILE](#)

# **INFORMATION SECURITY FOR SOUTH AFRICA**

Proceedings of the  
ISSA 2009 Conference

6 – 8 July 2009  
School of Tourism & Hospitality  
University of Johannesburg  
Johannesburg  
South Africa



*Edited by  
HS Venter, M Coetzee and L Labuschagne*

## **Preface**

PROCEEDINGS EDITORS: HS Venter, M Coetzee and L Labuschagne

PRODUCTION EDITOR: HS Venter

COVER DESIGNER: HS Venter

Copyright © 2009 Information Security South Africa (ISSA)

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, that the copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ISSA must be honored. Abstracting with credit is permitted. To copy otherwise, to publish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Request permission from The ISSA President, Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa, or [hventer@cs.up.ac.za](mailto:hventer@cs.up.ac.za).



**Publication Data**

ISBN 978-1-86854-740-1

Editors: Hein Venter, Marijke Coetzee and Les Labuschagne

Title of publication: Proceedings of the ISSA 2009 Conference

Publisher: ISSA

Place of publication: Pretoria, South Africa

Year of publication: 2009

Edition: First Edition, First Impression



UNIVERSITEIT VAN PRETORIA  
UNIVERSITY OF PRETORIA  
YUNIBESITHI YA PRETORIA

# TABLE OF CONTENTS

Preface.....	ii
Introduction.....	ix
Focus.....	xi
Conference Committees.....	xiii
Review Committee.....	xv
Review Process.....	xvii
Conference Sponsors.....	xix
<b>PART 1 – REVIEWED RESEARCH PAPERS.....</b>	<b>1</b>
A Best Practice Approach to Live Forensic Acquisition <i>MM Grobler and SH von Solms</i> .....	3
High-Level Integrated View of Digital Forensics <i>CP Grobler and CP Louwrens</i> .....	15
The Design of a Wireless Forensic Readiness Model (WFRM) <i>SJ Ngobeni and HS Venter</i> .....	35
BC3I – Towards Requirements Specification For Preparing an Information Security Budget <i>MT Dlamini, MM Eloff, JHP Eloff and K Hone</i> .....	53
Identification of Basic Measurable Security Components in Software Intensive Systems <i>RM Savola</i> .....	69

Proceedings of ISSA 2009

Discussing E-Government Maturity Models for Developing World – Security View <i>G Karokola and L Yngström</i> .....	81
Identification of Basic Measurable Security Components in Software Intensive Systems <i>A Nottingham and B Irwin</i> .....	99
Help Us! We Want To Be ‘E-Secured’: Digital Banking Customers’ Security Needs in South Africa <i>A Goldstuck and R Dagada</i> .....	117
An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System <i>H Meer</i> .....	137
A Framework for Web Services Security Policy Negotiation <i>T Lavarack and M Coetzee</i> .....	153
How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation <i>MP Zielinski and MS Olivier</i> .....	171
An Analysis of Authentication for Passive RFID Tags <i>GS Smith and M Coetzee</i> .....	189
An Introduction to Emerging Threats and Vulnerabilities to Create User Awareness <i>N Veerasamy and B Taute</i> .....	205
A Survey of Computer Crime and Security in South Africa <i>A Stander, A Dunnet and J Rizzo</i> .....	217
Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks <i>J Chetty and M Coetzee</i> .....	227

## Table of Contents

Automated Firewall Rule Set Generation through Passive Traffic Inspection <i>GC Pranschke, B Irwin and R Barnett</i> .....	243
Phishing: How an Organisation can Protect Itself <i>ED Frauenstein and R von Solms</i> .....	253
A Framework for the Rapid Development of Anomaly Detection Algorithms in Network Intrusion Detection Systems <i>RJ Barnett and B Irwin</i> .....	269
E-Mail Security Awareness at Nelson Mandela Metropolitan University (Registrar's Division) <i>R Boshoff and J van Niekerk</i> .....	279
Investigating Identity Concealing and Email Tracing Techniques <i>I Vural and HS Venter</i> .....	293
Enhanced Presence Handling <i>R Victor, A Rutherford and R Botha</i> .....	309
Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant? <i>R Dagada, MM Eloff and LM Venter</i> .....	327
Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation <i>KN Njenga and I Brown</i> .....	347
Integrating Information Assurance into System Administration <i>E Hjelm, NK Svendsen and SD Wolthusen</i> .....	363

Proceedings of ISSA 2009

**PART 2 – RESEARCH IN PROGRESS PAPERS ..... 377**

A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

*C Latzel, A Ruppen, and U Ultes-Nitsche ..... 379*

Usage Control Policy Enforcement in Openoffice.Org and Information Flow

*C Schaefer, T Walter, A Pretschner and M Harvan ..... 393*

The Design of a Logical Traffic Isolation Forensic Model

*I Dlamini and MS Olivier ..... 407*

Methodology for Considering Environments and Culture in Developing Information Security Systems

*J Mwakalinga, S Kowalski and L Yngström ..... 419*

The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics

*FR van Staden and HS Venter ..... 437*

Information Security Policies for Governmental Organisations: The Minimum Criteria

*SJ Ngobeni and MM Grobler ..... 455*

Concealing the Medicine: Information Security Education through Game Play

*T Monk, J van Niekerk and R von Solms ..... 467*

Management, Processing and Analysis of Cryptographic Network Protocols

*B Cowie, B Irwin and R Barnett ..... 479*

Mobile Communications Security Research at CSIR-MDS

*A Badimo and F Mekuria ..... 489*

## Introduction

ISSA2009 is the annual conference for the information security community that continues on the successful recipe established in 2000. We would like to thank Prof Jan Eloff and Prof Mariki Eloff who stepped down as conference chairs this year. They were founding members of ISSA and we would like to wish them all the best for their future endeavours. The new conference chairs, Prof Hein Venter and Dr Marijke Coetzee in conjunction with Prof Les Labuschagne undertake to build upon the good foundation that has been laid in the past by Prof Jan and Mariki Eloff for many years to come. The ISSA 2009 conference is held under the auspices of the University of Johannesburg Business IT Department, the University of Pretoria Department of Computer Science and the University of Johannesburg Academy for Information Technology.

The ISSA2009 Conference is held from Monday, 6 to Wednesday, 8 July at the University of Johannesburg's School of Tourism and Hospitality facility, in Auckland Park, Johannesburg, Gauteng, South Africa.

The conference has grown each year in various ways. Not only have delegate and presenter numbers been on the rise, but interest from industry has also grown and been displayed through sponsorship of the conference or aspects thereof. We believe that the quality and relevance of the information presented by industry practitioners and academics has also evolved over the years, as have the opportunities for senior research students to present their research to a critical and representative audience.

Conferences have become a major focus area - and often a money spinner - in many industries, so at any time you will see a number of conferences being advertised in fields such as information security. What sets the ISSA conference apart is that it is not intended to generate a profit for an organisation, and it does not encourage marketing of products and services through presentations. Instead, the proceeds from registration fees are reinvested to ensure that the conference grows each year. In exchange for their investment in the conference, sponsors are afforded an opportunity to present company-specific information that has a bearing on the conference themes, and presentations submitted by potential speakers are sent through a vigorous review process, managed by a team of respected international experts in information security.

## Proceedings of ISSA 2009

We trust that the annual ISSA conference will continue to be recognised as an platform for professionals from industry as well as researchers to share their knowledge, experience and research results in the field of information security.

To ensure ongoing improvement, we again encourage input from all those interested in the field of Information Security, particularly those who are actively seeking to progress the field, to take part and share their knowledge and experience.

We look forward to seeing old friends and new participants at ISSA2009.

### **ISSA 2009 Conference Organisers:**

Hein Venter

Marijke Coetzee

Les Labuschagne

July 2009



## Focus

Information security has evolved and in the last few years there has been renewed interest in the subject worldwide. This is evident from the many standards and certifications now available to guide security strategy. This has led to a more clear career path for security professionals.

The convergence of technologies together with advances in wireless communications, has meant new security challenges for the information security fraternity. As hotspots become more available, and more organisations attempt to rid their offices of "spaghetti" so the protection of data in these environments becomes a more important consideration.

It is this fraternity that organisations, governments and communities in general look to for guidance on best practice in this converging world.

Identity theft and phishing are ongoing concerns. What we are now finding is that security mechanisms have become so good and are generally implemented by companies wanting to adhere to good corporate governance, so attackers are now looking to the weak link in the chain, namely the individual user. It is far easier to attack them than attempt to penetrate sophisticated corporate systems. A spate of spyware is also doing the rounds, with waves of viruses still striking periodically. Software suppliers have started stepping up to protect their users and take some responsibility for security in general and not just for their own products.

The conference focuses on all aspects of information security and invites participation across the Information Security spectrum including but not being limited to functional, business, managerial, theoretical and technological issues.

Invited speakers will talk about the international trends in information security products, methodologies and management issues.

In the past ISSA has secured many highly acclaimed international speakers, including:

- Alice Sturgeon manages the area that is accountable for identifying and architecting horizontal requirements across the Government of Canada. Her topic made reference to An Identity Management Architecture for the Government of Canada

Proceedings of ISSA 2009

- Dr Alf Zugenmaier, DoCoMo Lab, Germany. His topic was based on Security and Privacy.
- William List, WM List and Co., UK. His topic was: Beyond the Seventh Layer live the users
- Prof. Dennis Longley, Queensland University of Technology, Australia. His topic was: IS Governance: Will it be effective?
- Prof. TC Ting: University of Connecticut, and fellow of the Computing Research Association, United States
- Prof. Dr. Stephanie Teufel: Director of the International Institute of Management in Telecommunications (iimt). Fribourg University, Switzerland
- Rich Schiesser, Senior Technical Planner at Option One Mortgage, USA
- Rick Cudworth, Partner, KPMG LLP, International Service Leader, Security and Business Continuity - Europe, Middle East and Africa
- Dario Forte - CISM, CFE, Founder, DFLabs Italy and Adj. Faculty University of Milano

The purpose of the conference is to provide information security practitioners and researchers worldwide with the opportunity to share their knowledge and research results with their peers.

The objectives of the conference are defined as follows:

- Sharing of knowledge, experience and best practice
- Promoting networking and business opportunities
- Encouraging the research and study of information security
- Supporting the development of a professional InfoSec community
- Assisting self development
- Providing a forum for education, knowledge transfer, professional development, and development of new skills
- Promoting best practice in information security and its application in Southern Africa
- Facilitating the meeting of diverse cultures to share and learn from each other in the quest for safer information systems

## Conference Committees

### **General Conference Chairs**

Hein Venter (Department of Computer Science, University of Pretoria)

Marijke Coetzee (Academy for Information Technology, University of Johannesburg)

Les Labuschagne (Department of Business Information Technology, University of Johannesburg)

### **Organising Committee**

Hein Venter (Department of Computer Science, University of Pretoria)

Marijke Coetzee (Academy for Information Technology, University of Johannesburg)

Les Labuschagne (Department of Business Information Technology, University of Johannesburg)

Leandi Ligthelm (Department of Computer Science, University of Pretoria)

### **Conference Programme Committee**

Hein Venter (Department of Computer Science, University of Pretoria)

Marijke Coetzee (Academy for Information Technology, University of Johannesburg)

Les Labuschagne (Department of Business Information Technology, University of Johannesburg)



UNIVERSITEIT VAN PRETORIA  
UNIVERSITY OF PRETORIA  
YUNIBESITHI YA PRETORIA

## Review Committee

Christer Andersson , Combitech, Sweden  
Sampson Asare , Computer Science Department, University of Botswana,  
Botswana  
Joachim Biskup , University of Dortmund, Germany  
Richard Baskerville , Georgia State University, USA  
Hettie Booysen , Private, South Africa  
Reinhardt Botha , Nelson Mandela Metropolitan University, South Africa  
Stelvio Cimato , University of Milano, Italy  
Nathan Clarke , University of Plymouth, UK  
Marijke Coetzee , University of Johannesburg, South Africa  
Mieso Denko , University of Guelph, Canada  
Paul Dowland , University of Plymouth, UK  
Lynette Drevin , Potchefstroom University, South Africa  
Mahmoud El-Hadidi, Cairo University, Egypt  
Jan Eloff, University of Pretoria, South Africa  
Mariki Eloff , University of South Africa, South Africa  
Sheikh Muhammad Farhan , University of Engineering and Technology,  
Pakistan  
Eduardo Fernandez , Florida Atlantic University, USA  
Stephen Flowerday, Nelson Mandela Metropolitan University, South Africa  
Dario Forte , University of Milano, Italy  
Steven Furnell , University of Plymouth, UK  
Dieter Gollmann , TU Hamburg-Harburg, Germany  
Anna Granova , University of Pretoria, South Africa  
Stefanos Gritzalis , University of the Aegean, Greece  
Talanja Grobler , University of Johannesburg, South Africa  
Ajantha Herath , Richard Stockton College of New Jersey, USA  
Andrew Hutchison , T-Systems South Africa (Pty) Ltd, South Africa  
Barry Irwin , Rhodes University, South Africa  
Christian Damsgaard Jensen , Technical University of Denmark, Denmark  
Jorma Kajava , University of Oulu, Finland  
Karthik Kannan , Purdue University, USA  
Sokratis Katsikas , University of the Aegean, Greece  
Les Labuschagne , University of Johannesburg, South Africa

Proceedings of ISSA 2009

Dennis Longley , Queensland University of Technology, Australia  
Marianne Loock , University of South Africa, South Africa  
Alko Meijer , Eclipse RDC, South Africa  
Kennedy Njenga, University of Johannesburg, South Africa  
Martin Olivier , University of Pretoria, South Africa  
Rolf Oppliger , eSECURITY Technologies, Switzerland  
Sylvia Osborn, University of Western Ontario, Canada  
Mauricio Papa , University of Tulsa, USA  
Guenther Pernul , University of Regensburg, Germany  
Dalenca Pottas , Nelson Mandela Metropolitan University, South Africa  
Laurette Pretorius, University of South Africa, South Africa  
Indrajit Ray, Colorado State University, USA  
Thomas Schlienger , International institute of management in  
telecommunications (iimt), University of Fribourg, Switzerland  
Mikko Siponen , University of Oulu, Finland  
Marco Slaviero, Sensepost, South Africa  
Alice Sturgeon, Treasury Board of Canada, Canada  
Stephanie Teufel, University of Fribourg, Switzerland  
Ulrich Ultes Nitsche , University of Fribourg, Switzerland  
Alta Van der Merwe , UNISA, South Africa, South Africa  
Hein Venter , University of Pretoria, South Africa  
Rossouw von Solms , Nelson Mandela Metropolitan University, South  
Africa  
Basie von Solms, University of Johannesburg, South Africa  
Louise Yngstrom , Stockholm University and the Royal Institute of  
Technology, Sweden  
Alf Zugenmaier , DoCoMo Euro Labs, Germany

## Review Process

The Review Process was undertaken by experienced and well respected Information Security experts. In a blind peer-review process full papers were scrutinised by an international panel of reviewers. The reviewers were asked to provide specific feedback and comments to authors. This feedback was provided to give a perspective on how a paper can be improved for final submission and inclusion in this - the formal conference proceedings.

A ‘Call for Papers’ was issued in January 2009, inviting anyone interested in making a contribution towards the conference by submitting a short abstract by the end of March 2009. Abstracts were received and subsequently divided into broad topics by the Programme Committee. The abstracts, within a broad field, were forwarded to a review panel in the field to judge on the possible acceptability of the abstract based upon the scope and depth of the subject matter to the conference as a whole. The authors were then requested to submit full papers by the end of April 2009. These draft papers were "anonomised", and then forwarded to two independent reviewers, with the request that the full paper should be reviewed and judged according to a number of criteria. Reviewers were asked to use a 10 point Likert scale to rate the following criteria:

- Originality
- Significance
- Technical Quality
- Relevance

Reviewers were also asked to give an Overall Rating as well as a Confidence in Rating for each the paper. In the next section, reviewers had to qualify their rating by providing a rationale for the Overall Rating given. This was followed by the Reviewer Comments that would assist the authors in improving and correcting their papers. Reviewers were asked to be as comprehensive as possible in this section.

The Programme Committee received the completed review forms from the Reviewers and combined the scores from the reviewers for each paper to determine whether they would be accepted or not. Only papers with a combined value above a certain threshold were accepted as full papers. In

## Proceedings of ISSA 2009

the event where two reviewers differed drastically from one another, the paper was sent to a third reviewer.

The reviewers' comments were forwarded to the author with the request to submit a final revised version of the paper by May 2009. Only those papers which were of an acceptable quality as recommended by both Reviewers are included in the Conference Proceedings as Reviewed Papers.

The review process used is based on what is considered the international de facto standard for blind paper reviews.



## Conference Sponsors and Organisers

### Sponsors

Unfortunately the ISSA conference organisers were unable to secure any sponsors for the conference in 2009. Should you be interested in becoming a sponsor in the future, please visit the ISSA website at [www.infosecsa.co.za](http://www.infosecsa.co.za).

### Conference Organisers



#### University of Johannesburg Department of Business IT

The Department of Business IT has extensive resources to facilitate excellence in terms of the graduate and post-graduate courses on offer. These include the lecturing staff, as well as computer laboratories, libraries and constant exposure to industry through various projects. We offer comprehensive qualifications that include vocational and academic direction of study. The main research focus areas include information security management, IT project management and advanced application paradigms.

Visit the Department's website at: [www.uj.ac.za/bit](http://www.uj.ac.za/bit)

### University of Pretoria Department of Computer Science



The University of Pretoria Computer Science Department offers opportunities for studies in BSc Information Technology and BSc Computer Science on under-

Proceedings of ISSA 2009

and post-graduate levels. These comprehensive, industry-relevant courses cover a number of the facets of information technology.

Visit the website at: [www.cs.up.ac.za](http://www.cs.up.ac.za)



### **University of Johannesburg Academy for IT**

The Academy for Information Technology offers studies in BSc Information Technology and BSc Computer Science. The four year BSc(IT) Hons degree has been formally accredited by the British Computer Society.

Visit the Department's website at: <http://www.uj.ac.za/csweb>



# **PART 1**

## **REVIEWED RESEARCH PAPERS**

Proceedings of ISSA 2009

## A BEST PRACTICE APPROACH TO LIVE FORENSIC ACQUISITION

MM Grobler<sup>1</sup>, SH von Solms<sup>2</sup>

<sup>1</sup> Council for Scientific and Industrial Research, Pretoria, South Africa

<sup>2</sup> Academy for Information Technology, University of Johannesburg

<sup>1</sup> marthiegrobler@gmail.com, mgrobler1@csir.co.za, 012 841 3262

<sup>2</sup> basievs@uj.ac.za, 011 559 2843

### ABSTRACT

The development of the Live Forensic discipline instigates the development of a method that allows forensically sound acquisition to stand fast in a court of law. The study presents the development of a comprehensive model for forensically sound Live Forensic Acquisition, the *Liforac model*.

The *Liforac model* presents a number of concepts that are already available within the Cyber Forensics discipline, combined as a single document. It composes four distinct dimensions: *Laws and regulations*, *Timeline*, *Knowledge* and *Scope*. These dimensions combine to present a wide ranging model to guide First Responders and forensic investigators in acquiring forensically sound digital evidence. The dimensions were identified as part of an intense research study on the current application of Live Forensics and the associated problems and suggested controls.

The *Liforac model* is an inclusive model that presents all aspects related to Live Forensic Acquisition, suggesting ways in which a Live Forensic Acquisition should take place to ensure forensic soundness. At the time of writing, this *Liforac model* is the first document of this nature that could be found for analysis. It serves as a foundation for future models that can refine the current processes.

### KEY WORDS

Forensically sound, Live Forensic Acquisition, Cyber Forensics, model

## **A BEST PRACTICE APPROACH TO LIVE FORENSIC ACQUISITION**

### **1 INTRODUCTION**

Up to date, forensic investigators approached live acquisitions with caution. The current norm is to perform traditional forensic acquisitions to ensure that evidence obtained remains forensically sound and useful in a court of law. However, new types of crime surfaced in the virtual world and traditional crimes are committed using advanced technology (Maat 2004:i). These developments leave Law Enforcement outdated and therefore Forensic investigators need to turn to Live Forensics to ensure successful investigations.

There is a close relationship between Cyber Forensics and the justice system. US-CERT (2005:1) defines Cyber Forensics as “... *the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications and storage devices in a way that is admissible as evidence in a court of law*”. This results in evidence admissible in a court of law (Jones 2007:2). Now, forensic investigators can acquire even more forensically sound evidence when implementing Live Forensic Acquisition.

This paper discusses a theoretical approach that underwrites forensically sound Live Acquisition, presented as the *Liforac model*. The model allows forensic evidence to stand fast in a court of law and covers all aspects relevant to Live Forensics. Although the idea of this model is not to present a rigid restrictive set of steps to follow, the intention is to develop a full set of guidelines to assist forensic investigators throughout the Live Forensic Acquisition process.

The proposed theoretical model consists of four distinct dimensions. These dimensions were identified as part of a research study on the current application of Live Forensics and associated problems and controls. Section 2 addresses the Live Forensic discipline and some of the associated benefits. Section 3 walks through the development of the model, addressing each of the dimensions. Section 4 concludes the paper.

### **2 MOVING TOWARDS LIVE FORENSIC ACQUISITION**

Live Forensics, referred to as Incident Response, is a methodology that advocates extracting live, real time system data before shutting down the system to preserve memory, process and network information that would

## A Best Practice Approach to Live Forensic Acquisition

otherwise be lost in a traditional forensic acquisition. The essence of this acquisition type is to minimise impacts to the integrity of the system while capturing volatile forensic data (McDougal 2006:5,9). Live Acquisition refers to the acquisition of a machine that is still running and can retrieve both static and dynamic, volatile data (Forte 2008:13). Traditional Dead Forensics focuses only on collecting and analysing information from stagnant file systems.

The Live Forensic discipline has not been perfected yet. Currently all endorsed tools and techniques have minor impacts on the underlying system's operating state and can be considered in court as inadmissible (McDougal 2006:5). However, forensic investigators argue that a complete chain of custody document should be sufficient to explain and motivate any system changes and accordingly lead to court admissibility. Some changes can be explained in the context of the investigation, analogous to the explanation of a detective's fingerprints on a ransom note (Adelstein & Richard 2007:14).

The main benefit of this Live Acquisition model is consistent and verifiable forensic acquisitions. Another benefit is that it requires little or no downtime from the system in question and that it can retrieve data that is only available in RAM (Adelstein & Richard 2007:3).

### 3 DEVELOPING A FORENSICALLY SOUND MODEL

To develop a useful model, it is necessary to include a number of wide ranging components to cover all aspects relevant to Live Forensics. Forensic investigators are responsible for technical insight, knowledge of the law and complete objectivity during investigations. Only then can investigators present direct evidence of suspected misconduct or potential exoneration (Stimmel 2008:1). The best way to ensure verifiable and repeatable results is by creating the *Liforac model* that investigators can apply consistently.

Figure 1 presents the proposed *Liforac model*, comprising of four distinct dimensions: *Laws and regulations*, *Timeline*, *Knowledge* and *Scope*. These dimensions combine to present a model that guides First Responders and forensic investigators in acquiring forensically sound digital evidence. The dimensions were identified as the four most prominent aspects during the preliminary literature study. A number of drivers were identified in the preliminary study that strongly directed the decision to divide the model into these four specific dimensions. The extent of these drivers is beyond the scope of this paper.

The *Liforac model* can prove useful to explain the work of cyber crime investigators to non-specialists. This can be especially supportive when presenting digital evidence in a court of law (Ciardhuáin 2004).

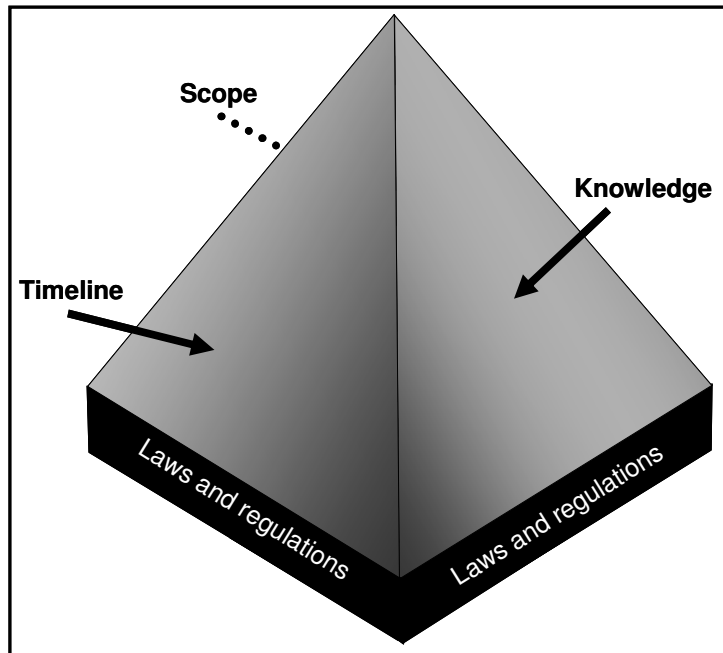


Figure 1: Liforac model

### 3.1 Laws and Regulations

The *Laws and regulations dimension* is the foundation of the *Liforac model*, forming the basis on which these dimensions rest. It considers in detail what the forensic investigator needs to know and do concerning laws and regulations to remain within the legal bound of the discipline. This dimension is not legally binding, but merely guides the organisation towards better technical understanding with regards to a legal subject.

With the emerging cyber crime rates and hike in cyber crime incidents, the *Laws and regulations dimension* is a very important part of the *Liforac model*. Not only is it necessary to pay attention to all aspects of cyber crime in order to do this, but these crimes need to relate to the legal discipline. This dimension divides into four sub dimensions:

- **Sub dimension 1: Common crime laws applicable to cyber crime.** Common crime laws, referred to as penal laws, are existing laws



## A Best Practice Approach to Live Forensic Acquisition

created with only traditional crimes in mind. The stakeholders wrote the laws in such a manner that interpretation within given circumstances can include the legal punishment of acts related to computers, digital evidence and cyber issues (Nare 2008).

- **Sub dimension 2: Specific cyber laws.** These laws, known as netlitigation, refer to laws created specifically with cyber crimes in mind. It addresses current issues related to cyber space, computers and electronic media or communication. Specific cyber laws are much more detailed and worth more in the event of a legal interpretation dispute. It helps organisations to prepare their systems for faster recovery in a cyber event and educate users on preserving electronic evidence.
- **Sub dimension 3: Court cases and precedents.** Court cases and precedents are crucial in the acceptance of any new technology in court. A court precedent can be defined as a “... *legal principle, created by a court decision, which provides an example or authority for judges deciding similar issues later*” (Lectric Law Library 2005). Precedents in court cases establish a principle or rule that another court needs to adopt when deciding cases with similar issues or facts. These laws are crucial in the acceptance of any new technology in court, for examples the Frye and Daubert tests.
- **Sub dimension 4: Definition of court admissibility.** The definition of court admissibility largely determines whether the court would allow Live Forensic Acquisition. This definition and its implementation has a big impact on the Live Forensic discipline and is in many cases the most important aspect to consider during the lifetime of a forensic investigation. To ensure that evidence can be admitted in court, the forensic investigator needs to ensure and maintain the accuracy, reliability and authenticity of the evidence at all times. The easiest way to accomplish this is by maintaining a proper chain of custody.

### 3.2 Timeline

The *Timeline* dimension focuses more on the process view of the model, indicating the sequence in which investigators need to execute processes. This dimension considers in detail what steps forensic investigators need to take to ensure a forensically sound investigation.

A timeline presents a visualisation of a sequence of events to show the relationship between the entities. This dimension presents all actions taken by forensic investigators, and presents it visually in the sequence it

should execute to ensure sound forensic practices. In essence, this specific timeline representation consists of implied and explicit processes. This dimension divides into five components:

- **Component 1: Implied processes.** These processes refer to specific processes that may not necessarily contribute directly to the successful completion of the dimension, but the absence of these processes may render the timeline unsuccessful. Implied processes specific for the *Liforac model* include how to secure potential evidence, how to preserve data integrity, how to record actions during an examination, the audit trail, how to analyse the collected data and information, and the establishment of a responsibilities matrix (Haggerty & Taylor 2006:14).
- **Component 2: Explicit processes.** These processes refer to specific processes that contribute directly to the successful completion of the dimension. Explicit processes specific for the *Liforac model* include awareness, authorisation, planning, notification, search for and identification of evidence, examination of evidence, hypothesis and the dissemination of information. These processes are largely based on Ciardhuáin's (2004) model.
- **Component 3: Before the investigation.** This timeframe ensures full coverage of all possible activities involved before the actual acquisition starts. Not only is it necessary to prepare all the people on the case involved, but a solid foundation might help the case in court. This timeframe has three themes: *awareness, authorisation* and *planning*. The sub activities include determining the power status of the computer and system, selecting the investigation mode (overt or covert), isolating the system in question and secure it promptly, selecting the analysis mode (local or remote) and comprehensive pre-acquisition planning.
- **Component 4: During the investigation.** This timeframe ensures full coverage of all possible activities for the duration of the acquisition. It guarantees that investigators collect all the necessary evidence in a manner that will lead to its successful admission in a court of law. Opposing counsel often question the integrity of this acquisition process and occasionally prove an inadequate chain of custody that lead to the exclusion of crucial evidentiary artefacts from the proceeding. This is often based on methods and techniques used during the acquisition process. This timeframe has three main themes: *notification, search and identify*, and *examination*. The sub activities include the chain of

## A Best Practice Approach to Live Forensic Acquisition

command, write blocking the target system, attaching the suspect hard drive to a forensic system, identifying logged on account and administrative rights, identifying the logged on system (real or virtual) and making a bit-by-bit copy of the suspect hard drive.

- **Component 5: After the investigation.** This timeframe ensures full coverage of all possible activities involved after the actual acquisition ends. This ensures that the chain of custody remains intact and the evidence are stored and returned safely after the investigation. This timeframe has three main themes: *hypothesis*, *information dissemination* and *controls*. The sub activities include updating the chain of command, securely sealing all packages, transporting and storing evidence, examining and analysing evidence with forensically sound software and providing a written report.

### 3.3 Knowledge

The *Knowledge* dimension indicates the different stages of awareness and understanding investigators need to perform sound Live Forensics. This dimension looks in detail at the people involved in successful Live Forensics: who they are and what training and skills they should possess.

With the ever-changing technologies, tools and techniques, forensic investigators need to stay updated with all new developments. To ensure that investigators are fully prepared for any type of forensic investigation, they need to ensure that their knowledge is up to standard to allow for any eventualities. This dimension divides into seven components:

- **Component 1: Computer Science.** Computer science is a wide discipline, containing a wide range of topics. For the purpose of being a forensic investigator, it is recommended that the individual have a proper computer science foundation and background. Although a computer science degree is not enforceable, it may help the investigator in understanding basic concepts. The knowledge built from these specialised topics may be helpful in certain forensic investigations. In some cases, computer science knowledge may be applied directly, whilst in others it ensures that investigators are more familiar with the specific scenario found at the crime scene.
- **Component 2: World Trends and Events.** World trends and events have a continual influence on Cyber Forensic knowledge. Forensic investigators need to update their knowledge on new trends in cyber crime and the combating of these crimes constantly. World

trends and events can have a dramatic impact on technology and related trends. In this case, it may be very helpful for forensic investigators to work in conjunction with the local CERT/CSIRT. These organisations work closely with CERTs/CSIRTs in other countries and can draw statistics regarding technological attack trends. For example, once a specific worm hits a specific country, it might take an average of 48 hours before the same worm generally hits South Africa. Cyber investigators can benefit from these statistics.

- **Component 3: Information Systems.** Information Systems are the organised collection, storage and presentation of information and related knowledge for decision-making. It can be defined as a collection of practices, algorithms and methodologies that transforms data into information and knowledge that is useful for individuals or groups of people (UMBC 2008). A proper information system foundation can aid a forensic investigator in the understanding of certain forensic principles and the interaction between the cyber criminal and his/her computer. Since there is a direct relationship between computers and information, this component is necessary in the knowledge dimension.
- **Component 4: Social Sciences.** Social sciences can play a role in Cyber Forensics due to its human and profiling nature. People tend to react in specific ways under certain circumstances, which may have an affect on the way the investigation is run. Forensic investigators now not only understand the hardware and software aspects of the suspect machine, but also may try to think like the person operating the suspect machine. He/she may psychologically step into the suspect's footsteps and think where the suspect may have hidden evidentiary files and folders. This discipline is not a prerequisite for forensics, but may make the investigator's task easier when the behavioural aspect is also considered.
- **Component 5: Forensic Sciences.** Forensic sciences are the core of Cyber Forensic investigations. When considering Biological Forensics, a basic understanding of this discipline contributes to a better understanding of Cyber Forensics. Many of the investigatory principles remain the same, although the physical application of the techniques and the tools differ drastically. A general understanding of this discipline may be beneficial.
- **Component 6: Law.** Cyber Forensics cannot stand separate from the law. Any forensic investigator need to have updated

## A Best Practice Approach to Live Forensic Acquisition

knowledge on current and pending legislation that may have an impact on the way forensic investigations are done. This aspect is so important that forensic investigators should not be allowed to enter the crime scene without sufficient knowledge for fear that they might contaminate the crime scene. A fully prepared forensic investigator should have a certain degree of legal knowledge.

- **Component 7: New Technology.** New technology, similar to world trends, has a persistent influence on Cyber Forensic knowledge. Every time new technology is publicly available, or an upgrade of software or a hardware component is on the shelves, investigators need to be trained on this. The chances are good that investigators may encounter these new technologies in an investigation. If they do not know how to handle these upgrades properly, investigators may encounter problems that may have a negative effect on the investigation. Forensic investigators need to update their knowledge on technology constantly to ensure their own forensic readiness.

### 3.4 Scope

The *Scope* dimension addresses practical problems related to Live Forensics. The concept of Live Forensic Acquisition is viable, but the identified problems drastically limit the scope of applicability of the dimension. This dimension looks in detail at the problems associated with Live Forensic Acquisition and identified five components, or practical problems that define the scope of the Live Forensic discipline.

At the moment, these components still pose serious problems to the successful admission of evidence to court, but the *Liforac model* will provide guidelines on handling these problems. This dimension has five components:

- **Component 1: Access to the machine.** Gaining access to the machine is the first practical problem that an investigator may encounter. Not only must the investigator gain access to the building and specific office in which the computer is located, but also to the physical machine by using a username/password combination. Some of the controls for this practical problem include a legit search warrant, cooperation from the suspect and system administrator and reasonable.
- **Component 2: Dependency on operating system.** The current forensic practices require interaction with the suspect machine's operating system. Each operating system needs to be treated differently during a forensic investigation and accordingly can pose a major practical problem. This practical problem has one

possible control to counter this dependency: a thorough foundation of related knowledge.

- **Component 3: Data modification.** Any process can modify computer data during acquisition, from user applications to the operating system itself. With current legislations, any data modification can render the evidence inadmissible in court. Some of the controls for this practical problem include thorough forensic training and up-to-date research.
- **Component 4: Demonstrate the authenticity of evidence.** All potential evidence needs to be properly authenticated before a court of law can accept it as legit evidence. This practical problem has a number of controls: expert witness testimony, comparison by expert witnesses with precedents, circumstantial evidence, public records, evidence produced as result of an accurate process or system, evidential weight, digital signatures, hashing techniques, timestamps and checksums.
- **Component 5: Court acceptance.** Computer technology and digital evidence have not always been accepted by the judicial system. Without the court's extensive knowledge of all new technological developments, forensic investigators may have some trouble to introduce digital evidence. One control has been identified for this practical problem: awareness and education.

#### 4 CONCLUSION

Irrespective of the method of retrieval, investigators present the evidence to court. If the data are admissible in court, cyber investigators refer to it as forensically sound. Very few courts currently accept Live Forensic Acquisition as forensically sound due to the lack of court precedence and criminals' liking to exploit new technology in an innovative manner.

The development of the Live Forensic discipline and acquisition technique instigated the development of a method that allows forensically sound acquisition to stand fast in a court of law. The hypothesis of this paper is that forensic investigators using the *Liforac model* are likely to be more successful in a court of law. The application of this model is not a foolproof method to ensure that a case will be won in court, but rather a method to ensure that opposing counsel cannot argue forensically unsound methods and techniques.

The *Liforac model* is a comprehensive model that presents all aspects related to Live Forensic Acquisition, suggesting ways in which a



## A Best Practice Approach to Live Forensic Acquisition

Live Forensic Acquisition should take place to ensure forensic soundness. At the time of writing, this *Liforac model* is the first document of this nature that could be found for analysis. It serves as a foundation for future models that can refine the current processes.

### 5 REFERENCES

- Adelstein, F. & Richard, GG. 2007. *Live Forensics Tutorial. Part 2: Live Forensics*. Available from: [boanchanggo.tistory.com/attachment/hk360000000001.ppt](http://boanchanggo.tistory.com/attachment/hk360000000001.ppt) (Accessed 3 April 2009).
- Ciardhuáin, SO. 2004. An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*. Volume 3, Issue 1. Pp 1 - 22.
- Forte, DV. 2008. Volatile data vs. data at rest: the requirements of digital forensics. *Network Security*. Volume 2008, Issue 6. Pp 13 - 15.
- Haggerty, J. & Taylor, M. 2006. Managing corporate computer forensics. *Computer Fraud & Security*. Volume 2006, Issue 6. Pp 14 - 16.
- Jones, R. 2007. *Safer Live Forensic Acquisition*. University of Kent at Canterbury. Available from: <http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf> (Accessed 11 January 2008).
- Lectric Law Library. 2005. *The 'Lectric Law Library's Lexicon on Precedent*. Available from: <http://www.lectlaw.com/def2/p069.htm> (Accessed 30 October 2008).
- Maat, SM. 2004. *Cyber Crime: A Comparative Law Analysis*. University of South Africa. Available from: <http://etd.unisa.ac.za/ETD-db/theses/available/etd-08172005-103637/unrestricted/00front.pdf> (Accessed 14 January 2008).
- McDougal, M. 2006. *Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT)*. Available from: [http://www.foolmoon.net/downloads/Live\\_Forensics\\_Using\\_WFT.pdf](http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf) (Accessed 3 April 2009).
- Nare, S. 2008. Personal interview. 10 September 2008.
- Stimmel, CL. 2008. *Best Practices for Computer Forensics in the Field*. Available from: <http://ezinearticles.com/?Best-Practices-for-Computer-Forensics-in-the-Field&id=124243> (Accessed 10 January 2008).
- UMBC. 2008. What is an Information System (IS). *University of Maryland, Baltimore County*. Available from: <http://www.is.umbc.edu/aboutIS.asp> (Accessed 10 November 2008).

Proceedings of ISSA2009

US-CERT. 2007. *Quarterly trends and analysis report*. Available from:  
[http://www.us-cert.gov/press\\_room/trendsandanalysisQ107.pdf](http://www.us-cert.gov/press_room/trendsandanalysisQ107.pdf) (Accessed  
17 January 2008).



# HIGH-LEVEL INTEGRATED VIEW OF DIGITAL FORENSICS

CP Grobler<sup>1</sup>, CP Louwrens<sup>2</sup>

University of Johannesburg<sup>1</sup>

Nedbank SA<sup>2</sup>

[rsn@netactive.co.za](mailto:rsn@netactive.co.za)<sup>1</sup>

[buksl@nedbank.co.za](mailto:buksl@nedbank.co.za)<sup>2</sup>

## ABSTRACT

We are living in a world where there is an increasing need for evidence in organizations. Good digital evidence is becoming a business enabler. Very few organizations have the structures (management and infrastructure) in place to enable them to conduct cost effective, low-impact and efficient digital investigations (Sommer, 2005). Digital Forensics (DF) is a vehicle that organizations use to provide good and trustworthy evidence and processes.

The current DF frameworks concentrate on reactive investigations, with limited reference to DF readiness and live investigations. However, organisations use DF for other purposes. The paper proposes that DF consists of three components: Proactive (ProDF), Active (ActDF) and Reactive (ReDF). ProDF concentrates on DF readiness and the proactive, responsible use of DF to demonstrate good governance and enhance governance structures. ActDF consider the gathering of live evidence during an ongoing attack with limited live investigation and ReDF deals with the traditional DF investigation. The paper discusses each component and the relationship between the components.

Proceedings of ISSA 2009

**KEY WORDS:**

Digital forensics, Digital forensic readiness, Information Security governance, live investigations, Proactive Digital forensics, Active Digital Forensics, Reactive Digital Forensics

## HIGH-LEVEL INTEGRATED VIEW OF DF

### 1 INTRODUCTION

We are living in the knowledge age where information and knowledge is the most sought after commodity. Criminals, competitors and even employees exploit loopholes in current security architectures and control structures, use anti-forensic techniques and tools to hide their traces and apply forensic tools and techniques to obtain the required information to commit cyber crimes.

Organizations spend a lot of time, money, and effort in planning for incidents, natural disasters or security breaches by drafting incident response, disaster recovery and business continuity plans. These plans identify an incident and prescribe the best way to recover and continue with the business as quickly as possible. Very little thought is given to the identification and preservation of digital evidence and the correct structuring of processes for possible prosecution (Sommer, 1999).

Often, when asked for specific digital evidence, most organizations do not have all the evidence available (Clark, 2006). According to Sommer in the Guide to Investigations and Evidence (Sommer, 2005), most organizations underestimate the demand for digital evidence. Typically, evidence is required for fraudulent or disputed transactions; to support allegations of employee misbehaviour; to investigate suspected terrorism, to demonstrate due diligence with respect to good corporate governance, measuring legal and regulatory compliance; to avoid charges of negligence; to assist law enforcement and support insurance claims after a loss. This evidence is not only information stored, but can be logs generated by business processes, snapshots of systems, cell phone records, access control records etc. DF tools can retrieve the evidence required in a in a legally acceptable format and provide a chain of evidence and custody.

However, the nature of incidents and attacks has changed. Investigations need relevant, admissible live digital evidence for example volatile evidence (memory (RAM) content), swap files and network processes to determine the root-cause of an incident and to successfully prosecute the perpetrator. A famous example is the Code Red worm where

you can only conduct a 'live' investigation as the worm is memory resident and never writes to the disk. Many real-time systems cannot be powered down and investigations must be done on the live systems. Current DF investigation methodologies do not address the gathering of live evidence sufficiently.

There is a need for a comprehensive DF management framework (DFMF) that will

- Prepare organizations for DF investigations by the proactive identification and the availability of enough admissible evidence, and the restructuring of relevant processes to be forensically sound;
- Use DF tools and techniques to enhance governance frameworks in organizations;
- Gather and analyze live evidence during ongoing attacks; and
- Successfully investigate incidents to determine the root-cause of an incident and successfully prosecute a perpetrator.

The current DF models do not address the above-mentioned needs. The paper proposes a high-level framework that will consider 3 components, ProDF, ActDF and ReDF. The components will provide the backbone in the formulation of a comprehensive DFMF which is part of the broader study. The paper discuss the different components of DF by

- Defining and discussing the goals of ProDF;
- Defining and discussing the goals of ReDF,
- Defining and discussing the goals of ActDF; and
- Discuss how the different components interact to provide a high-level overview of DF.

The next part of the paper discusses ProDF.

## **2 PROACTIVE DIGITAL FORENSICS**

Being Proactive is defined as 'creating or controlling a situation rather than just responding to it' (Soanes C, 2005). ProDF, as discussed in this paper is the forensic preparation of an organization to ensure successful, cost effective digital investigations with minimal business activity disruption and ensuring that 'good' (admissible) evidence and sound processes are in place and available when needed for an investigation or during the normal flow of business.

## High-Level Integrated View of Digital Forensics

There are specific requirements per country, jurisdiction and industry for admissible evidence. The quality of evidence will determine the success of any investigation. The paper proposes a definition for Comprehensive Digital Evidence (CDE) *as digital evidence that will have evidentiary weight in a court of law and that contains all the evidence necessary (relevant and sufficient) to determine the root-cause of the incident, link the attacker to the incident and will result in a successful prosecution of the perpetrator*. The paper will use CDE to refer to evidence that meets the legal requirements to be admissible in a court of law.

From the literature studied, most of the current DF models include a ‘preparation’ or a ‘DF readiness’ step (Beebe & Clark, 2005; Casey, 2004; CP Louwrens et al., 2006; Rowlingson, 2004). DF readiness is defined as: *the ability of an organization to maximize its potential to use CDE evidence whilst minimizing the costs of an investigation- adapted from Rowlingson (Rowlingson, 2004)*.

However, organizations use DF in more areas. Nikkel (Nikkel, 2006) has identified external and internal drivers for the use of DF in organizations. External drivers are Legal and Regulatory requirements and best practices. Internal drivers are internal legal departments who need evidence after an incident; The ability to prove compliance e.g. legal compliance; The need for evidence by Human Resources for internal hearings; Risk management; The IT department to investigate e.g. security breaches or equipment misuse; The use of DF tools for non-forensic purposes e.g. password retrieval and disk recovery; and Continuous auditing by the internal audit department.

The paper propose a definition for Proactive DF *as the proactive restructuring and defining of processes, procedures and technologies to create, collect, preserve and manage CDE to facilitate a successful, cost effective investigation, with minimal disruption of business activities whilst demonstrating good corporate governance*.

The authors have identified the following goals for ProDF:

- Become DF ready;

Proceedings of ISSA 2009

- Enhance the Governance programs (IT and IS) of the organization by proving (assessing) the effectiveness of controls, measured against IT and IS objectives (related to business objectives);
- Improve IS / IT performance with the responsible use of DF tools to improve effectiveness and efficiency in organization;

The next part of the paper will briefly discuss each goal.

## 2.1 Become DF Ready

After comparing different viewpoints of DF readiness and preparation phases, the paper has identified the following goals for DF readiness (Beebe & Clark, 2005; CP Louwrens et al., 2006; Garcia, 2005; Rowlingson, 2004):

- *Provide and prepare the infrastructure* (systems and networks) to support DF investigations;
- *Develop an evidence management plan (EMP)* that will concentrate on the identification, legal gathering, preservation, handling, retrieving, retention and archiving of CDE. The EMP must include the construction of a digital evidence map that will contain all the information about the evidence i.e. category, location, retention time, reference procedures to collect and retrieve evidence, regulatory collection requirements (Casey, 2007); and the development of evidence management policies and procedures e.g. policy for secure storage, acquiring, preservation and handling of evidence, secure evidence policy and evidence transport;
- *Augment organizational risk mitigation plans* for example include evidence and process requirements in risk assessment, incident response, business impact analysis, business continuity and disaster recovery plans by linking the evidence requirement to the digital evidence map to determine the completeness and admissibility of the evidence; Implement an Intrusion Detection System (IDS) with active monitoring capabilities and define trigger events for ActDF investigations; Prepare for containments of incidents to include containment on live systems.
- *Develop a DF training and awareness strategy* with education, training and awareness programmes for organization;
- *Develop a management capability* that will define the management structure that will outline the internal and external DF investigators

and the role and responsibilities of the Computer Emergency Response Team (CERT);

- *Document and validate a DF investigation (DFI) protocol* against best-practice;
- To allow an *investigation to proceed at a cost* in proportion to the incident;
- To *minimize interruption* to the business from any investigation;

**2.2 Enhance the Governance programs (IT and IS) of the organization by proving (assessing) the effectiveness of controls, measured against IT and IS objectives (related to business objectives).**

Corporate Governance reports and legislation, for example: Sarbanes-Oxley (*Sarbanes-Oxley Act*, 2002) and King 2 (*King II Report on Corporate Governance*, 2003) states that management is responsible and accountable for the IT infrastructure, applications and information of the organization. King 2 states that the board must ensure ‘that a systematic, documented assessment of the processes and outcomes surrounding key risks is undertaken’ (*King II Report on Corporate Governance*, 2003).

DF tools can be utilized to assess the controls implemented; the DF investigation process followed can provide the documented proof of the assessment. Management can then provide reasonable assurance and documentation to prove due diligence. The effective utilization of DF tools and techniques can enable management to enhance the governance structures of the organization by providing evidence to measure performance or compliance. DF readiness as defined concentrates on evidence availability and preservation and does not provide for assessment of controls.

Organization should manage the implementation and use of DF. The board must include DF in the management structure of the organization by assigning a position with responsibility and authority to a person. It must also clearly stipulate the relationship (and segregation of duties) between the DF team, Information Security, Risk Management, Internal Audit and Legal departments.

### **2.3 Improve IS / IT performance with the responsible use of DF tools to improve effectiveness and efficiency in organization;**

It is essential to design, configure, and implement systems and processes in such a way to enable DF in the organization for example to design DF friendly file structures. The responsible use of DF tools and techniques can be used to improve the effectiveness of IT systems for example disk data recovery. The CSI 2008 computer (Richardson, 2008) indicates that 41% of respondents use DF tools and techniques as part of their security suite,

However, controls must be in place to prevent the unauthorized use of DF tools for example the use of password crackers and anti-forensic activities for example data destruction, manipulation and data hiding.

ProDF will therefore address the need to prepare organizations for DF investigations by being DF ready, and the responsible application of DF tools and techniques to enhance governance frameworks in organizations. The next part of the paper discusses ReDF.

## **3 REACTIVE DIGITAL FORENSICS**

No organization is fully prepared for incidents. ReDF as defined by this paper concentrates on the traditional DF investigation that will take place after an incident has been detected. Should an incident occur, there should be an acceptable proven DF investigation protocol in place as specified by ProDF on how to conduct the investigation (CP Louwrens et al., 2006). The goals of ReDF are to:

- determine the root-cause of the incident;
- link the perpetrator to the incident;
- minimize the impact of an incident; and
- successfully investigate an incident;

The paper defines *Reactive DF as the analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of digital media which is digitally stored or encoded for evidentiary and/ or root-cause analysis and the presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents.*

The authors have studied various DF methodologies or investigation protocols from literature and propose that the following phases with steps that should be included in the DF investigation protocol of an



organization: (Barayumureeba & Tushabe, 2004; Beebe & Clark, 2005; Carrier, B & Spafford, 2003; Casey, 2004; Ciardhuain, 2004; CP Louwrens et al., 2006; Forrester & Irwin, 2007; Rowlingson, 2004).

### **3.1 Phase 1: Incident response and confirmation.**

This phase includes the following steps: Detect an Incident / activity; Report the incident; Determine the assessment of worth (Validate incident Assess damage / impact), Incident Confirmation; Formulate a hypothesis; Obtain an authorisation – internal and external; Determine a containment strategy; Formulate an Investigation plan; Coordinate the resources; Accelerate the investigation; Notification of the investigation – *determine the relevance*.

### **3.2 Phase 2: Physical Investigation (if relevant)**

Although it is a DF investigation, it is essential to include the physical crime scene to gather as much evidence as possible to ensure a successful investigation. Steps include to Secure the physical crime scene; Survey of crime scene for potential evidence; Search and collect (secure hardware, secure transport); Documentation (label and seal all evidence); Acquire the evidence; Analyze the evidence; Identify possible digital evidence – to be sent to Digital investigation team; Reconstruct the event; Make a finding; Transport the evidence; and Store the evidence.

### **3.3 Phase 3: Digital Investigation**

During this phase the actual digital investigation will start. The steps followed during this phase are essential and will determine the success of the investigation. The steps are:

#### **3.3.1 Evidence acquisition**

This step includes Identification and seizure of evidence; Collection of evidence; Acquire the relevant evidence (recovery, harvesting, reduction) – if live evidence is required, activate the ActDF component; Ensure integrity (Preservation / forensic copy, Competent people, Secure evidence); Authenticate – timestamp; Transport of the evidence; Storage of the evidence; and Document the acquisition process.

### **3.3.2 Analysis**

The investigative team will Revisit the investigation plan; Review the relevance of tools and expertise available; Develop a hypothesis; Analyze the evidence (Examine evidence – best evidence, Assess the evidence – means motivation and opportunity, Experimentation); Test the hypothesis (apply fusion and correlation); Reconstruct the event; Make a finding; Validate the results of analysis; Document the case; and Secure the documentation.

### **3.3.3 Service restoration**

During this phase, the intention is to restore systems as fast as possible if necessary by interacting with information security risk management team to restore services ASAP;

### **3.4 Phase 4: Incident reconstruction**

During this phase the investigation team will Consolidate physical investigation (phase 2) and digital investigation (phase 3) findings. If, during the reconstruction process, the investigation team identify missing evidence to support the hypothesis; phase 2 and / or 3 may be repeated to obtain the evidence. The final outcome of this phase will be a well documented report with supporting CDE that support the hypothesis.

### **3.5 Phase 5: Present findings to Management / authorities.**

The investigation team will prepare the case by Considering the legal jurisdiction location requirements; Incorporate the timeline of the entire case; Determine the target audience; Prepare expert witness; Prepare exhibits; Use appropriate presentation aids; and Preserve the chain of custody. Present the case and preserve the evidence. The protocol must also provide an appeal process.

### **3.6 Phase 7: Dissemination of result of P/H / Incident closure**

It is essential to review the outcome of the case to identify and apply lessons learned. Finally depending on the policies and requirements all evidence must be preserved, returned or disposed.

The phases as identified in this section seem to be a waterfall framework with some repetition if needed between the different phases. ReDF as discussed meet the need to investigate incidents to determine the

root-cause of an incident and successfully prosecute a perpetrator. The next part of the paper will briefly discuss ActDF.

#### **4 ACTIVE DIGITAL FORENSICS**

When an incident occurs, the Intrusion Detection System (IDS) of an organization will detect it and the Incident Response (IR) protocol of the organization will be activated. It is however becoming essential to integrate live forensic investigation protocols with the IR protocol to ensure that relevant and admissible live CDE is available if required for investigatory purposes. IR protocols do not consider the importance of evidence identification, gathering and preservation of live data (Sommer, 1999).

Various tools and methodologies exist to conduct live investigations, but as it is a new field, it faces numerous challenges. According to Ioeng and Leung (Ioeng & Leung, 2007) live forensic investigations are hampered due to missing definitions of live forensics; the absence of standard procedures in live investigations; and the certification and affectation of live evidence.

Traditional ReDF investigation methodologies will ensure that no changes are made to the evidence and the seized content. Live investigators uses software tools that make unavoidable changes to data acquired, the live investigative process must be documented in a forensic sound manner to maintain the chain of custody, so that the evidence gathered will be admissible in a court of law.

Live analysis is often associated with incident response and intrusion detection systems, but is auxiliary to the IS programs. Virus software is an example of a live analysis tool. Most of the live investigation tools and techniques are software based, however current research is considering the use of hardware devices to acquire evidence (Carrier, BD & Grand, 2004).

Live forensic investigations are currently being done by using remote forensic preservation and acquisition tools, e.g. EnCase Enterprise edition and ProDiscover (Casey & Stanley, 2004). These tools use live analysis techniques that will use software that pre-exist on the system during the timeframe being investigated (Carrier, Brian, 2006). The target machine is monitored from a remote site data can be acquired in a forensic

sound way by the aid of a tool. Typical activities include keyword searches, copying and extraction of files and records from the live remote site. The user is not aware of the process and an investigation can continue without him being aware of it. The investigator can acquire evidence in a live production environment. Remote forensic investigations focus more in transforming ReDF examination procedures onto live, production environments.

The investigator can also use network forensics to identify sources of live network evidence. It is not possible to log all activities on a network, but it is essential that during a live investigation to identify potential sources for example DNS and whois servers, websites, ftp servers, local Ethernet servers, Bluetooth piconets, database servers, chat servers, network routing tables or reply messages of SOAP servlets (Nikkel, 2005). Evidence that can be gathered is for example slanderous web pages, illegal files, traffic from port scans, routing tables, wireless signal strength and direction.

Other software techniques identified by Carrier et al. (Carrier, BD & Grand, 2004) to gather live evidence include virtual machines, physical memory devices, hibernation and process pseudo files. All of the above techniques are software-based and rely on the operating system, but the operating system kernel is not a trusted resource as it can have a malicious kernel. This poses a threat to the reliability of the evidence. A second problem is that the operating system must execute a command and therefore will have to write to memory and therefore destroy evidence in the process.

Carrier et al. (Carrier, BD & Grand, 2004) has proposed a hardware based memory acquisition procedure. They propose the use of a hardware expansion card pre-installed in a PCI bus that will gather volatile evidence and write it to external storage device.

The rationale of the various techniques differs as remote online forensic investigations capture data disregarding the order of volatility (Jeong & Leung, 2007). The other live investigation techniques will consider the order of volatility of the evidence.

The authors have studied current 'live or remote or real time' methodologies and propose to include current live forensic tools and

techniques, real time investigations as well as remote investigations as part of ActDF (Foster M, 2004; Jeong & Leung, 2007; Payer, 2004; Ren & Jin, 2005). There are no or very limited methodologies for ActDF investigations.

The paper proposes the following definition for ActDF: *Active DF is the ability of an organization to gather (identify, collect and preserve) CDE in a live environment to facilitate a successful investigation.*

The goals for ActDF are:

- Collect relevant live CDE (including volatile evidence) on a live system or production environment by using appropriate tools and technologies;
- Minimize the effect and impact of an ongoing incident; and
- Provide a meaningful starting point for a reactive investigation within the parameters of the risk control framework of the organization.

The paper identified the following phases for ActDF from the literature (Foster M, 2004; Jeong & Leung, 2007; Payer, 2004; Ren & Jin, 2005). It is essential to apply relevant incident / crime scene protocols (Casey, 2004) e.g. consider physical crime scene investigation requirements not to destroy any evidence. From literature studied, some of the current frameworks depend on the technology used. The authors formulated the following phases independent of any tool or technology:

#### **4.1 Phase 1: Incident response and confirmation.**

The investigator must adhere to the defined steps for this phase as specified by ReDF, but must determine which volatile or live evidence must be acquired to successfully investigate incident as it is prescribed by the ProDF component or potential missing evidence for new or unknown incidents; Formulate ActDF investigation plan; If risk management policies allow it continue with ActDF investigation, otherwise start the reactive investigation. There may also be a pre-defined trigger event to start active monitoring or other procedures as soon as an incident alert is activated. As ActDF deals with ongoing or real time incidents the containment strategy and plan is very important because the systems will remain live and may not be powered down.

#### **4.2 Phase 2: ActDF investigation.**

**Evidence acquisition** - (phase 3 of ReDF applies). Collect additional live evidence lacking from, or required by the CDE map using appropriate tools, technologies, or applications that will be required to profile the attacker, gather volatile evidence or to determine the source of the attack. Secure and authenticate all the extracted data by hashing immediately after collection process to preserve before analysis. It is essential to document all actions performed to prove that chain of custody of the evidence acquired was maintained.

It is important to automate and activate the appropriate evidence collection tools, technology or applications as soon as possible (Can be immediately after an incident alert has been issued). Jeong et.al suggests to: Impose minimal user intervention; Ensure that all actions performed are necessary and least intrusive; Ensure minimal modification of static digital evidence; Data acquisition should follow the order of volatility and priority of digital evidence collection; Acquire non-priority or volatile evidence through traditional evidence collection ; and Copy or extraction of data should only be performed when original data and timestamp is not affected (Jeong & Leung, 2007).

**Analysis** (phase 3 of ReDF applies). Analyze preliminary evidence to determine if sufficient evidence has been gathered to reconstruct the incident and to support the initial hypothesis; Document all activities at all times to ensure the integrity of all evidence; Maintain the chain of evidence and custody; and Validate the processes at all times during the Active DF evidence investigation phase. It is important to ensure the reliability and admissibility of the results.

#### **4.3 Phase 3: Event reconstruction.**

This phase uses the results from the analysis step to do a limited reconstruction of the incident. The aim is to determine if the missing or live required evidence has been acquired to determine when to terminate active DF investigation. The termination conditions will be prescribed by the Risk management framework for example cost too high, enough CDE, impact reassessed etc. Repeat phase 2 if live evidence is still lacking.

#### **4.4 Phase 4: ActDF termination.**

If sufficient evidence has been gathered or the investigation is terminated due to other reasons, the investigators will prepare documented case files with CDE for the reactive investigation team to complete investigation. As soon as the ActDF investigation is terminated, the reactive component will continue to analyze and reconstruct the incident using all evidence (including static CDE or physical evidence) required to conclude the investigation.

The ActDF component meets the need to gather live evidence during ongoing attacks. The next part of the paper will discuss the relationship between the different components of DF to demonstrate the dependency between the components.

### **5 RELATIONSHIP BETWEEN PRODF, REDF AND ACTDF.**

Using the definitions and goals of ProDF, ReDF and ActDF it is clear that the different components of DF are dependent on each another. Both active and reactive investigations depend heavily on the quality and availability of CDE, the soundness of processes, education level of investigators and staff and the availability of acceptable tools and technologies which is determined by ProDF component.

To demonstrate the relationship figure 1 depicts the typical flow of activities once an incident alert is issued by the IDS of the organization.

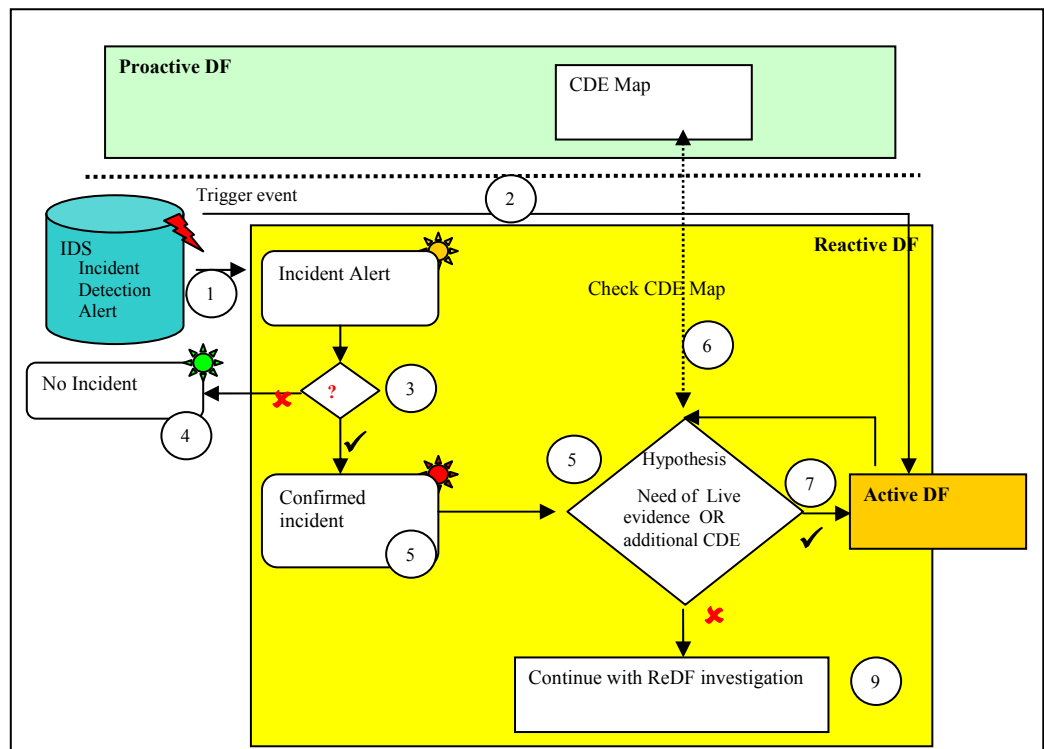
The incident alert or accusation (1) is the starting point of an investigation; Organizations can define a trigger event (2) that will start live data acquisitions as soon as certain types of incidents alerts are detected. The next step is to determine the assessment of worth (3) – to determine if the suspicious activity is an incident (Consider if it is intentional, criminal, or determine the reliability of the source of the alert and the potential impact of incident). The result of the assessment of worth step will determine the next step in the process as it will determine the whether to investigate or not. These two steps will always take place after any suspicious activity. The result of the two steps will be either ‘no incident’ (4) or ‘incident confirmation’ (5).

After an incident has been confirmed, a hypothesis will be set. It is then important to determine if sufficient evidence exist to investigate the

incident (6). To determine if there is sufficient evidence, the investigator must consult the digital evidence map of the organization (7), as well as the risk profiles and risk profile case scenarios.

If there is not sufficient evidence or the need for live evidence, ActDF must start (8), otherwise the ReDF component will be activated (9).

Once the investigator is satisfied that sufficient evidence exist, the ActDF component is terminated and the ReDF component will be activated (9).



*Figure 1: Relationship between DF components*

The three components ProDF, ActDF and ReDF address all the needs for a DFMF as identified in paragraph 1 of the paper. The authors will use the 3 components to propose a DF management model manage



and implement DF in an organization by investigating what is required in terms of *PROCESS* (What, Where, How, When), *POLICIES* required (What, Where, How, When, Why), *PEOPLE* (Who), *GOVERNANCE* (Why, How), *LEGAL* and *JUDICIARY* (Why, How) and *TECHNOLOGY* (How, Where). This model will be discussed in another paper.

## 6 CONCLUSION

Current DF frameworks do not cover all applications DF as discussed in this paper, but concentrate on digital investigations. The paper has proposed an integrated view of DF containing three components: ProDF, ReDF and ActDF.

The ProDF component deals with DF readiness i.e. the preparation of the organization for all known incidents to ensure that the required CDE is available to investigate an incident successfully. Staff will be trained and IR processes, policies and procedures will exist to guide next step should an incident occur. Proper management structures should be in place to prescribe who will be responsible for what and when in the organization.

ProDF also propose the responsible use of DF tools and techniques for other purposes than investigations for example assessment of controls and availability of evidence to prove due diligence with respect to good corporate governance and to enhance governance frameworks.

ReDF is the traditional DF investigation after an incident has been detected. It will use all CDE available to determine the root-cause of the incident, reconstruct the incident and prepare a case for prosecution in a court of law or internal hearing. After an incident is confirmed and live evidence is required or if it is an ongoing attack, the ActDF component will be activated.

The ActDF component will deal with the gathering of live evidence in a real time, or in a live environment. It is not a complete investigation, but will only gather required live evidence or missing evidence required and then hand the evidence and documentation over to the ReDF component to complete the investigation.

The paper has discussed the relationship between the different components. The successful implementation of ProDF will provide a solid

foundation for the implementation of DF in organisation. ReDF and ActDF concentrate on providing an acceptable protocol to ensure successful investigations.

## 7 REFERENCES

- Barayumureeba, V & Tushabe, F 2004, 'The enhanced digital investigation process model', paper presented to DFRWS 2004.
- Beebe, N & Clark, J 2005, 'A hierarchical, objectives-based framework for the digital investigations process ', *Digital Investigation, Elsevier*, vol. 2, pp. 147-67.
- Carrier, B 2006, 'Risks of live Digital Forensic analysis', *Communications of the ACM*, vol. 49, no. 2, pp. 56 - 61.
- Carrier, B & Spafford, E 2003, 'Getting physical with the digital investigation process', *International journal of Digital Evidence*, vol. 2, no. 2.
- Carrier, BD & Grand, J 2004, 'A Hardware-Based Memory Acquisition Procedure for Digital Investigations', *Digital Investigation Journal*, no. 1(1).
- Casey, E 2007, 'Digital Evidence maps - A sign of the times', *Digital Investigation, Elsevier*, vol. 4, no. , pp. 1-2.
- Casey, E 2004, *Digital Evidence and Computer Crime*, 2nd ed, Elsevier Academic Press.
- Casey, E & Stanley, A 2004, 'Tool review - remote forensic preservation and examination tools', *Digital Investigation*, vol. 1, pp. 284-97.
- Ciardhuain, SO 2004, 'AN extended model of cybercrime investigations', *International journal of Digital Evidence*, vol. 3, no. 1.
- Clark, A 2006, 'Are you ready for Forensics?' <<http://www.inforenz.com/press/20060223>>.
- CP Louwrens, S vonSolms, C Reeckie & Grobler, T 2006, 'A control Framework for Digital Forensics', paper presented to IFIP11.9 International Conference on Digital Forensics, Orlando Florida.
- Forrester, J & Irwin, B 2007, 'A Digital Forensic investigative model for business organisations', paper presented to IFIPSec 2007, Sandton.
- Foster M, WJ 2004, 'Process Forensics: A pilot study on the use of checkpointing technology in computer forensics', *International journal of Digital Evidence*, vol. 3, no. 1.
- Garcia, J 2005, 'Proactive and Reactive Forensics', viewed 5 September 2005,

## High-Level Integrated View of Digital Forensics

- <[http://rediris.es/cert/doc/reuniones/af05/proactive\\_n\\_reactive\\_forensics.pdf](http://rediris.es/cert/doc/reuniones/af05/proactive_n_reactive_forensics.pdf)>.
- Ieong, R & Leung, H 2007, 'Deriving Cse-specific Live Forensics Investigation Procedures from FORZA', paper presented to Symposium on Applied Computing archive  
Proceedings of the 2007 ACM symposium on Applied computing Seoul, Korea, 2007.
- King II Report on Corporate Governance*, 2003.
- Nikkel, BJ 2005, 'Generalizing sources of live network evidence', *Digital Investigation*, vol. 2, no. 3, pp. 193-200.
- Nikkel, BJ 2006, 'The Role of Digital Forensics within a Corporate Organization', paper presented to May 2006, IBSA Conference, Vienna.
- Payer, U 2004, 'Realtime Intrusion-Forensics A proptotype implementation', paper presented to Terena Networking conference.
- Ren, W & Jin, H 2005, 'Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation', paper presented to 2005 ACM Symposium on Applied Computing, Santa Fe, New Mexico, USA., March 13-17, 2005,.
- Richardson, R 2008, *CSI Computer Crime & Security Survey*, CSI.
- Rowlingson, R 2004, 'A ten step Process for Forensic Readiness', *International journal of Digital Evidence*, vol. 2, no. 3.
- Sarbanes-Oxley Act*, 2002, USA, <[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_bills&docid=f:h3763enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf)>.
- Soanes C, HS 2005, *Oxford Dictionary*, 3 edn, Oxford University press, 10: 0-19-861022-X, <<http://www.askoxford.com/dictionaries/?view=uk>>.
- Sommer, P 1999, 'Intrusion Detection Systems as Evidence', *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. Volume 31 , , no. I23-24 (December 1999), pp. 2477 - 87
- Sommer, P 2005, 'Directors and Corporate Advisors' Guide to Digital Investigations and Evidence', *Information Assurance Advisory Council*, viewed 3 June 2007, <<http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf>>.

Proceedings of ISSA 2009

The Design of a Wireless Forensic Readiness Model (WFRM)

## **THE DESIGN OF A WIRELESS FORENSIC READINESS MODEL (WFRM)**

**SJ Ngobeni<sup>1</sup> and HS Venter<sup>2</sup>**

Information and Computer Security Architecture Research Group (ICSA),  
University of Pretoria, Pretoria, South Africa

<sup>1</sup>sngobeni@csir.co.za, 012 841 4410

<sup>2</sup>hventer@cs.up.ac.za, 012 420 3654

### **ABSTRACT**

The proliferation of wireless mobile communication technology has emerged and this has resulted in the increase of the wireless users. On the other hand, cyber crime in WLANs has appeared to be gradually increasing world wide. Wireless network forensics is seen as not only a counterproposal but as a solution to the rapid increase of cyber crime in WLANs. However, the key issues impacting wireless network forensics are, firstly, it is an enormous challenge to monitor and collect all the communications generated by the communicating mobile devices and conduct a proper digital forensic investigation. Secondly, network traffic only exists for split seconds, and because of its large volume, it may be retained for a limited time before storage space is depleted. Therefore this suggests that WLANs are not forensically ready to gather enough evidence that can be used for subsequent forensic purposes. In an attempt to address this issue, this paper proposes a Wireless Forensic Readiness Model (WFRM) with the capabilities of monitoring, preserving and analysing wireless network traffic.

### **KEY WORDS**

WLANs, forensic readiness, traffic, Access Point

## **THE DESIGN OF A WIRELESS FORENSIC READINESS MODEL (WFRM)**

### **1 INTRODUCTION**

The proliferation of mobile devices that connect to Wireless Local Area Networks (WLANs) has ushered in an era of pervasive computing [1]. The most important function of a WLAN is to provide wireless broadband connectivity at public locations like airports, railway stations, conference centres and hotels. The high broadband connectivity allows people to access and share services like data, voice and video through their mobile devices. However, cyber criminals are always making it their mission to access these services in an unauthorised way and pilfer valuable information.

Investigative techniques, forensic tools and network-based forensic techniques have rapidly evolved to track down the rapid increase in cyber crime [2]. However, one of the most noteworthy challenges of investigating criminal activity in a WLAN environment is obtaining all necessary evidence related to the crime [1]. This challenge is as a result of the fact that, firstly, all devices participating in a WLAN environment are mobile. This suggests that they are not always connected to the network; therefore it becomes difficult to monitor and collect information about the communications generated by these devices and investigate it. Secondly, network traffic only exists for split seconds, and because of its large volume, it may be retained only for a limited time before storage space is depleted. It stands to a reason, therefore, that WLANs are not forensically ready to gather enough evidence that can be used for subsequent forensic purposes.

To attend to this problem, this study proposes a Wireless Forensic Readiness Model (WFRM) with the capability of monitoring, preserving and analysing wireless network traffic in order to come up with credible evidence that can associate a security breach with a suspected mobile device. The concept of wireless forensic readiness arose in this study as a recommendation for improving the efficiency of a digital forensic investigation [3]. Further explanation on digital forensic readiness is provided in the background section of this paper. Traffic monitoring in a

## The Design of a Wireless Forensic Readiness Model (WFRM)

wireless network is mandated by law in many countries [5]. The most significant function of the proposed model is to monitor wireless network traffic and log information about this traffic for later analysis in case a security breach has occurred and a digital forensic investigation is warranted. For the purpose of the proposed model, all traffic that passes through the Access Points (APs) will be intercepted.

The remainder of this paper is structured as follows: Section 2 provides background information about WLANs, the digital forensic processes and digital forensic readiness. This paper proceeds to present the proposed model in Section 3. How the model is integrated and a discussion thereof is presented in Section 4. Section 5 concludes the paper and discusses future work.

## 2 BACKGROUND

This section discusses some background concepts regarding WLANs, digital forensic processes and digital forensic readiness. Each concept is described in a separate section, starting with a definition of the concept, followed by its challenges, and finally its role in the proposed model.

### 2.1 Wireless Local Area Networks

By definition, a Wireless Local Area Network (WLAN) is a network that links two or more computers without any physical connection [6]. The lack of physical connection between wireless networks makes it discreet, since its participating mobile devices are potentially far removed. This is indeed an issue to be considered when evidence is identified and collected within a digital forensic investigation that may involve wireless traffic. When a digital forensic investigation is conducted, the lack of physical connection between communicating wireless devices may cause the identification of such devices to be problematic. There is consequently a good chance that some of these devices may be left undiscovered [7]. WLANs utilise spread spectrum technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broader coverage, for example WiMAX, GPRS/HSDPA, and still be connected to the network [8].

For home users, wireless networks have become popular owing to ease of installation and location freedom that results from the increased popularity of laptops and PDAs. For business, public businesses such as coffee shops and malls have begun to offer wireless access to their customers. Some services are even provided free of charge. Large wireless network projects are set up in many major cities. For instance, Google is providing a free service to Mountain View in the US, and California has entered a bid to do the same for San Francisco. New York City has also launched a pilot programme to cover all five municipalities of the city with wireless Internet access [8]. In South Africa, a number of soccer fields are currently being constructed for the 2010 Soccer World Cup. A large number of people will be attracted internationally to come and watch the 2010 World Cup games. Therefore, it is planned that wireless networks be deployed at these soccer stadiums so that people will be able to access and share services like voice, video and data through their mobile devices while watching a soccer match.

As WLANs are more widely deployed, wireless security is becoming a serious concern for an increasing number of organisations [9]. It is therefore essential that a forensic readiness mechanism with the capability to combat the unrelenting increase of cyber crime should be put in place without any further delay.

## **2.2 Forensic readiness**

Digital forensic readiness claims that the effort to perform a digital forensic investigation should decrease while at the same time maintaining the level of credibility for the digital evidence being collected [4]. The decrease in effort referred to here is the time and cost required for an incident response during a digital forensic investigation. For example, if an organisation is forensically prepared, then there will be no huge difference between the amount of time spent by the intruder to launch the attack and the amount of time required by the cyber forensic experts to respond to the attack. In general, reducing the time to respond to an incident during a digital forensic investigation will definitely reduce the cost required to respond to that particular incident.



## The Design of a Wireless Forensic Readiness Model (WFRM)

Dave Dittrich [10] – head of the honeynet project – discusses an incident that took an intruder a period of about two hours to launch an attack, but it took the cyber forensic experts a period of about 40 billable hours to respond to that incident. The reason why it took so long to respond to this incident is that, the organisation that was investigated was not forensically prepared for any such incident. This paper therefore claims that organisations, which deploy WLANs that are of high risk to cyber attack, should be forensically ready to collect any digital evidence in advance so that, in the event of a crime being committed over a WLAN, such collected data is ready to be used for subsequent digital forensic investigations.

### 2.3 Digital forensic process

A digital forensic process is defined as a procedure that is followed to investigate a particular digital criminal activity and that procedure must be acceptable in a court of law [11]. Digital forensics is hard work; therefore the cyber forensic experts need some tools to assist them in conducting the digital forensic investigation. Every digital forensic investigation need to follow the digital forensic process. The following phases represent the general digital forensic process [11]:

1. Define the scope and goals of the investigation
2. Determine the work and materials
3. Acquire images of the devices to be examined
4. Perform the digital forensic analysis
5. Prepare the report

The most popular tools used in digital forensic investigations are Encase [14] and FTK [15]. The phases of the digital forensic process for Encase include preview, imaging or acquisition, verification, recovery and analysis, and restoration, while the phases of the digital forensic process for FTK include detection, identification, analysing, preservation and reporting. Table 1 present a comparison between the phases of Encase, FTK and the phases of the model proposed in this paper, called the Wireless Forensic Readiness Model (WFRM).

*Table 1. Digital forensic phases for the FTK, Encase and WFRM*

<b>Digital forensic process</b>		
<b>Encase</b>	<b>FTK</b>	<b>WFRM</b>
1. Preview	1. Detection	1. Monitoring
2. Imaging/Acquisition	2. Identification	2. Logging
3. Verification	3. Analysis	3. Preservation
4. Recovery and analysis	4. Preservation	4. Analysis
5. Restoration	5. Reporting	5. Reporting
6. Archiving		

Table 1 indicates that only the analysis phase of the digital forensic process is common to Encase, FTK and the WFRM model. Both the preservation and analysis phases are common to the FTK and the proposed model. However, it is worth noting that the digital forensic process for FTK and Encase is more or less the same when relating them to the general digital forensic process. This also suggests that the phases of the digital forensic tools also co-relate although they are named differently. The reason for the inconsistent naming of the phases between the various tools is because the digital forensic process has not been standardised yet. The digital forensic process, however, as taken from [11], is one that the authors assume as an acceptable general digital forensic process as used in this paper.

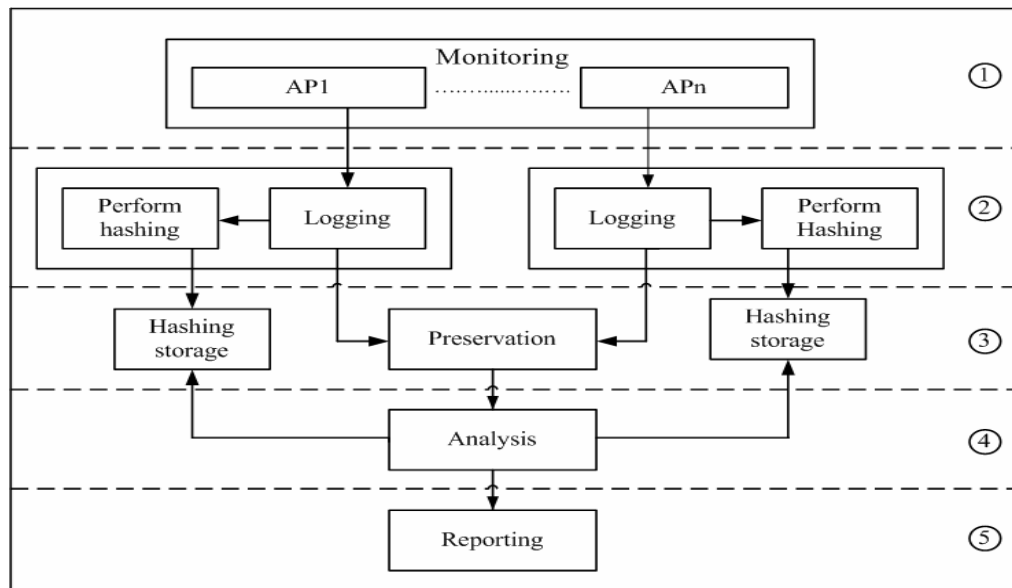
### **3 THE COMPONENTS OF THE PROPOSED MODEL**

This section presents the Wireless Forensic Readiness Model (WFRM). This section starts by presenting an overview of the WFRM as a black-box. This is followed by a detailed discussion of the components that constitute the proposed model. Lastly the proposed model and all its components are presented. The complete depiction of the WFRM appears in Figure 6, but its components are discussed in separate sections below.

## The Design of a Wireless Forensic Readiness Model (WFRM)

### 3.1 Overview of the WFRM

The principal concept addressed by the WFRM is that it monitors wireless network traffic from various Access Points (APs). The monitored traffic is logged in a log file, and then preserved to maintain its integrity. Thus the information needed by the cyber forensic experts is rendered readily available should it be necessary to conduct a digital forensic investigation. The availability of this digital information may maximise chances of using it as evidence and reduce the cost of conducting the entire digital forensic investigation. This is because a part of the digital forensic process (i.e. the monitoring, logging and preservation) has already been conducted. Figure 1 indicates a block diagram of the WFRM. The block diagram shows how the components of the model interact with each other. The shaded area in the block diagrams from Figure 2 up to Figure 5 represents the component that is described in each particular subsection that follows.



*Figure 1. A block diagram for the WFRM*

The numbers from 1 to 5, represented with circles in figure 1, demonstrates the phases of the digital forensic process of the WFRM as shown in Table 1. Number 1 represent the monitoring phase, number 2

represents the logging phase, number 3 represents the preservation phase, number 4 represents the analysis phase and number 5 represents the reporting phase.

### 3.2 Traffic monitoring

Figure 2 demonstrates the traffic monitoring component whereby Mobile Devices (MDs) are connected to a WLAN through various Access Points (APs). This can be denoted by  $AP_i = \{AP_1, AP_2, AP_3, \dots, AP_n\}$ ; where  $AP_i$  denotes a set of APs from  $AP_1$  up to  $AP_n$ . In general, there can be many APs in a single WLAN environment. Each AP monitors all the traffic generated by the MDs, which connects to each AP. For security purposes, the monitoring component uses a firewall to filter both inbound and outbound wireless traffic. Filtering is defined as the process of controlling access to the WLAN by examining all the packets based on the content of their headers. However, a firewall can not detect all the misconduct of the WLAN since some other MDs may obscure their identities and will appear as if they are legitimate users of the network – therefore the proposed model employs another component called the Capture Unit (CU) that logs all the monitored traffic. The CU is discussed in detail in the next section.

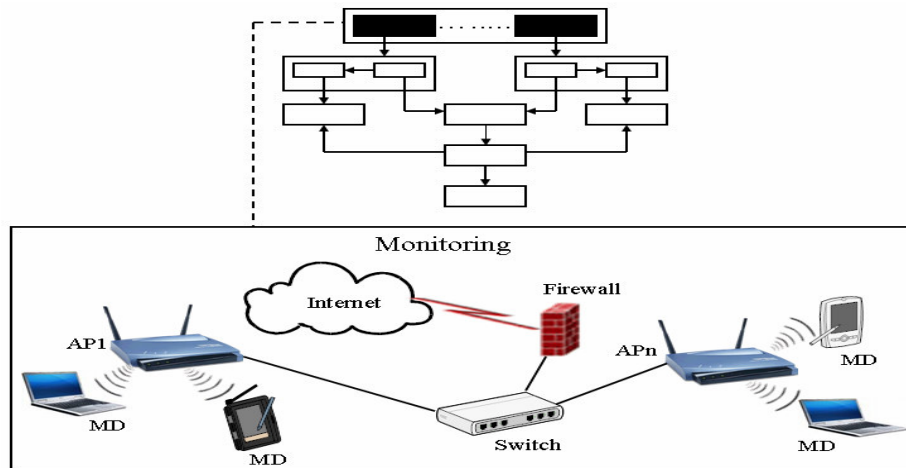
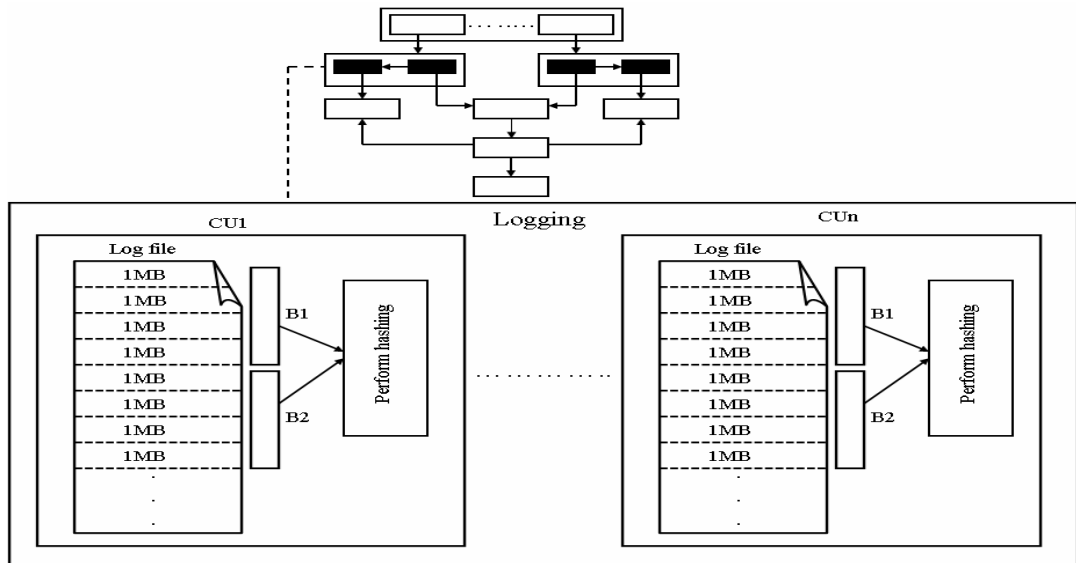


Figure 2. Traffic monitoring component

## The Design of a Wireless Forensic Readiness Model (WFRM)

### 3.3 Logging

The CU component logs all the traffic monitored by the APs. Each AP has its own associated CU that logs the traffic passing through the AP. The CU logs the traffic in a log file as represented in figure 3. The log file is divided into separate storage areas with each storage area consisting of, for example, 1 Megabyte (1MB) of data. As traffic is being monitored from the AP and stored in a log file, the storage area of the log file becomes limited. Therefore, this component creates a block of data per several MBs, i.e. B1 in Figure 3 represents a block of data consisting of 4MBs, for example. A block is a fixed-size unit of data that is transferred together to permanent storage space, as described in the next section. For the purpose of this model, the logged traffic is the packets. Therefore, whenever this study refers to ‘traffic’, it means all the packets passing through the APs. Finally, the CU then send the accumulated blocks of data to the Evidence Store (ES) for analysis purposes and creates a hash per each block of data that is sent to the hashing storage for preservation purposes, as explained in the next section.



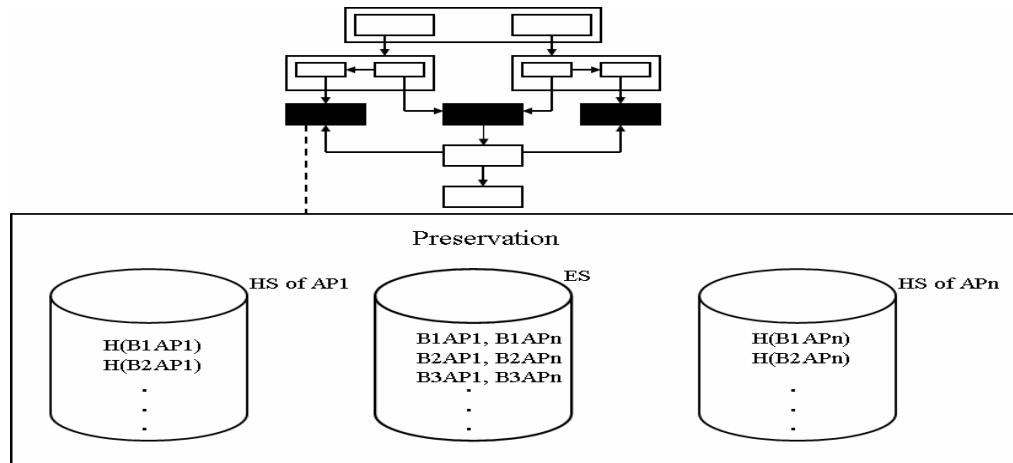
*Figure 3. Logging component*

### 3.4 Preservation of Logs

The primary goal of evidence preservation in WLANs is to ensure that absolutely no changes to the logged data have taken place since the data was collected [12]. Figure 4 demonstrates how the logs are being preserved in the proposed model. The Evidence Server (ES), as represented in figure 4, store all the blocks of data received from various CUs. In general, the ES act as a central storage of all the data monitored from the APs. The ES logs the blocks of data in chronological order. These blocks of data are stored according to the AP from which the traffic was monitored. For example, in the ES, B1AP1 means that block 1 represents the first block of traffic monitored from the first AP, whereas B1APn means that block 1 represents the first block of the traffic monitored from the nth AP.

It is worth noting that, the data stored in the ES is needed only for analysis purposes. The analysis of this data will only take place if a particular incident has been reported on the WLAN, which then needs to be investigated. The hash values of the blocks of data created in the perform hashing subcomponent within the CU is then transferred to the hashing storages represented as “HS of AP1” (Hashing Storage of AP1) and “HS of APn” (Hashing storage of APn) as represented in figure 4. There is a hashing storage for each AP on the WLAN. The H(B1AP1) in HS of AP1 shown in Figure 4 represents the hash value of the first block from the first AP, and H(B1APn) in HS of APn represents the hash of the first block from the nth AP and so on. The proposed model adopts the MD5 hashing technique. The MD5 hashing technique is not addressed in to detail in this paper since the focus is on forensic readiness, however, a detailed discussion of the MD5 hashing technique can be obtained in [12]. Hashing is described as a mathematical function that creates a unique fixed-length string from a message of any length [12]. The result of a hash function is a hash value, sometimes called a message digest. It is worth noting that the hashed blocks of data will only be used to check that, during a digital forensic investigation, the logged data on the ES has not been altered. This is a requirement of the digital forensic process [11].

### The Design of a Wireless Forensic Readiness Model (WFRM)



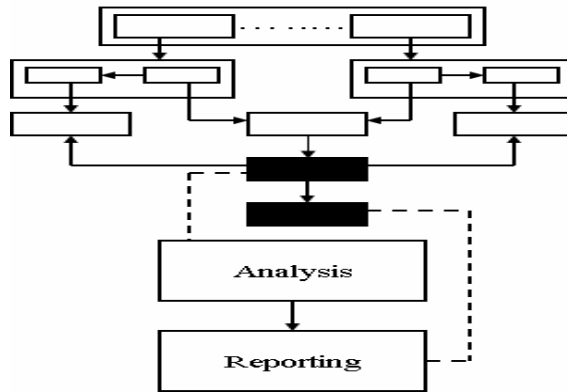
*Figure 4. Preservation component*

### 3.5 Analysis and reporting of logs

The main purpose of the analysis and reporting component is to mine and extract the data from the ES to come up with evidence that can associate a particular adversary with a criminal activity committed on the WLAN. The analysis component is the one responsible for mining data from the ES; however, it is not within the scope of this study to discuss data mining into details, but the use of data mining techniques should not be overlooked during the process of conducting a digital forensic investigation. The analysed data will then be passed to the reporting component.

The reporting component contains the final evidence of the entire digital forensic investigation. It is used by the cyber forensic experts when testifying in a court of law that an intruder was found to be guilty due to the evidence they possess from the investigation. It is then the decision of the prosecutor within a court to decide whether the intruder is guilty or not based on the evidence presented by the cyber forensic experts.

Proceedings of ISSA 2009



*Figure 5. Analysis and reporting components*

#### 4 THE WFRM – PUTTING IT ALL TOGETHER

This section is devoted to the integration of the proposed model. The WFRM (see Figure 6) is depicted with all its components as explained above. These components show how wireless traffic is monitored in the WLAN, how the monitored traffic is logged, preserved and how it is stored for analysis purposes in order to render information that is forensically ready to be used by forensic experts. This section starts by providing a presentation where by all the components of the WFRM are integrated together. A detailed discussion of the proposed model is then presented, and lastly a discussion on the interception of communication or traffic monitoring related issued is presented.

The numbers from one to five represented with circles in figure 6 depicts the phases of the digital forensic processes.



The Design of a Wireless Forensic Readiness Model (WFRM)

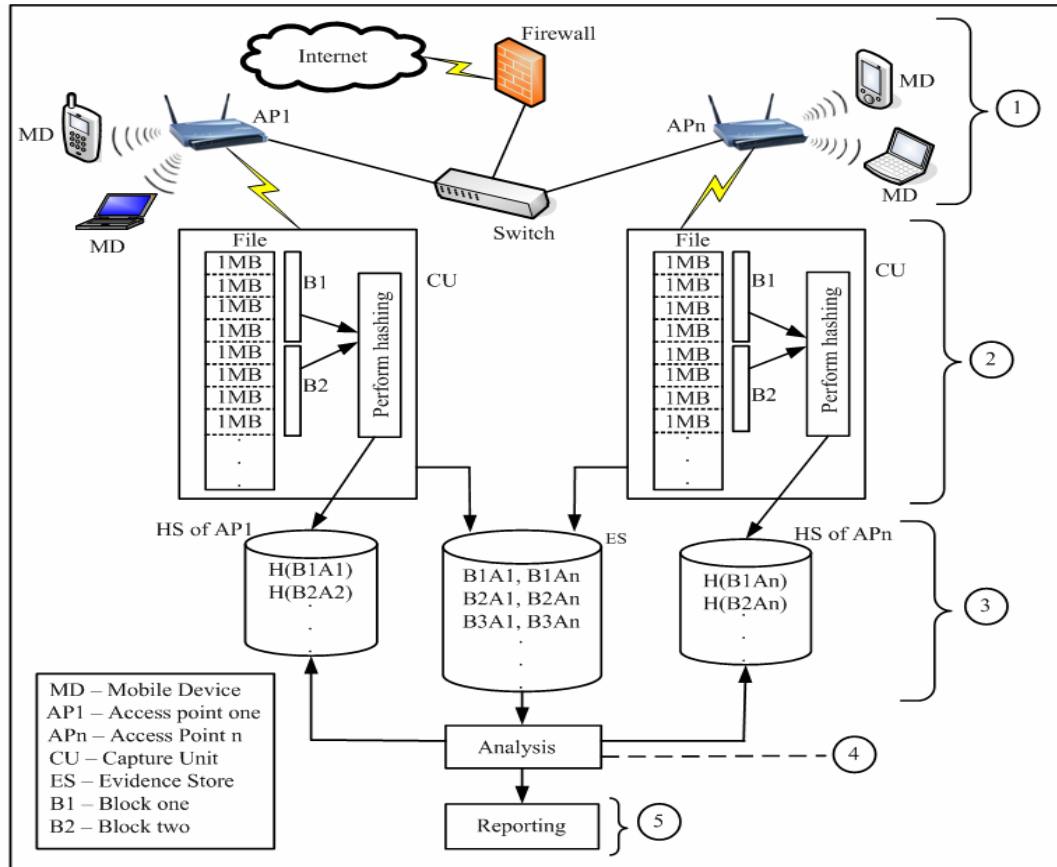


Figure 6. The Wireless Forensic Readiness Model (WFRM)

**4.1 Integrating the WFRM components**

Figure 6 shows all the components of the WFRM. The monitoring component indicates four mobile devices and two APs. Two of the MDs are connected to each AP. These MDs might be busy with internet access in a particular WLAN. This study assumes that the proposed model depicts a particular device deployed closer to the WLAN. This device has the capabilities of monitoring wireless traffic, logging the monitored traffic, preserving the traffic, and analysing the traffic. The component

which does the logging receives all the monitored wireless traffic from an AP and stores the data in a log file. The log file is divided into storage units of, say, 1MB. As the log file accumulates data, every fourth block, for example, are associated as a block of data. These blocks are then first transferred to the ES component. This study assumes that the ES is a sufficiently large mass storage device. Secondly, hashes of each of these blocks are created and transferred to the hashing storage. In this way the integrity of the data that flows through the WLAN is preserved.

Let's assume that an incident is being reported on the WLAN. Responding to the reported incident will not require much effort because the digital data is already forensically ready. The cyber forensic experts will just extract the data from the ES and do the analysis. The integrity of the analysed data can be proven by simply creating hash values of each block from where the evidence was extracted, and match that with the original hash values of each block as stored in the hashing storage. If the hashes match, it proves that the extracted evidence was, in fact, the original evidence, proving that the original evidence was not tampered with or manufactured.

#### **4.2 Discussion of the WFRM**

This section discusses the WFRM by outlining its advantages and disadvantages. This section then proceeds to discuss the traffic monitoring issues in a WLAN environment.

Once the traffic generated by the devices that connect to a WLAN has been monitored and preserved, it is ready to be analysed and used by cyber forensic experts to conduct the actual digital forensic investigation. Seeing that this information is forensically ready and forensically sound, the cyber experts' time and cost for conducting the entire digital forensic investigation is considerably minimised. In fact, the information needed for the investigation has been made readily available and the first part of the digital forensic process, i.e. the monitoring, logging and preservation phases, have been completed. A disadvantage of the WFRM, however, may be the fact that the traffic monitored from the APs requires a large amount of storage, and this may prove to be expensive. However, the authors are not too concerned about this disadvantage since storage space

## The Design of a Wireless Forensic Readiness Model (WFRM)

becomes ever cheaper. Nevertheless, the authors are working on introducing compression on the WFRM as a mechanism to minimise the amount of storage required to log the entire stream of traffic that passes through the network.

It was mentioned earlier that one of the functions of the WFRM is to monitor wireless network traffic. Traffic monitoring may also be referred to as interception of communication as presented in the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICCA). The RICCA act, act No. 70 of 2002 [13], prohibits the interception of communication, however section 6(2)(bb) makes a provision that a person may intercept communication only for the purpose of investigation or detecting unauthorised use of that communication system. Section 5(2)(a) states that the interception of communication may only take place if the entity that does the interception has given a prior consent in writing to the applicable law enforcement authorities.

Lastly, the authors are aware that the digital forensic process for FTK, EnCase and the WFRM as presented in Table 1 are logically more or less the same; however, this paper puts more emphasis on the design of a readiness model for wireless forensic purposes which comprise the somewhat different digital forensic phases of our model. Thus, the practical implementation if the digital forensic process employed by the proposed model is much different from that of conventional digital forensic process models of, for example, FTK and EnCase.

## 5 CONCLUSION

The most important issue addressed in this paper is that it is quite a challenge to conduct a digital forensic investigation in a WLAN environment. This is due to the fact that all the devices that participate in such an environment are mobile – therefore it becomes an enormous challenge to monitor and collect all the communications generated by these mobile devices and conduct a proper digital forensic investigation. WLANs are not forensically ready, as was suggested in this paper. In an attempt to solve this problem, this study proposed a WFRM that has the capability to monitor wireless traffic while these mobile devices are still

connected to the wireless network. As discussed in this study, the monitoring, logging and preservation of the traffic was proposed.

Whilst the development of the proposed model, as a proof of concept, is still in an early stage, there are a number of areas that still need to be addressed as future work. The first of these is the effective storage constraints of the log files. As traffic is monitored from the APs and stored on the log files, the storage space of the log files will eventually be depleted, however, as mentioned in section 4.2, the authors proposed that, compressing the blocks of data while maintaining the integrity of the data might be a solution to this problem. The second area of future research includes that of analysis. It is understood that several approaches exist for analysing digital data in order to determine evidence for forensic purposes, however, a new approach still needs to be identified specifically to cater for the analysis of the potential large amounts of data gathered by the model proposed in this study. Lastly, this research will also investigate issues like infrastructure requirements as one of the requirements for forensic readiness, evidence admissibility requirements and evidence management with regards to the retention period of information logged by the ES.

## 6 REFERENCES

- [1] Newman, R. (2007). *Computer Forensics, Evidence Collection and Management*. Auerbach Publications.
- [2] Arthur, K., Olivier, M. & Venter, H.S. (2007). *Applying the Biba Integrity Model to Evidence Management*. IFIP International Conference on Digital Forensics.
- [3] Rowlingson, R. (2004). *A Ten Step Process for Forensic Readiness*. International Journal of Digital Evidence, Vol. 2, Issue 3, pp1-5.
- [4] Endicott-Popovsky, E., Frincke, D.A. & Taylor, C.A. (2007). *A Theoretical Framework for Organizational Network Forensic Readiness*. Journal of Computers, Vol.2, NO.3, pp1-11.
- [5] ITU-T, (6 May 2008). *Technical Aspects of Lawful Interception*. Available from: [http://www.itu.int/dms\\_pub/itu-t/oth/23/01/T23010000060001PDFE](http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060001PDFE). (Accessed 26 November 2008).

## The Design of a Wireless Forensic Readiness Model (WFRM)

- [6] Peikari, C. & Fogie, S. (2003). *Wireless Maximum Security*. Sams Publishing, Indianapolis, Indiana, USA.
- [7] Turnbull, B. & Slay, J. (2007). *Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection Process*. Proceedings of the 40<sup>th</sup> Annual Hawaii International Conference on Systems Sciences (HICSS'07).
- [8] Wireless LANs, (15 March 2004). *What is a Wireless LAN?*. Available from: <http://www.wirelesslans.org/>, (Accessed 20 October 2008).
- [9] He, C. & Mitchell, J.C. (2005). *Security Analysis and Improvements for IEEE 802.11i*. The 12<sup>th</sup> Annual Network and Distributed Systems Security Symposium (NDSS'05), pp 90-110
- [10] Tan, J. (2001). *Forensic Readiness*. The CanSecWest Computer Security Conference.
- [11] Casey, E. (2007). *Handbook of Computer Crime Investigation, Forensic Tools and Technology*. Elsevier Academic Press, San Diego USA.
- [12] Solomon, M.G., Barrett, D. & Broom, N. (2005). *Computer forensics, The Best First Step towards a Career in Computer Forensics*. SYBEX Inc, San Francisco, London.
- [13] RICCA Act, (22 January 2002). *Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002*. Order No. 24286. Available from: <http://www.info.gov.za/acts/2002/a70-02/>, (Accessed 15 March 2009).
- [14] Encase. (18 August 2008). *The Industry leading eDiscovery Solution*. Available from: <http://www.guidancesoftware.com/ediscovery/index.aspx>, (Accessed 05 April 2009).
- [15] Forensic Toolkit. (10 July 2008). *Access Data, A pioneer in digital investigations since 1987*. Available from: <http://www.accessdata.com/forensictoolkit.html>, (Accessed 05 April 2009).

Proceedings of ISSA 2009

BC3I – Towards Requirements Specification For Preparing an Information Security Budget

## **BC3I – TOWARDS REQUIREMENTS SPECIFICATION FOR PREPARING AN INFORMATION SECURITY BUDGET**

**MT Dlamini<sup>1</sup>, MM Eloff<sup>2</sup>, JHP Eloff<sup>1,3</sup>, K Hone<sup>1</sup>**

<sup>1</sup>Information and Computer Security Architectures Research Group  
Department of Computer Science, University of Pretoria, South Africa

<sup>2</sup>School of Computing, UNISA, Pretoria, South Africa

<sup>3</sup>SAP Meraka UTD, CSIR, South Africa

{<sup>1</sup>mdlamini, <sup>3</sup>eloff}@cs.up.ac.za, Tel.:+27129999100

<sup>2</sup>eloffmm@unisa.ac.za, Tel.:+27124296336

<sup>1</sup>[KarinH@tebank.com](mailto:KarinH@tebank.com) Tel.: +27115185619

### **ABSTRACT**

The entire business landscape finds itself on the verge of a recession because of ongoing global economic turmoil. Thus, there is a heightened need to minimise and mitigate business risk and scrutinise information spending while ensuring compliance with regulatory mandates. This calls for decision makers to become vigilant in their spending and move towards an optimised information security investment. The main aim of this paper is to provide decision makers with a set of requirements to be considered when implementing a cost-effective and optimal information security budget; in a manner that preserve organisations' information security posture and compliance status. Research reported on in this paper forms part of an ongoing project known as the BC3I (Broad Control Category Cost Indicators) framework.

### **KEY WORDS**

Information security spending, requirements, controls, economics, information security breaches, regulatory compliance.

## 1 INTRODUCTION

Information security is a continuously changing discipline that requires continuous adaptation to new and ever-changing information security threats, countermeasures and the global business landscape. The global business landscape is on the verge of facing a recession following the ongoing global economic turmoil. This came as a result of the collapse of the United States of America's sub-prime mortgage market (Kiviat, 2009). Organisations must quickly adapt to the prevailing economic climate by becoming more vigilant in their spending in general and more so on overheads such as information security expenditure (Researchandmarkets, 2007; Tipton & Krause, 2003; Timms, 2004).

Alas, despite the lingering global economic turmoil and encouraging developments in information security, a survey conducted by Symantec late last year (2008) revealed that the global underground economy is booming at millions of dollars in advertised goods and services (Symantec, 2008; Ko, 2008). While the whole world is in the worst economic crisis, the underground economy continues to flourish.

Despite all the years of hard work on information security technology improvements, harsh compliance regulatory penalties and more coordinated law enforcements, information security breaches are still ubiquitous and have seriously damaging consequences (Grossklags, Chuang & Christin, 2008; Fumey-Nassah, 2007; Schneier, 2002). Clearly, something is not working effectively in the information security arena.

Are the organisations putting in enough effort to protect their information assets or are they not taking any precautions? Is it too little or just enough or more? How much is really enough? This paper investigates the requirements to provide input for the preparation of a budget for information security. Research done in preparation of this paper is part of an ongoing project known as the BC3I framework (Broad Control Category Cost Indicators) (Dlamini, Eloff & Eloff, 2009).

The remainder of the paper is structured as follows: Section 2 gives a brief background on the economics of information security; Section 3 discusses related work on information security investment; Section 4



discusses the requirements to be considered when implementing a cost effective information security, and Section 5 concludes the paper.

## 2 RELATED WORK

The field of economics of information security has become an important field of study (Tsiakis & Stephanides, 2005; Huang, Hu & Behara, 2006; Anderson & Moore, 2006; Anderson & Moore, 2007). For the past seven years, researchers have identified several topics of interest but this paper focuses only on **the economics of information security investment** (Gordon & Loeb, 2002; Camp, 2006; Anderson & Moore, 2006; Grossklags, Christin & Chuang, 2008; Hulthen, 2008).

The related literature investigated for this research project is structured as follows:

- A brief overview of the field of the economics of information security investment.
- Optimal allocation of resources to information security activities, with specific reference to the work of Gordon and Loeb (2002).

### 2.1 The Economics of Information Security Investment

This paper focuses on the topic of information security investment which is viewed from two opposing perspectives: either from the system defender's or the attacker's point of view.

Investing in information security is a trade-off; organisations can either choose to invest in security or not to invest (Anderson, 2001; Ioannidis, Pym & Williams, 2009). There are both direct and indirect benefits and costs involved. Directly, investing in information security reduces the risk exposure – though at an opportunity cost of other profitable investment. Not investing in information security guarantees more money – but at an opportunity cost of not having secure information assets. Indirectly investing in information security can help those who have not invested to “a free ride”. Those who do invest, could easily become victims of threats that come from those who fail to invest (what economists call externality). Information security practitioners have to consider the trade-offs and related issues when they scrutinise and make information security investment decisions.

Given the current threat landscape, the consequences of not investing in information security can prove to be more costly than the consequences of investing (Fumey-Nassah, 2007). Chapman (2009) highlight that organisations are losing billions of dollars because of information security breaches. The amount of time and effort that is involved in recovering from an information security breach, besides compliance fines and penalties to be paid is also a cause of concern. Over the years, organisations have therefore been left with no option but to invest in information security.

## **2.2 An Optimal Allocation of Funds to Information Security**

Organisations need adequate information security at a reasonable cost. For information security to make business sense; organisations must strike the right balance between the likelihood of risk and the cost to reduce such risk (Su, 2006). This has proven not an easy task to do. Goetz and Johnson (2006) point out that a majority of executives view information security as a “bottomless pit that never gets full” and some see it as “necessary evil that hinders productivity” (Conray-Murray, 2003). This is mainly due to the failure of information security managers to quantify their expenditure and the likelihood of the risk, faced by the information assets materialising. This failure has led executives to ask “how much is really enough for information security?”

In answering the fore-going question and contrary to the views of “a bottomless information security pit that never gets full”; researchers argue that there is actually an optimal point for information security spending (Anderson, 2001; Huang, Hu & Behara, 2008) which several researchers have tried to determine. It is not advisable to invest below or beyond this point.

Huang et al. (2006) use an economic model to determine optimal information security spending for organisations under multiple attacks. Modelling with variables such as system vulnerability, potential loss, budget and investment effectiveness, they demonstrate how to optimally allocate information security investments.

Wang and Song (2008) propose modelling with information security requirements, opportunity costs of the risks and budget constraints. They use a multi-objective decision-making framework to determine the

## BC3I – Towards Requirements Specification For Preparing an Information Security Budget

optimal information security investment. Unfortunately, the modelling approaches discussed in both Huang et al. (2006) and Wang and Song (2008) do not provide a definite figure or the exact point of optimality for an information security investment. Srinidhi et al. (2008) also present a model to assist information security managers to optimally allocate financial resources to information security so as to guarantee productivity and the safety of information assets.

In 2002, Gordon and Loeb proposed an economic model (G&L model hereafter) to determine the optimal allocation of funds among different assets with different vulnerabilities to information security. Unlike the work of Huang et al. (2006) and Wang and Song (2008), their findings show that the optimal investment for protecting an information asset must at least be less than or equal to 37% of the total loss expected of the information asset. Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model's assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss of an information asset.

Tanaka, Matsuura and Sudoh (2005) subsequently conducted an extensive empirical study using the G&L model. Their work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu et al. (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level. Matsuura (2008) remarks that the G&L model derive it's economic benefit from threat reduction, but concludes that this is not sufficient. Therefore Matsuura extended the G&L model to include a measure of productivity.

Huang et al. (2008) have since extended the G&L model to include a risk-averse decision maker instead of a risk-neutral decision maker and adopted the expected utility theory. They have modelled the relationship between potential loss, the extent of risk aversion and the effectiveness of an information security investment. The majority of the work done seems to concentrate on how much to invest in information security. However, several important shortcomings still exist as pointed out in the next paragraph.

### **2.3 Recommendations drawn from the reviewed literature**

The problem with the current body of knowledge is that it does not provide or recommend a set of requirements that decision makers have to consider when they develop their budgeting models. Requirements can act as a bridge in attempting to solve the problem of optimal resource allocation for information security.

Furthermore, decision makers need to provide evidence of the success of their information security spending. Due to the difficulty in establishing the monetary value of information security benefits, requirements can also be used to act as the measure of success or failure of models for the allocation of resources.

Requirements elicitation is therefore an acceptable departure point in the attempt to find solutions to the optimal and effective allocation of funds for information security.

## **3 REQUIREMENTS**

The need for efficient and effective budgeting and spending on information security is driven by a number of different high-level requirements, ranging from technological to strategic issues. The elicitation of requirements for preparing an information security budget as proposed in this paper is structured as follows:

3.1 Requirements gleaned from existing approaches

3.2 Additional requirements

### **3.1 Requirements gleaned from existing approaches**

The following list of requirements was identified from literature as referenced in this paper:

- Information security should be viewed as a multi-disciplinary field and therefore the budget should reflect implementation issues across the spectrum of people, process and technology.
- The budget should reflect implementation issues on the defence as well as attack side, i.e. proactive versus reactive.
- Careful consideration should be given to striking a balance between following a “standard-of-due-care” approach and following an approach based on risk assessment.

## BC3I – Towards Requirements Specification For Preparing an Information Security Budget

- An information security budget should address more than merely regulatory and standards compliance.

An information security budget should be based on assumptions clearly communicated to senior management, with specific reference to the % coverage of vulnerability exposure as well as the % acceptable risk levels.

### **3.2 Additional Requirements**

The authors of the paper in hand have identified the following additional requirements to be considered when preparing a budget for information security:

- 3.2.1 Taking cognisance of the three organisational levels
- 3.2.2 Compiling and using a well-defined Information Security Architecture
- 3.2.3 Other non-functional requirements

#### **3.2.1 Taking cognisance of the three organisational levels**

Cognisance has to be taken of the three well-known organisational levels, namely strategic, tactical and operational. These levels are to be used as a framework for organising the proposed requirements (Rolfsdotter Karlsson, 2008).

##### **3.2.1.1 Strategic Level**

On the strategic level, the budget for information security should be aligned with the vision and mission statement of the organisation, the business goals, legal obligations, overall risk appetite and policy statements. Any money spent should be in direct support of realistic and reachable business goals and priorities of the organisation. The business goals are derived from the vision, mission and values that are translated into the critical success factors of the organisation (Rolfsdotter Karlsson, 2008). This ensures that information security programmes are tightly coupled to the overall business strategy.

Legal obligations are stipulated in national and international regulatory requirements and laws. Organisations are forced to adhere to these or face prosecution if they do not.

Industry related laws and regulations must also be taken into account. Policy documents may also confirm the intent of an organisation, for example to protect the privacy of third parties. A policy describes the specific steps that an organisation will take and expects its employees to adhere to these in order to reach the organisation's business goals.

#### 3.2.1.2 Tactical Level

The tactical level includes risk analysis for the identification of threats; standards and any compliance requirements. Thus it plays an important role in identifying threats to the security of information assets. It plays a guiding role in deciding 'how much' to spend on 'what'. Butler (2003) identifies a number of shortcomings of risk analysis, such as that exact investment decisions have to be made based on 'guesstimated' information.

Compliance with international standards also influences the spending on information security. Many countries have equivalent standards on national level that reflect ISO/IEC 27002, such as the British Standard BS ISO/IEC 27002:2005 and the AS/NZS ISO/IEC 17799:2006 standard in New Zealand and Australia.

#### 3.2.1.3 Operational Level

On the operational level, both operational and technological requirements need to be considered. Operational requirements include aspects such as affordability of manpower, resources, optimal protection levels and feasibility. Furthermore, the operational level includes administrative requirements referring to guiding the user's actions to meet business goals and objectives as specified on the strategic level.

Technological requirements include both ICT infrastructure components such as controls on the hardware and software levels. When selecting controls, identification of an optimal mix of controls is of vital importance.

### **3.2.2 Compiling and using a well-defined Information Security Architecture**

Eloff and Eloff (2005) proposed a number of requirements for the establishment of an information security architecture. These requirements – originally defined for developing information security architecture – can

## BC3I – Towards Requirements Specification For Preparing an Information Security Budget

also be translated into requirements for information security budgets. The requirements state that information security architecture should

- **be holistic and encompassing:** The budget for information security should indeed be holistic and refer to the full spectrum of controls to be implemented. The requirement of holism involves the inclusion of all aspects when budgeting for security. the budget should not focus on isolated aspects but on all aspects.
- **make suggestions on how different controls can be synchronised and integrated to achieve maximum effect:** Very few organisations today spend enough time on the synchronisation and integration of controls, resulting in a potential over expenditure and duplication of controls. The synchronisation and integration of controls in most cases are organisation specific.
- **include a comprehensive approach to information security risk management:** The relationship between a comprehensive approach towards risk management and the information security budget is self-explanatory as the budget for information security should very clearly indicate how much risk mitigation is planned for, as well as the acceptable risk that the organisation will endure.
- **be measurable to demonstrate adherence to the requirements as set out.** Research has shown that it is somehow difficult to establish the monetary value of information security controls and of the benefits derived (Abrams et al., 1998; Conrad, 2005; Pfleeger & Pfleeger, 2007; Srinidhi et al., 2008). Despite these difficulties, the results should be expressed in monetary terms.

### 3.2.3 Other non-functional requirements

Non-functional requirements are viewed as those that impose constraints on the compilation of the budget for information security. Previous work done by the authors of this paper, as reported in Dlamini et al. (2009), suggest the following high-level non-functional requirements:

- **Flexibility:** This requirement recognises the fact that organisations are different and that they exist in different sectors. One prescribed solution regarding information security controls will not satisfy the requirements of all organisations.
- **Cost effectiveness:** Organisations must be able to identify and implement those controls that will protect their information resources



in the most cost-effective way. Implementing all the controls may be a matter of “overkill”, thus just “enough” should be implemented.

Lastly, the existing and current information security budget must not be ignored as a valuable input into future budget definitions. The existing budget will also shape where recurring costs must be budgeted for, e.g. licensing fees on information security tools, hardware upgrades on information security technology.

### 3.3 SUMMARY

In a nutshell, the UML diagram depicted in Figure 1 is used to model the requirements for preparing an information security budget as proposed in this paper.

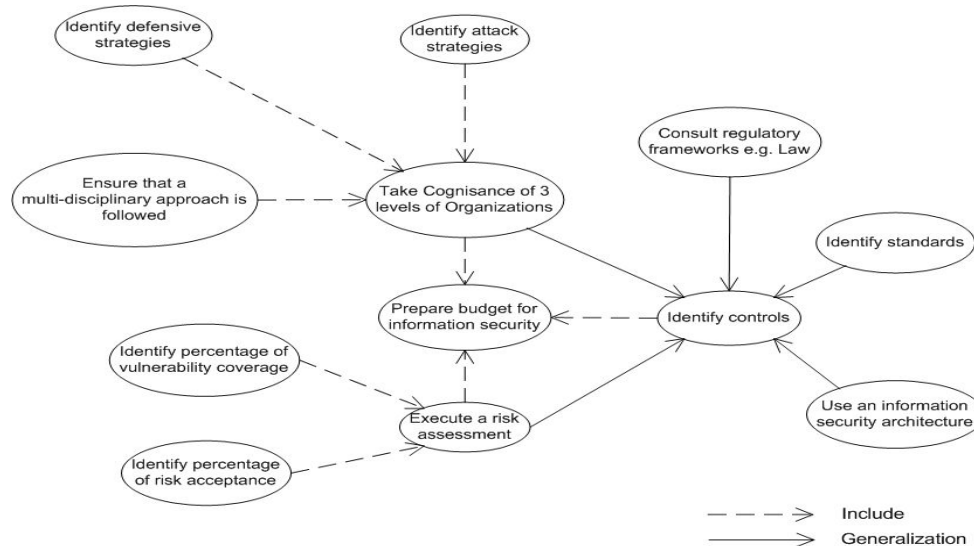


Figure 1: Use case and collaboration diagram for preparing an information security budget

Consider the above diagram. The identification of controls can be generalised as being the output of activities such as controls identified by means of regulatory investigations, standards, use of information security architecture, risk analysis, as well as cognisance of the three organisational levels. These generalisations are depicted by fixed lines whereas the broken lines show activities that should be included in the activity when preparing a budget for information security.



#### 4 CONCLUSION

The current economic crisis is affecting organisations world-wide and all are required to spend money wisely. This also applies to spending on information security. Current models and approaches to determine *how much* to spend on *what* in order to safeguard information assets do not consider the total picture of an organisation and the environment in which it operates? In this paper the authors approached this problem holistically and identified the requirements to be considered when preparing an information security budget. These requirements are presented in a “use case” diagram that illustrates the potential interaction between the different components.

#### Acknowledgments:

The support of SAP Research CEC Pretoria towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and cannot necessarily be attributed to SAP Research.

#### 5 REFERENCES

Abrams, M.D., Johnson, C.M., Kahn, J.J. and King, S.G. (1998) Considerations for Allocating Resources for Information Security. Available online at [www.c4i.org/caris.pdf](http://www.c4i.org/caris.pdf), accessed on 09 February 2009.

Anderson, R. (2001) Why Information Security is Hard – An Economic Perspective, the *17<sup>th</sup> Annual Computer Security Applications Conference*, 10 - 14 December 2001, New Orleans, Louisiana, USA.

Anderson, R. and Moore, T. (2006) The Economics of Information Security, *Science* 314(5799): 610-613, 27 October 2006.

Anderson, R. and Moore, T. (2007) Information Security Economics – and Beyond. Available online at: [http://www.cl.cam.ac.uk/~rja14/Papers/econ\\_crypto.pdf](http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf), accessed on 12 January 2009.

Proceedings of ISSA 2009

Butler, S.A. (2003) Security Attribute Evaluation Method, PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

Camp, L.J. (2006) The state of Economics of Information Security, *I/S: Journal of Law and Policy*, 2(2): 189-205.

Chapman, G. (2009) Cybercrime losses top \$US1 trillion. Available online at: <http://www.australianit.news.com.au/story/0,24897,24997483-24169,00.html>, accessed on 19 February 2009.

Conrad, J.R. (2005) Analyzing Risks of Information Security Investments with Monte-Carlo Simulations, *Fourth Workshop on the Economics of Information Security*, 2-3 June 2005, Kennedy School of Government, Harvard University.

Conray-Murray, A. (2003) Strategies & issues: justifying security spending. Available online at: <http://www.itarchitect.com/articles/NMG20020930S0002.html>; accessed on 18 July 2007.

Dlamini, M.; Eloff, J.H.P. and Eloff, M.M. (2009) BC3I – A Model for Information Security Cost Indicators, submitted to the *Journal of Research and Practice in Information Technology*.

Eloff J.H.P. and Eloff M.M. (2005) Information Security Architecture, *Computers Fraud & Security*, 2005(11): 10-16, Nov 2005.

Fumey-Nassah, G. (2007) The Management of Economic Ramification of Information and Network Security on an Organization, *Proceedings of the Information Security Curriculum development Conference '07*, 28 – 29 September 2007, Kennesaw, Georgia, USA.

Goetz, E. and Johnson, M.E. (2006) Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA. Available online at [http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO\\_RiskManage/Overview.pdf](http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf), accessed on 18 February 2009.

BC31 – Towards Requirements Specification For Preparing an Information Security Budget

Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investments, *ACM Transactions on Information and System Security*, (5)4: 438-457, November 2002.

Grossklags, J., Chuang, J. and Christin, N. (2008) Security Investment (failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents, *The Seventh Workshop on the Economics of Information Security*, 25 -28 June 2008, The Center for Digital Strategies, Tuck School of Business at Dartmouth College, Hanover, USA.

Huang, C.D., Hu, Q. and Behara, R.S. (2006) Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Huang, C.D., Hu, Q. and Beraha, R.S. (2008) An Economic analysis of the optimal information security investment in the case of a risk averse firm, *The International Journal of Production Economics*, 2008(114): 793 - 804

Hulthen, R. (2008) Communicating the Economic Value of Security Investment: Value at Security Risk, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Ioannidis, C., Pym, D. and Williams, J. (2009) Investments trade-offs in the Economics of Information Security, *the thirteenth Proceedings of the conference of Financial Cryptography and Data Security*, 23 – 26 February 2009, Barbados, USA.

ISO/IEC 27002:2005, July 2007 *Information technology - Security techniques - Code of practice for information security management*, renumbered in 2007.

Kiviat, B. (2009) How to Fix the Housing Market, Times Magazine. Available online at: <http://www.time.com/time/magazine/article/0,9171,1879184-2,00.html>, accessed on 19 February 2009.

Proceedings of ISSA 2009

Ko, C. (2008) Underground Economy Booming Online, Says Symantec, IDG News Service. Available online at: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123142&source=rss\\_ind130](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123142&source=rss_ind130), accessed on 10 January 2009.

Liu, W., Tanaka, H. and Matsuura, K. (2007) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSIJ Digital Courier*, 3: 585 – 599.

Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Pfleeger, C.P. and Pfleeger, S.L. (2007) *Security in Computing*, 4<sup>th</sup> edition, Pearson Education, Inc, United States.

Researchandmarkets (2007) IT Security Market Report 2007, UK. Available at: <http://www.bharatbook.com/productdetail.asp?id=11035>, accessed [18 February 2009]

Rolfsdotter Karlsson, A., (2008) *Managing Performance Measurement: A study of how to select and implement performance measures on a strategic, tactical and operational level*, Master's Thesis, University of Gävle, Sweden.

Schneier, B. (2002) Computer Security: It's the Economics, Stupid, 1<sup>st</sup> Workshop on the *Economics of Information Security*, 16 -17 May 2002, University of California, Berkeley, USA.

Srinidhi, B., Yan, J. and Tayi, G.K. (2008) Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, *Working paper Series 2008-17*, School of Economic Sciences, Washington State University, USA. Available online at [www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi\\_Yan\\_GiriJune2008MISQ.pdf](http://www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune2008MISQ.pdf), accessed on 09 February 2009.

BC31 – Towards Requirements Specification For Preparing an Information Security Budget

Su, X. (2006) An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Symantec (2008) Symantec Report on the Underground Economy (July 2007 – June 2008), Whitepaper. Available online at: [eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_underground\\_economy\\_report\\_11-2008-14525717.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf) accessed on 09 January 2009.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, 2005(24): 37-59.

Timms, S. (2004) Information Security Breaches Survey 2004: Executive Summary, PriceWaterhouseCoopers, Department of Trade and Industry, UK. Available online at: [http://www.entrust.com/resources/pdf/ukdti\\_infosecbreachsurvey2004\\_execsumm.pdf](http://www.entrust.com/resources/pdf/ukdti_infosecbreachsurvey2004_execsumm.pdf), accessed on 18 February 2009.

Tipton, H.F. and Krause, M. (2003) *Information Security Management Handbook, 5<sup>th</sup> Edition*, Auerbach Publication, New York, USA.

Tsiakis, T. and Stephanides, G. (2005) The Economic Approach of Information Security, *Computers & Security*, 24(2): 105-108.

Wang, Z. and Song, H. (2008) Towards an optimal information security investment strategy, *IEEE Conference on Networking, Sensing and Control 2008*, April 6 – 8, 2008, pp. 756 – 761.

Willemson, J. (2006) On the Gordon and Loeb Model for Information Security Investment, presented at *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, University of Cambridge, UK, 26-28 June 2006. Available online at <http://www.ut.ee/~jan/publ/economics.ps>, accessed on 27 November 2007.

Proceedings of ISSA 2009

Identification of Basic Measurable Security Components in Software Intensive Systems

**IDENTIFICATION OF BASIC MEASURABLE  
SECURITY COMPONENTS IN SOFTWARE INTENSIVE  
SYSTEMS**

**Reijo M. Savola**

VTT Technical Research Centre of Finland  
P.O. Box 1100, 90571 Oulu, Finland

**ABSTRACT**

Appropriate information security solutions for software-intensive systems, together with evidence of their security performance help to prevent serious consequences for businesses and the stakeholders. Security metrics can be used to offer this evidence. We investigate practical and holistic development of security metrics for software-intensive systems. Our approach is security requirement-centric. The high-level security requirements are expressed in terms of lower-level measurable components applying a decomposition approach. Detailed security metrics are developed based on the basic measurable components identified at the leaf level of the decomposition.

**KEY WORDS**

Security metrics, security measurements, security requirements

# **IDENTIFICATION OF BASIC MEASURABLE SECURITY COMPONENTS IN SOFTWARE INTENSIVE SYSTEMS**

## **1 INTRODUCTION**

The increasing complexity of software-intensive and telecommunication products, together with pressure from security and privacy legislation, are increasing the need for adequately validated security solutions. To obtain evidence of the information security performance of systems needed for the validation, services or products, systematic approaches to measuring security are needed. The field of defining security metrics systematically is very young. Because the current practice of security is still a highly diverse field, holistic and widely accepted measurement and metrics approaches are still missing.

The rest of this paper is organized in the following way. Section 2 gives a short introduction to security metrics. Section 3 introduces the proposed security metrics development process. Section 4 discusses threat and vulnerability analysis, and the next section security requirements. Section 6 describes decomposition of security requirements. Section 7 explains issues important in the measurement architecture and evidence collection, Section 8 discusses the further steps of metrics development. Section 9 presents related work and finally, Section 10 summarizes the study with some future research questions and conclusions.

## **2 SECURITY METRICS**

Security metrics and measurements can be used for decision support, especially in assessment and prediction. When using metrics for prediction, mathematical models and algorithms are applied to the collection of measured data (e.g. regression analysis) to predict the security performance. The target of security measurement can be, e.g., an organization, its processes and resources, or a product or its subsystem. In general, there are two main categories of security metrics: (i) security metrics based on threats but not emphasizing attacker behavior, and (ii) security metrics predicting and emphasizing attacker behavior. In this



## Identification of Basic Measurable Security Components in Software Intensive Systems

study, we concentrate in the former type of metrics. Security metrics properties can be quantitative or qualitative, objective or subjective, static or dynamic, absolute or relative, or direct or indirect. According to ISO 9126 standard [1], a direct measure is a measure of an attribute that does not depend upon a measure of any other attribute. On the other hand, an indirect measure is derived from measures of one or more other attributes. See [2] and [3] for examples of security metrics.

### **3 PROPOSED SECURITY METRICS DEVELOPMENT PROCESS**

In this study, we use the following iterative process for security metrics development, partly based on [4]. The steps for the process are as follows:

1. Carry out threat and vulnerability analysis. Identify and elaborate threats of the system under investigation and its use environment. If enough information is available, identify known or suspected vulnerabilities. This work can continue iteratively as more details of the target will be known.
2. Define and prioritize security requirements, including related requirements critical from security point of view, in a holistic way based on the threat and vulnerability analysis. The most critical security requirements should be paid the most attention. Pay attention to the simplicity and unambiguity of the requirements.
3. Identify *Basic Measurable Components* (BMC) from the higher-level security requirements using a decomposition approach. BMCs relate the metrics to be developed to security requirements.
4. Develop measurement architecture for on-line metrics and evidence collection mechanisms for off-line metrics.
5. Select BMCs to be used as the basis for detailed metrics based on their feasibility and criticality.
6. Define and validate detailed security metrics, and the functionalities and processes where they are used.

The steps are iterative and the order of the steps can be varied. Steps 1 and 2 should be started as early as possible in the research and development lifecycle and elaborated iteratively as the system design becomes more mature. If possible, steps 3 and 4 can be carried out in parallel to each other. Step 4 can be initiated already during the architectural design phase provided that suitable information is available.

#### 4 THREAT AND VULNERABILITY ANALYSIS

Threat analysis is the process of determining the relevant threats to an SUI (System under Investigation). The outcome of the threat analysis process is preferably a prioritized description of the threat situations. In practice, there are many ways to carry out threat analysis, from simply enumerating threats to modeling them in a more rigorous way. The extent of threat analysis depends, e.g., on the criticality of the use cases in the SUI. The following threat and vulnerability analysis process can be used, based on the Microsoft threat risk modeling process [5]: (1) identify security objectives, (2) survey the SUI architecture, (3) decompose the SUI architecture to identify functions and entities with impact to security, (4) identify threats, and (5) identify vulnerabilities.

The security objectives can be decomposed, e.g., to identity, financial, reputation, privacy and regulatory and availability categories [6]. There are many different sources of risk guidance that can be used in developing the security objectives, such as laws, regulations, standards, legal agreements and information security policies. Once the security objectives have been defined, it is important to analyze the designed SUI architecture and to identify different components, data flows and trust boundaries. To identify the functions and entities with impact to security objectives, the architecture can be decomposed further. Threats are the goals of the adversary and for a threat to exist it must have a target asset. To identify threats, the following questions can be asked [7]:

1. How can the adversary use or manipulate the asset to modify or control the system, retrieve or manipulate information within the system, cause the system to fail or become unusable, or gain additional rights?
2. Can the adversary access the asset without being audited, or skip any access control checks, or appear to be another user?

The threats can be classified using a suitable model like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) [5]. DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) [5] is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat.

## Identification of Basic Measurable Security Components in Software Intensive Systems

Vulnerability analysis can be carried out after appropriate technological choices have been made. Vulnerabilities in the technology and implementation affect to threats of the system. In vulnerability analysis, well-known vulnerability listings and repositories such as OWASP (Open Web Application Security Project) Top 10 [6] can be used. Metrics from Common Vulnerability Scoring System (CVSS) [8] can be used to depict how easy or hard it is to access and exploit a known vulnerability in the system.

### 5 SECURITY CRITICAL REQUIREMENTS

Security requirements derive from *threats*, *policies* and *environment properties*. Security requirements that are derived from threats are actually countermeasures. Security policies are security relevant directives, objectives and design choices that are seen necessary for the system under investigation. Environment properties contribute to the security of the SUI from outside – either advancing or reducing it. The explanation for the security-advancing effect of the environment is that it could to contain a countermeasure solution against a threat, outside the SUI. In general, every security risk due to a threat chosen to be cancelled or mitigated must have a countermeasure in the collection of security requirements. In general, the state of practice in defining security requirements is not at matured level. According to [9], the most current software requirement specifications are either (i) totally silent regarding security, (ii) merely specify vague security goals, or (iii) specify commonly used security mechanisms (e.g., encryption and firewalls) as architectural constraints. In the first case security is not taken into account in an adequately early phase of design. In the second case vague security goals (like “the application shall be secure”) are not testable requirements. The third case may unnecessarily tie architectural decisions too early, resulting in an inappropriate security mechanism. Security requirements are often conceived solely as non-functional requirements along with such aspects as performance and reliability within the requirements engineering community [10]. From the security engineering viewpoint this is a too simplified way of thinking; security cannot be represented only by non-functional requirements since security goals often motivate new functionality, such as monitoring, intrusion detection and access control, which, in turn, need functional requirements. Unfortunately, satisfactory

approaches to capturing and analyzing non-functional requirements have yet to mature [11].

## 6 DECOMPOSING REQUIREMENTS

The core activity in the proposed security metrics development process is the decomposition the security requirements. In the following, we discuss the decomposition process and give an example of it.

### 6.1 Decomposition Process

The following decomposition process (based on [12]) is used to identify measurable components from the security requirements:

1. Identify successive components from each security requirement (goal) *that are essential and contribute to the success* of the goal.
2. Examine the subordinate nodes to see if further decomposition is needed. If so, repeat the process with the subordinate nodes as current goals, breaking them down to their essential components.
3. Terminate the decomposition process when none of the leaf nodes can be decomposed any further, or further analysis of these components is no longer necessary. When the decomposition terminates, all leaf nodes should be measurable components.

### 6.2 Example Decomposition: Authentication

In general, the model depicted in Fig. 1 can be used for high-level authentication decomposition [12] during the process of identifying potential metrics for authentication performance. Similar decompositions can be defined for authorization, confidentiality, integrity, availability and so on.

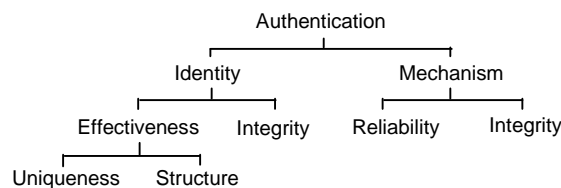
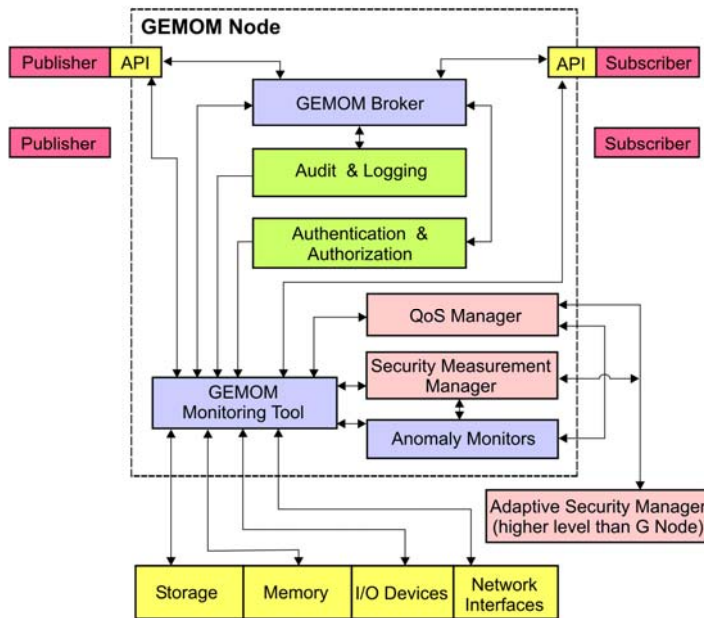


Figure 1. Decomposition of authentication

## Identification of Basic Measurable Security Components in Software Intensive Systems



*Figure 2.* Example of information flows.

Different authentication mechanisms (e.g. password authentication and various forms of biometrics and any combination) can be used for different authentication needs. Fig. 1 comments that the security level of authentication mechanisms is depending on their level of reliability and integrity. There are many ways to use metrics and their combinations.

### 7 MEASUREMENT ARCHITECTURE AND EVIDENCE COLLECTION

In the case of on-line metrics, the measurement architecture and data flow needs to be designed, in parallel to the overall architectural and data flow design of the SUI. Similarly, in the case of off-line metrics, the evidence collection mechanisms and criteria need to be planned. In many cases, on-line and off-line measurements can be dependent on each other.

Identification of measuring points and development of evidence collection mechanisms can be carried out, e.g., from data flow diagrams and protocol descriptions. As an example, Fig. 2 shows a conceptual picture of information flows of a distributed messaging system (GEMOM,

Genetic Message Oriented Secure Middleware [13]). Security metrics of the Security Monitor module can use information from the Broker module, Audit and Logging module and the Authentication and Authorization module. In addition, the metrics get information from memory, storage, Input-Output devices and network interfaces.

## **8 DETAILED METRICS DEVELOPMENT**

The detailed development of chosen security metrics includes formalizing the metric to a computational form. Different weights can be associated to different metrics to indicate the relative importance or weights among the components. A “close to correct” weight assignment is critical, since in practice there are no analytical results for determining the relative priorities of the elements besides careful use of one’s expertise and judgment [12].

### **8.1 Authentication and Authorization Metrics**

Use of authentication mechanisms from different authentication categories makes the authentication stronger, the categories being: (i) something you know, (ii) something you have and (iii) something you are. *Authentication strength value* (e.g. from 0 to 1) can be assigned. In the case of multi-modal authentication the security strength value can be increased. In a similar way, strengths can be assigned to different authentication mechanisms, algorithms and protocols. In addition to metrics that measure the performance of authentication, metrics that express the attacker behaviour can be developed, such as (i) number of authentication failures, (ii) proportion of failed authentications, and (iii) a measure of authentication trends. False positives in authentication are attackers falsely permitted access and false negatives are authorized users who are hindered from accessing the systems they should be able to use. Regarding federated identity management and single sign-on, typical use patterns based on use cases can be defined or recorded from the system. The actual patterns from logs can be compared to the typical use patterns [4].

Most authorization metrics can be based on the log and metadata information of the users and objects they access or trying to access. This data can be used to investigate authorization mechanism use trends and to track extraordinary user behaviour. In addition, metrics from CVSS

## Identification of Basic Measurable Security Components in Software Intensive Systems

(Common Vulnerability Scoring System) [8] can be used to illustrate how easy or hard it is to access and exploit a known vulnerability in the system. Leaving a known vulnerability in the system might be a deliberate choice decided in the risk management process. CVSS's *access vector metric* measures whether the vulnerability is exploitable locally or remotely and *access complexity metric* measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system or service [4].

### 8.2 Confidentiality and Integrity Metrics

Cryptographic confidentiality strength metrics measure the performance of cryptographic protection used to ensure the end-to-end confidentiality of messages, logs and metadata. Different algorithms can be used based on the level of confidentiality needed. The protection in physical media (storage and memory) and the protection from unauthorized access to them is important. The reliability and effectiveness of access control are important too. *Confidentiality impact metric* of CVSS measures the impact on confidentiality of a successful exploit of vulnerability in the system. As in the case of confidentiality, cryptographic integrity strength metrics measure the level of cryptographic protection used to ensure the data integrity in messages, metadata, logs and storages (persistent data). *Integrity impact metric* of CVSS measures the impact to integrity of a successfully exploited vulnerability (none, partial, complete) [4].

### 8.3 Availability and Non Repudiation Metrics

Availability metrics from safety and reliability engineering can be used to measure the availability dimension. *Availability impact metric* of CVSS measures the impact to availability of a successfully exploited vulnerability (none, partial, complete).

In non-repudiation, it is important that proof-of-identity evidence can be obtained from the system. The evidence should be consistent, reliable and its integrity should be protected. Consistency, reliability and integrity metrics can be used for non-repudiation. Cryptographic strength metrics can be used to measure the performance of cryptographic algorithms used to ensure the non-repudiation of messages [4].



#### **8.4 Metrics based on Other Requirements**

Some other requirements potentially have effect to the security performance of the system. Application-level and business requirements should be taken into account in the security metrics development. Note that business environment and constraints affect a lot the impact and exposure of security risks. Usability and performance of security solutions are very important design objectives [4].

#### **8.5 Doubts about Security Metrics**

The feasibility of measuring security and developing security metrics to present actual security phenomena has been criticized in many contributions. In designing a security metric, one has to be conscious of the fact that the metric simplifies a complex socio-technical situation down to numbers or partial orders. McHugh [15] is skeptical of the side effects of such simplification and the lack of scientific proof. Bellovin [16] remarks that defining metrics is hard, if not infeasible, because an attacker's effort is often linear, even in cases where exponential security work is needed. Another source of challenges is that luck plays a major role [17] especially in the weakest links of information security solutions. Those pursuing the development of a security metrics program should think of themselves as pioneers and be prepared to adjust strategies as experience dictates [14].

### **9 RELATED WORK**

Wang and Wulf [12] describe a general-level framework for measuring system security based on a decomposition approach. CVSS [8] (Common Vulnerability Scoring System) is a global initiative designed to provide an open and standardized method for rating information technology vulnerabilities from a practical point of view. NIST's Software Assurance Metrics and Tool Evaluation (SAMATE) project [18] seeks to help answer various questions on software assurance, tools and metrics. OWASP (Open Web Application Security Project) [6] contains an active discussion forum on security metrics. More security metrics approaches are surveyed in [2] and [3].



## 10 CONCLUSIONS AND FUTURE WORK

Feasible and widely accepted approaches for security metrics development of software-intensive systems are still missing. We have introduced a novel methodology for security metrics development based on threats, policies, security requirements and requirement decomposition. The methodology is highly iterative and the order of steps can be varied depending on the information available.

Further work is needed in the development of generic and application and domain specific security requirement model decompositions, ways to define measurement architectures, evidence collection and selection of measurable components. Furthermore, heuristics for assessment of the feasibility of candidate component metrics are needed. The approach and parts of it need to be validated by experimentation in practical use scenarios originating from different application domains.

## 11 REFERENCES

- [1] ISO/IEC 9126-4, Software Engineering – Product Quality – Part 4: Quality in Use Metrics, 2000.
- [2] Savola, R., A Novel Security Metrics Taxonomy for R&D Organisations, Proceedings of the 7th Annual Information Security South Africa (ISSA) Conference, July 7-9, 2008, Johannesburg, South Africa.
- [3] Herrmann, D. S., Complete Guide to Security and Privacy Metrics, Auerbach Publications, 2007, 824 p.
- [4] Savola, R. and Abie, H., Identification of Basic Measurable Security Components for a Distributed Messaging System. In SECURWARE 2009, June 18-23, 2009, Athens, Greece, 8 p.
- [5] Howard, M. and LeBlanc, D., Writing Secure Code, Second Edition, Microsoft Press, 2003.
- [6] OWASP (Open Web Application Security Project), Threat Risk Modeling, web reference: [www.owasp.org](http://www.owasp.org)
- [7] Swiderski, F. and Snyder, W., Threat Modeling, Microsoft Press, 2004.
- [8] Schiffman, M., A Complete Guide to the Common Vulnerability Scoring System (CVSS). White paper.

Proceedings of ISSA 2009

- [9] Firesmith, D., Specifying Reusable Security Requirements, *Journal of Object Technology*, Vol. 3, No. 1, Jan/Feb 2004, 61-75.
- [10] Chung, L., Nixon, B. A., and Yu, E., Using Quality Requirements to Systematically Develop Quality Software, 4th Int. Conference on Software Quality, McLean, VA, October 1994.
- [11] Nuseibeh, B. and Easterbrook, S., Requirements Engineering: A Roadmap, *The Future of Software Engineering*, Special Volume published in conjunction with ICSE 2000, A. Finkelstein, Ed., pp. 35-46.
- [12] Wang, C. and Wulf, W. A., Towards a Framework for Security Measurement, 20th National Information Systems Security Conference, Baltimore, MD, Oct. 1997, pp. 522-533.
- [13] Abie, H., Dattani, I., Novkovic, M., Bigham, J., Topham, S. and Savola, R., GEMOM – Significant and Measurable Progress Beyond the State of the Art, ICSNC 2008, Sliema, Malta, Oct. 26-31, 2008, pp. 191-196.
- [14] Payne, S. C., A Guide to Security Metrics, SANS Institute Information Security Reading Room, 2006.
- [15] McHugh, J., Quantitative Measures of Assurance: Prophecy, Process or Pipedream? Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, VA, May 2001 (2002).
- [16] Bellovin, S. M., On the Brittleness of Software and the Infeasibility of Security Metrics, *IEEE Security & Privacy*, July/August 2006, p. 96.
- [17] Burris, P. and King, C., A Few Good Security Metrics, METAGroup, Inc. Oct 2000.
- [18] Plack, P. E., SAMATE's Contribution to Information Assurance, *IANewsletter*, Vol. 9, No. 2, 2006.

Discussing E-Government Maturity Models for Developing World – Security View

## **DISCUSSING E-GOVERNMENT MATURITY MODELS FOR DEVELOPING WORLD – SECURITY VIEW**

**Geoffrey Karokola<sup>1</sup> and Louise Yngström<sup>2</sup>**

Department of Computer and System Sciences  
Stockholm University/Royal Institute of Technology  
Forum 100, SE-164 40 Kista, Sweden  
Tel: +46 (0)8 16 1697, Fax: +46 (0)8 703 90 25  
E-mails: {[karokola<sup>1</sup>](mailto:karokola@dsv.su.se), [louise<sup>2</sup>](mailto:louise@dsv.su.se)}@[dsv.su.se](mailto:dsv.su.se)

### **ABSTRACT**

The development of Information and Communication Technology (ICT) systems towards materialization into e-Government applications is expected to tremendously change the ways governments deliver their core business services to citizens and how citizens can interact with their governments. There are also high expectations that these changes will play major roles in the socio-economic developments. For these reasons there are several so called maturity models being developed to guide and benchmark e-government developments in developing countries. These models describe various stages, three to six, referring to technological complexity. However, we do not see explicitly that security is addressed as a specific issue at the various stages, nor do we see how cultural, legal, economical and managerial security related issues are incorporated.

Being part of the ongoing research in the area, the paper attempts to critically investigate, evaluate and analyze eleven existing e-government maturity models, and discuss the findings in the light of research findings from four government institutions located in the Sub-Saharan Africa.

### **KEY WORDS**

e-Government, Maturity Model, ICT/IT Security, Technical, Non-technical, Developing Countries

## **DISCUSSING E-GOVERNMENT MATURITY MODELS FOR DEVELOPING WORLD – SECURITY VIEW**

### **1 INTRODUCTION**

Over recent years there has been an enormous development of Information and Communication Technology (ICT) systems towards e-government applications. Similarly, governments have also considered e-government as a powerful tool that can change ways they conduct and deliver their core business services to citizens and how citizens can interact with their governments. Also, there are higher expectations that adoption and use of e-government application could improve efficiency, effectiveness, accountability, and transparency of government service delivery, and at the same time improve active participation of citizen in public decision-making processes – hence realization of socio-economic development [2, 9, 11, 13, 22]. Various studies [2, 13] show that while most of the developed countries are in the final stages of e-government development - developing countries are still in the early stages of e-government development. This gap is heavily influenced by the existence of technological and non-technological related issues including lack of proper ICT infrastructures, readiness, awareness, economical, and political will.

However, to guide and benchmark e-government development, researchers and academia proposed different types of e-government development models, so called maturity models. These models outline various stages for e-government development. For instance West [23] proposed a three stage model, Layne & Lee [11] four stage models, while Deloitte & Touche [21] proposed a six stage model. Nevertheless, as governments' moves towards adoption of e-government applications – security has become a critical factor influencing its development at all stages of e-government development [1, 5, 9, 10, 11, 12, 20]. This creates need for holistic approach to explicitly addressing and incorporating security as a specific issue at the various stages of the development models [1, 19]. These include technical and non-technical security related issues such as cultural, legal, economical and managerial. According to the World Bank [25] e-government is defined as “the government owned or

## Discussing E-Government Maturity Models for Developing World – Security View

operated systems of information and communication technologies that transform relations with citizens, the private sector and/or other government agencies so as to promote citizens' empowerment, improve service delivery, strengthen accountability, increase transparency, and improve government efficiency". However, the concept of e-government has no clear definition; because it is defined by objective of activities rather than by the technology – therefore it requires broad definition and wider understanding for a government to be able to implement it successful [2, 6, 13].

*This paper should not be read as a critique to the e-government maturity models to be evaluated but rather should be read as a catalyst towards enhancing security to these models.*

The paper attempts to critically investigate, evaluate and analyze eleven existing e-government maturity models, and discusses the findings in the light of research findings from four government institutions located in Tanzania – one of the countries located in the Sub-Saharan Africa. The rest of the paper is organized as follows: chapter two outlines the research process and methodology used, the third chapter presents an overview of e-government development maturity models and specific security related issues. Chapter four presents and discusses the research findings, and lastly conclusion and recommendation is given in chapter five.

## **2 RESEARCH PROCESS**

The research methodology used in this study is based on qualitative and quantitative methods. The process was divided it into two phases. Phase one was to conduct a desk review in the area of e-government, e-government development models, and security documentations. The second phase employs a research survey where questionnaires and in-depth interviews were conducted. This phase was later complemented with documentation reviews from the studied settings such as e-government strategies, and ICT security policies. Six Tanzanian government institutions including ministries, departments and agencies were earmarked and contacted.

The Contacted groups were at the strategic level (Directors and decision makers), tactical level (Managers) and operational level (Technical staff and users). All interviewees were in one way or other

responsible for delivery of e-government services to the public. Interviews were conducted between mid to late April 2009. In the analysis process data triangulation method was used to facilitate validation and verification of research findings of primary data with secondary information. However for the purpose of this paper – findings from four institutions (three ministries and one agency) are used.

### **3 AN OVERVIEW OF E-GOVERNMENT DEVELOPMENT MODELS AND SECURITY ISSUES**

E-Government developments are influenced by so called e-government development models [9, 11, 14]. These models are specifically designed to guide the implementation and development of e-government applications in a stage-wise manner – from immature (one-way communication) to the mature (digital democracy) stage. The advantage of having a stage-wise approach is to offer governments abilities to measure the progress and also to generate momentum that could subsequently be maintained [9].

Therefore, in this section, based on the ISO 17799 security standards ten principles (*i.e Business Continuity Planning, System Access Control; System Development and Maintenance; Physical and Environmental Security; Compliance; Personnel Security; Security Organization; Computer & Network Management; Asset Classification and Control; and Security Policy*)[19], we critically investigate, evaluate, and present the short-listed widely known eleven (11) e-government maturity models, namely: Asia Pacific, Chandler and Emmanuel, Deloitte and Touche, Gartner, Hiller and Blanger, Moon, Howard, Layne and Lee, UN and DPEPA, Darral West, and World Bank. In the process, we give a synopsis of each model. Finally, the models' summary is given.

#### **3.1 Layne and Lee's four stage model**

Layne and Lee (2001) regard e-government as an evolutionary phenomenon based on the authors' observation and experience in the area. They propose four stages of e-government development. Basically, the model is based on technical, organizational, and managerial dimensions. The full description of the models' four stages is given: *Cataloging* – this stage is meant for delivery of some basic information through website. In most cases the websites are considered to be static; it enables citizens as users to access on-line presentation and downloadable forms.

## Discussing E-Government Maturity Models for Developing World – Security View

*Transactional* - is a stage that propagates the former, whereby it enables citizens to do on-line transactions (two-ways communication). *Vertical integration* – this stage focuses on the automation of more government workflows and also transformation of government services; it includes integrating government functions at different levels such as these of local and states governments. And finally *Horizontal integration* – this focuses on systems integration between different levels and functions for providing users with a unified and seamless service.

Synopsis–1: In spite of the model being focused on functionality which is grounded on combination of technical, organizational and managerial feasibility – it does not consider the potential benefit of political changes. In addition, the model design has fairly considers technical security related issues in particular at the transactional; and gave very low consideration non-technical ones, such as cultural and ethical, legal and regulatory, and economical [11].

### 3.2 Chandler and Emanuel’s four stage model

Chandler and Emanuel (2002) developed a four stage model. The narrations of the stages are: *Information* – this is a preliminary stage, were most of government services delivery is available on-line. Citizen can access government information over a website (static) – this is a one-way communication between government and citizen. *Interaction* – this is the advanced stage of the former; simple interaction between citizens and governments are enhanced; various website features and functionality are available including search, and emails; at this stage the communication is two ways. *Transaction* – refers to services that enable transactions of values between citizen and government; citizen can pay taxes, submit forms on-line. And *Integration* – this is the final stage where vertical and horizontal integration of services across government and agencies occurs. Citizen can access information on-line from one service centre.

Synopsis–2: Chandler and Emanuel [6] model focuses partly on citizen-centric and functionality. Also it gave fairly little technical security consideration at the transaction stage. However, the model ignores not only the specific non-technical security related issues but also the potential benefits of political changes [6].



### 3.3 Gartner's four stage model

Gartner group (2000) developed an e-government maturity model with four stages. These are: *Web presence* – this is the initial stage where government provides website (static) with basic information that the citizen can access. *Interaction* – government provides a website with various capabilities such as search engines, documents downloading and emails; this is used as a tool for interaction between parties involved (government, agencies and citizen). *Transaction* – citizen (users) can conduct complete on-line transaction including buying and selling activities. And *Transformation* – this is the last phase, where all government operational processes are integrated, unified and personalized.

*Synopsis-3:* In general, the model focuses on citizen-centric and partly functionality which is grounded on technology, organizational and managerial feasibility. In addition, the model partly considers technical security at its transaction stage while on the other hand the model fairly consider specific security (non-technical) related issues or the potential benefit of political changes [22].

### 3.4 United Nation's five stage model

United Nation (2001) proposed a five stage model with a focuses on web-based public service delivery. Description of the model stages are: *Emerging web presence* – this is the initial stage were government websites provides mostly basic and limited static information with less options for citizens. *Enhanced web presence* – this is the second stage were there are improvement of government websites in-terms of providing dynamic, specialized and regularly updated information. Among the website features include search facilities, on-line help, and site maps. And *Interactive web presence* – users and service providers are connected to government portals (websites); Interaction became more sophisticated than in the former stage. Services such as search facilities and accessibility of various forms are enhanced. Others are *Transactional web presence* – this stage allows two-way interactions between the citizen and the government; users can conduct complete on-line transaction including buying and selling activities. And *Seamless/Networked web presence* – this is the most sophisticated level of e-government service delivery; all services and functions across all government levels are integrated; citizens can access any kind of services from a central location at any given time.



## Discussing E-Government Maturity Models for Developing World – Security View

*Synopsis-4:* The model is centered to web-based and functionality. The model development is based on technology and managerial aspects. In addition, the model fairly considers specific issues related to technical security at its transactional stage. Furthermore, the model does not consider the potential benefit of political changes [17].

### 3.5 West's four stage model

Darral West (2000) proposed a four stage model of e-government development. The stages and description of the model are: *Billboard* – this is the stage where websites (static) are used for information display. Various types of information can be posted on the website including reports and publication; this way citizen (visitor) could easily access and consume the displayed information. *Partial service delivery* – at this stage government starts to set services on-line for citizen to access; at this level the on-line website has more capabilities and functionalities include sorting and searching of information. *Full integrated service delivery* – one stop centre is created (government portal) with full integrated online services; citizen can easily access government and agencies information from one service centre. And *Interactive democracy with public outreach and accountability* – according to West [23] this is the final stage of e-government development. Government website develops into a system wide political transformation with executable and integrated on-line services. Citizens can easily access government information and also customize the on-line government information service delivery system(s).

*Synopsis-5:* Darral West [23] model focuses on functionality and citizen-centric. In addition, the model gave fairly little consideration security (technical and non-technical) as a specific issue. However, it considers the potential benefit of political changes at its highest stage [23].

### 3.6 Hiller and Blanger's five stage model

Hiller and Blanger (2001) proposed a model with five stages, namely: *Information dissemination* – this is the initial stage of the government to disseminate information to the citizen by posting it on the website (static), the communication is one-way. *Two-way communication* – at this stage government uses enhanced websites with various capabilities such as emails and downloadable forms to interact with citizen (users). And *Service and financial transaction* – this is advanced stage than the

previous one, government offers online services including financial transaction to citizen (users). This phase requires more sophisticated technology. Others are *Vertical and horizontal integration* – the government integrates various systems at different levels vertically and horizontally. Finally is Political participation – government involves citizen in political participation activities including online voting and forums.

*Synopsis-6:* We see that the model focuses on functionality and it considers the potential benefit of political changes. However, the model gave attention to security at its financial transaction stage – and ignores other specific security related issues including these of non-technical [24].

### **3.7 Moon's five stage model**

Moon (2002) developed a five stage model. The stages are One way communication, Two-way communication, Transformation, Vertical and horizontal integration, and Political participation. However, if we compare the two models Moon (2002) and Hiller and Blanger (2001) there are large similarities in particular from stage two to five, which were already described above, under 3.6. For that reason, we only give the description of stage one of the model (*One way communication*), which is considered as the preliminary stage of e-government developments where government disseminates information to the citizen by posting on the website, and citizens can access online.

*Synopsis-7:* As the model stages are similar to Hiller and Blanger, the model focuses on functionality and also considers the potential benefit of political changes. However, the model gave attention to security at its financial transaction stage – and ignores other specific security related issues including these of non-technical [24].

### **3.8 Asia Pacific's six stage model**

Asia Pacific (2004) region based on their experience of e-government development – proposed a six stage model. The model stages and their description are: *Setting up an email system and internal network* – this is the initial stage where most of government systems focuses on internal processes that supports basic administrative functions such as e-mails and payroll. *Enabling inter-organizational and public access to information* – this stage involves government into developing systems that will help in

## Discussing E-Government Maturity Models for Developing World – Security View

managing its workflow from paper based to electronic format (inter-organizational); Also at this stage citizen (public) are able to access government information through the use of internet. *Allowing 2-way communication* – government and the citizen (public) use ICT as enabler for communication. For instance telephone, fax numbers or email addresses are posted on a website, this encourage public to send messages to the government and receive response. And *Allowing exchange of value* – at this level, ICT is used to support development of more flexible and convenient ways for citizens to conduct business with the government. Citizens have the opportunity to utilize the available on-line government services including tax assessment, visa application and license renewals. Others are: *Digital democracy* – citizen use ICT as an enabler that can potentially support participatory and democratic processes. For instance use of on-line applications that empowers citizen and civil organization to vote. The final stage is *Joined-up government* - this is the final stage were there is both vertical and horizontal integration of service delivery, a web-portal integrates information and services from various government bodies/agencies. This way citizen and other stakeholders get seamless services without needing to know what government, department or agency is responsible.

*Synopsis–8*: This model focuses on citizen-centric and functionality. Also it considers the potential benefit of political changes. However, with the exception of one stage (Allowing of exchange of value) - security related issues (technical and non-technical) are not explicitly addressed as specific issues [3].

### 3.9 Deloitte and Touche’s six stage model

Deloitte and Touch (2001) presents a six stage model based on the view that e-government objectives should serve citizens building a long term relationship. The full description of each of the stage is as follows: *Information publishing* – at this stage government sets up websites (static) for providing information to citizen /users. At this stage the communication is on-way; *Official-two way transaction* – this is an advanced stage of the former were information are transacted and exchanged between citizen as users and government/agencies as service providers; *Multipurpose portal* – government uses a single portal as a single point of entry to effectively provide services to its departments,

agencies and to citizen; *Portal personalization* – this stage provides citizen/users with the opportunity to customize the portal based on their desired features; *Clustering of common services* – all government services and operational processes are clustered along common lines so as to provide unified and seamless services to citizen; and the last stage is *Full integration and enterprise transaction* – government changes its structure and provide more sophisticated, integrated and personalized services to citizen.

*Synopsis–9:* Like other models, the model focus is grounded on citizen-centric. However, apart from ignoring the potential benefit of political changes, it also gave fairly little attention to specific related security issues - technical and non-technical [21].

### **3.10 Howard’s three stage model**

Howard (2001) developed a three stage model. The stages of the model are: *Publishing* – this is the initial stage of e-government development where Information about activities of government is available online. *Interacting* – this is the advanced stage of the former, citizens have the ability to do simple interactions with governments; available services at this level include sending e-mail, chat rooms, and/or filling and sending forms. And finally *Transacting* – based on the model design this is the highest stage of e-government development. The stage enables citizens to conduct transactions over the Internet, including purchasing /payment of licenses and permits.

*Synopsis–10:* The model focuses on functionality and at the same time on citizen-centric. Unfortunately, the model does not consider the potential benefit of political changes nor the specific security related issues in particular non-technical [8].

### **3.11 Word Bank’s three stage model**

Word Bank (2003) proposed a three stage model. These are: *Publishing* – this is the first stage, government disseminates information to citizen through website; all important information is posted on the website. *Interactivity* – at this phase government interacts with citizen. Websites are enhanced with interactive capabilities such as feedback forms and email. And lastly is *Completing transaction* – this is the final stage of e-government development; citizen/users can use the opportunity of the

## Discussing E-Government Maturity Models for Developing World – Security View

available technically enhanced website to conduct complete and secure transactions on-line.

*Synopsis-11:* The model focus is on both functionality and citizen-centric. Also the model development does not consider the potential benefit of political changes. Security is addressed only at its final stage, completing transaction. Therefore the model lacks most security related issues [25].

## **4 FINDINGS AND DISCUSSION**

### **4.1 Findings**

This section presents our research findings regarding the specific related security issues and challenges.

#### **4.1.1 Security Issues and Challenges for the Evaluated e-Government Development Models**

Given the criticality of e-government applications in supporting institution/organizational core business processes, it is essential that e-government applications be implemented and operated in a secure way [5, 9, 12]. Therefore, it is imperative for e-government maturity models to include security layer that clearly defined the specific security requirements (technical and non-technical) at each of the e-government development stages. Being guided by the ISO 17799 standards ten principles [18] and the systemic holistic approach [19], we therefore highlight some specific security issues and challenges transpired in the course of this study. It is very unfortunately that from the evaluation of the eleven models presented above – very few models design had considered security as a specific issue. These models considered security mostly at the transaction stage [9]. It is imperative for e-government development models to include security layer at each of the stages. The security layers would comprise of specific technical and non-technical security related issues based on the model's stage requirement.

Stage one referred by all model as the beginning of e-government development/ implementation. Hence it requires much of security awareness and training programmes. Awareness at this level will create ownership and trust not only to government, and stakeholders but also to citizens [9, 11]. Also, at this stage the security layer should include

security issues related to: development and maintenance of e-government systems application – this will ensure security becomes part of systems operation, protection of confidentiality, integrity and authenticity of information, and also maintaining security of application system software and data; Access Control – that control access to information, prevent unauthorized access to systems, and networked services. Also Compliance matrix to security standards and personal security should be considered as part of the security layer. Furthermore the security layer should integrate non-technical security related issues including managerial and operations – at different levels; legal laws and regulations (i.e cyber laws); cultural and ethical; and economical issues – government support [4, 5, 9, 18].

Therefore, as the e-government model stages grows in terms of technological sophistication and complexity (i.e from one-way to two-way communication and so on) – the security layer needs to be updated to match with the security requirement at that particular stage of the e-government development model.

#### 4.1.2 Findings from the Research Survey

The research findings from the four institutions revealed that Tanzania has got a national level e-government implementation strategy of which is propagated to the rest of the ministries, departments and agencies (MDA's). As of today Tanzania has a total of twenty Ministries, fifteen departments, and more than seventeen agencies. In the analysis, we code the named institutions in the following order: *Ministry of Lands, Housing and Human Settlement Development (MLHHS) referred as W*; *Prime Minister's Office – Regional Administrative and Local Governments (PMO-RALG) as X*; *President's Office – Public Service Management (PO-PSM) as Y*; and *The Tanzania Ports Authority (TPA) referred as Z*.

- *The state of e-government development (e-government maturity level) –choosing Gartner's e-government development model as our reference, the research findings from four institutions revealed that all three ministries (W, X, Y) were still at stage two (interaction stage) of e-government development, while the named agency (Z) is in the process of moving towards stage three (transactional stage). Agency Z is now heavily enhancing its ICT infrastructure and resources to meet stage three functional and operational requirements.*

Discussing E-Government Maturity Models for Developing World – Security View

- *Necessity of security being part of e-government development models* – When asked if there is a need for having specific security (technical and non-technical) related issues integrated into stages of e-government development models – the result was that more than 95% of the respondent ranked it higher (fully agree). Likewise, when asked the importance of having benchmarking standards that clearly define the security requirements at each of the e-government development stage – more than 90% of interviewee ranked it higher (fully agree).
- *Ranking of requirements for security components and related issues* – when asked to rank the given security components (technical and non-technical issues) – the result was as shown in the table 1 below followed by its pictorial presentation in figure 1:

*Table 1: Survey results for how important it is deemed that technical and non-technical security requirements are addressed.*

Description of technical and Non-technical related issues	Score ranges from 0 – 100 % , 100% being Fully Agree				
	W	X	Y	Z	Average Score
Technical related security issues					
• Use of strong Access Control mechanisms	80	100	100	100	95
• Encryption of classified critical information	80	60	80	60	70
• Network security mechanism i.e use of Firewalls, IDPS, VPN	80	80	100	100	90
• Backups (BCP and Disaster recovery)	80	80	80	80	80
• Use of anti-virus and malicious codes software's	100	100	100	100	100
Non-technical related security issues					
• Managerial and operational	80	80	80	100	85
• Economical	80	80	100	80	85
• Legal and Regulatory	80	80	60	80	60.75
• Cultural and ethical	60	80	60	60	65



Proceedings of ISSA 2009

• Citizens/public trust	80	80	80	100	85
• Awareness	100	100	100	100	100

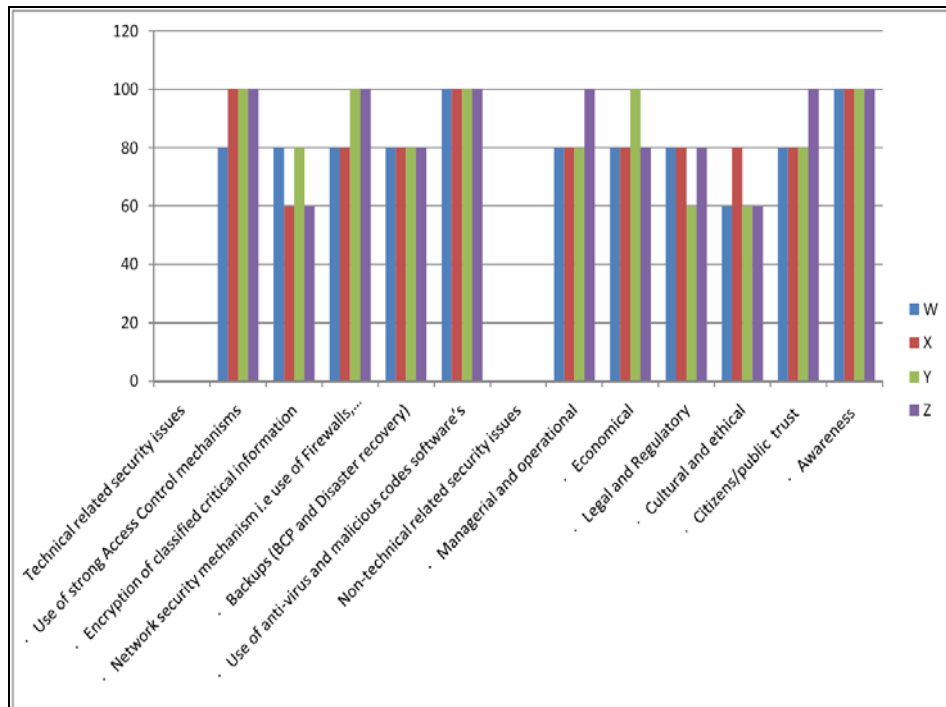


Figure 1: Security related issues (technical and non-technical) – survey results showing level of importance to be addressed

In addition, other issues related to security facets such as confidentiality of data supplied, integrity, non-repudiation, identification of who did what, services availability mechanisms and implementation were also cited as major obstacles to current e-government development in the area [15, 16].

## 4.2 Discussion

The findings analysis presented above shows that more than 40% of the eleven evaluated e-government development models did not consider security as a specific issue related to both technical and non-technical requirements. The rest of the models like Layne and Lee [11] slightly



## Discussing E-Government Maturity Models for Developing World – Security View

presented technical security related issues in particular at the transactional stage. However, the research survey conducted in four institutions, presented above, shows that for effective and efficient e-government service delivery – security related issues and challenges needs to be explicitly addressed [2, 16]. Developing a security layer that integrates technical and non-technical security related issues should be the way forward. The security layer needs to reflect the pertinent requirements of each stage of e-government development model. The security layer requirements at stage one is given in section 4.1.1. Thus, as the e-government model stages grow in terms of technological complexity (i.e from one-way to two-ways communication and so on) – it is important to have security layers at higher stages upgraded to match with the security requirements at that particular stage. Moreover, the challenge remains; currently we don't have a common e-government maturity model that reflects standard stages, i.e the same stage is now defined with different names and focus.

## 5 CONCLUSION AND RECOMMENDATION

The paper critically investigates, evaluates, analyzed and presented findings from the eleven e-government development models. The findings were later complemented with the research findings from four government institutions located in Tanzania – one of the developing countries located in the sub-Saharan Africa. In the course of the analysis ISO 17799 ten principles were used to guide the analysis and discussion. Various security issues and challenges related to technical and non-technical requirements - were presented and discussed in a wider dimension with the main focus on the e-government development model stages. Finally, the security layer was proposed. However, in the course of this process, the following are worth mentioning:

- The evaluated e-government development models focuses either on functionality, or citizen-centric or both.
- The naming of the stages, particularly stage one and two, includes many buzzwords with slightly different focus, even though the main foci were conceptually more or less the same.
- Security requirements (technical and non-technical) related issues are not the main foci for the design/ development of the model.

Proceedings of ISSA 2009

- Few models consider lower level technical security requirements; in particular at the transaction stage.
- Some of the models did consider at all neither the transactional stage nor the potential benefit of digital democratic stage.
- The security layer that comprehensively covers critical specific technical and non-technical security related requirements at all of the model stages (based on the selected/new model) needs to be developed.

Therefore, in light of our analyses and interviews, we have identified that it is demanded important for e-government development models to include a security layer at each of the model's stages. The security layers should comprise of specific technical and non-technical security related requirements based on the model's stage requirements, and possibly, founded on the ISO 17799/27000 standard principles. Though there are a number of studies focusing on reviewing the stages of existing e-government development models – development process of any new model should consider the inclusion of a security layer as a specific issue at each of the model stages.

## 6 REFERENCES

- [1] B. Bredow, M. Wimmer, (2002) A Holistic Approach for Providing Security Solution in e-Government; *Proceedings of the 35<sup>th</sup> Hawaii International Conference on System Sciences*; [Also available at <http://www.csd.computer.org/comp/proceedings/hicss/2002/1435/05/14350128b.pdf>., Last accessed on 15<sup>th</sup> of April, 2009]
- [2] Basu, Subhajit (2004) “e-Government and Developing Countries: An Overview”; *International review of law computers & technology*, Volume 18, No. 1, Pages 109-132
- [3] Clay G. Wescott “e-Government in the Asia-Pacific Region; [Also available at [http://www.adb.org/documents/papers/e\\_government/egovernment.pdf](http://www.adb.org/documents/papers/e_government/egovernment.pdf); last accessed on 05<sup>th</sup> of April, 2009]
- [4] Bishop, Matt (2006), “Computer Security – Arts and Science” *Addison-Wesley*, ISBN: 978-0-201-44099-7
- [5] C. Lambrinouidakis, S. Gritzalis, F. Dridi, G. Pernul, “Security requirements for e-Government services: a methodological approach for developing a

Discussing E-Government Maturity Models for Developing World – Security View

- common PKI-based security Policy” Elsevier. Computer Communication 26 (2003) 1873-1883
- [6] Chandler, S., and Emanuels, S.(2002), ‘Transformation Not Automation’, Proceedings of 2nd European Conference on EGovernment, St Catherine’s College Oxford, UK, 2002, 91-102
- [7] Ebrahim, Z., Irani, Z., and Al Shawi, S., ‘E-Government Adoption: Analysis of Adoption staged Models’ *Proceedings of the 3rd European Conference on e-Government; Jul 3-4, 2003; Trinity College Dublin, Ireland*
- [8] Howard, M., ‘e-Government Across the Globe: How Will ‘e’ Change Government?’, [Available at <http://www.gfoa.org/services/gfr/archives/2001/08/gfr0801.pdf>; Last accessed on 26<sup>th</sup> of March, 2009]
- [9] Irani, Z Al-Sebie M, Elliman T: ”Transaction stage of e-Government system: identification of its location & importance” *Proceedings of the 39<sup>th</sup> Hawaii International Conference on System Sciences*
- [10] J. Gil-Garcia, T. Pardo, e-Government Success Factors: Mapping Practical Tools to Theoretical Foundations; *Government Information Quarterly, 2005 - Elsevier*
- [11] Layne, K, & Lee, L. (2001). Developing fully functional e-government: A four stage models, *Government information Quarterly* 8, 122-136.;
- [12] M. Just, D. Rosmarin Meeting the challenges of Canada’s Secure Delivery of e-Government Services.[Available at [http://middleware.internet2.edu/pki05/proceedings/just-canada\\_egov.pdf](http://middleware.internet2.edu/pki05/proceedings/just-canada_egov.pdf) [Accessed on February 15<sup>th</sup>, 2009]
- [13] Ndou, Valentina, e-Government for Developing Countries: Opportunities and Challenges; [Available at <http://publications.ksu.edu.sa/IT%20Papers/eGov/unpan018634.pdf>; Last accessed 10<sup>th</sup> of March, 2009]
- [14] O. Signore, F. Chesi, M. Pallotti (2005), e-Government: challenges and Opportunities [Available at <http://www.w3c.it/papers/cm2005Italy.pdf>; Last accessed on 23<sup>rd</sup> of February, 2009]
- [15] TZ-eGov, Tanzania e-Government Strategy (2008)
- [16] TZ-ICT, Tanzania National ICT Policy, March 2003. [Available at <http://www.tanzania.go.tz/>]
- [17] UN, “Benchmarking E-government: A Global Perspective ”, Assessing the Progress of the UN Member States, Available at: <http://www.unpan.org/egovernment.asp>

Proceedings of ISSA 2009

- [18] ISO 17799, [available at <http://www.17799central.com/>, Last accessed on 20<sup>th</sup> of April, 2009]
- [19] Yngström, Louise (1996) “A Systemic-Holistic Approach to Academic Programmes in IT Security” PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, ISBN: 91-7153-521-7
- [20] Z. Zhou, C. Hu (2008), “Study on the e-Government Security Risk Management”. IJCSNM International Journal of Computer Science and Network security, VOL 8 No. 5; [Also available at [http://paper.ijcsns.org/07\\_book/200805/20080531.pdf](http://paper.ijcsns.org/07_book/200805/20080531.pdf), Last accessed on 25<sup>th</sup> of March, 2009]
- [21] Deloitte and Touche (2001), “The citizen as customer” CMA management VOL 74 No. 10, p.58
- [22] Baum C & Maio, D (2000) Gartner’s Four phases of e-government model, Gartner’s group
- [23] D. M West (2004) “E-government and the transformation of service delivery and citizen attitudes” Vol. 64, No. 1
- [24] M J Moon (2002), “The Evolution of e-Government among Municipalities: Rhetoric or Reality? [Available at <http://www.jstor.org/stable/3110357?seq=2>, Accessed on 21<sup>st</sup> of April, 2009]
- [25] World Bank (2001) Issue Note: E-Government and the World Bank. November 5, and World Bank (2003) World Development Indicators, [Available at <http://www.worldbank.org/data/wdi2003/>, Last accessed on 10 of January, 2009]

Investigating the Effect of Genetic Algorithms on  
Filter Optimisation within Fast Packet Classifiers

## INVESTIGATING THE EFFECT OF GENETIC ALGORITHMS ON FILTER OPTIMISATION WITHIN FAST PACKET CLASSIFIERS.

Alastair Nottingham<sup>1</sup> and Barry Irwin<sup>2</sup>

Security and Networks Research Group  
Department of Computer Science  
Rhodes University, Grahamstown

<sup>1</sup>anottingham@gmail.com, <sup>2</sup>b.irwin@ru.ac.za

### ABSTRACT

Packet demultiplexing and analysis is a core concern for network security, and has hence inspired numerous optimisation attempts since their conception in early packet demultiplexing filters such as CSPF and BPF. These optimisations have generally, but not exclusively, focused on improving the speed of packet classification. Despite these improvements however, packet filters require further optimisation in order to be effectively applied within next generation networks. One identified optimisation is that of reducing the average path length of the global filter by selecting an optimum filter permutation. Since redundant code generation does not change the order of computation, the initial filter order before filter optimisation affects the average path length of the resultant control-flow graph, thus selection of an optimum permutation of filters could provide significant performance improvements. Unfortunately, this problem is NP-Complete. In this paper, we consider using Genetic Algorithms to 'breed' an optimum filter permutation prior to redundant code elimination. Specifically, we aim to evaluate the effectiveness of such an optimisation in reducing filter control flow graphs.

### KEY WORDS

Genetic Algorithms; Packet Classification; Permutation Optimisation

# INVESTIGATING THE EFFECT OF GENETIC ALGORITHMS ON FILTER OPTIMISATION WITHIN FAST PACKET CLASSIFIERS.

## 1 INTRODUCTION

This paper details a preliminary investigation into the use of genetic algorithms in improving the efficiency and performance of complex packet classification tasks. This paper serves to motivate the inclusion of such techniques in the design of a GPGPU-based offline packet classifier, intended for fast classification of network telescope data. We are thus less concerned about filter update latency than we are about classification performance, as it is assumed that filter sets will rarely change. Furthermore, we are tolerant of the significant initialisation overhead required by genetic algorithm based solutions, if this may significantly improve performance, for obvious reasons.

In this section, we provide a brief overview of packet filters, and the specific optimisation which we intend to investigate.

### 1.1 A Note on Terminology

Packet filtering and classification may refer to a number of different, domain specific operations performed on packet data in order to derive or retrieve useful information. These include, but are not limited to, IP routing, demultiplexing, analysis and intrusion detection [14, 12, 4]. In this paper, packet filtering and classification refer to the analysis of arbitrary packet header information within an architecture compatible with application level packet demultiplexing.

### 1.2 Brief History

The field of packet filtering and classification has a long history of research and development, pioneered by the CMU/Stanford Packet Filter (CSPF), a memory-stack-based packet filter [10], and later by BSD Packet Filter (BPF), which provided the foundation for modern register-based filter machines [6, 4]. BPF implemented a RISC based pseudo-machine, in which filters were created using a low level assembler language, and translated into a directed acyclic control flow graph (CFG) for packet processing [10].

## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

BPF was succeeded by several similar packet filters, engineered to improve both classification efficiency and flexibility. This began with the Mach Packet Filter (MPF), targeted at the Mach micro-kernel, which introduced packet fragment handling and packet matching optimisations [16], and was followed closely by the PathFinder packet classifier, which leveraged a declarative packet-masking mechanism to match a packet against a line of cell patterns within a directed acyclic graph structure [11].

The successes of both MPF and PathFinder paved the way for the Dynamic Packet Filter (DPF), which leveraged dynamic code generation to exploit run-time information at compile time, thus improving the efficiency of filter operation [6, 4]. Dynamic code generation proved successful in reducing redundancy, often significantly, and thus was incorporated into a subsequent BPF descendant, BPF+, in the form of JIT compilation [4]. BPF+ also introduced a significant number of concurrent and interdependent optimizations, including constant folding, predicate propagation and partial redundancy elimination, in order to reduce the number of nodes in its filter tree [4]. As a result, significant improvements to overall performance were noted.

Since the introduction of BPF+, there has been relatively little development within the field of packet demultiplexing. The Extended Packet Filter (xPF) incorporated simple extensions for statistics collection into the BPF model [9], while the Fairly Fast Packet Filter (FFPF) used extensive buffering to reduce memory overhead, among other optimisations [5]. Finally, the Swift packet filter used CISC based pseudo-machine to minimise filter update latency, further reducing instruction overhead and command interdependence [15]. Despite this, a number of alternative methods for improving filter performance still remain relatively unexplored. One such method is that of filter permutation optimisation prior to control flow graph construction.

### 1.3 Problem Statement

The number of redundant operations that may be eliminated from a packet classification control flow graph is often dependent on the permutation of filters prior to optimisation. Thus, by finding an optimum permutation, a minimum control flow graph may be created, improving the efficiency of the filter program. As finding an optimum permutation of filters is analogous to the traveling salesman problem, there exists no polynomial time solution. In this paper we conduct a pilot study to assess the applicability and possible performance improvements that may result from implementing a genetic algorithm to approximate an optimum filter permutation.

## 1.4 Optimising Filter Permutation

Packet classification techniques typically comprise comparing a subset of a packets header information to a set of static values in order to identify a packet as a particular type, thus determining its destination, as well as other relevant information. When a packet filter contains more than one filter program, comparison overlap in multiple filters is nearly unavoidable. For instance, a significant proportion of protocols utilise IP within their network layer to facilitate and maintain connections, and thus filters for these protocols will all test for an IP header, introducing significant redundancy [4]. 1 provides an illustration of a simplified filter program comprising three separate filters, represented as a control flow graph.

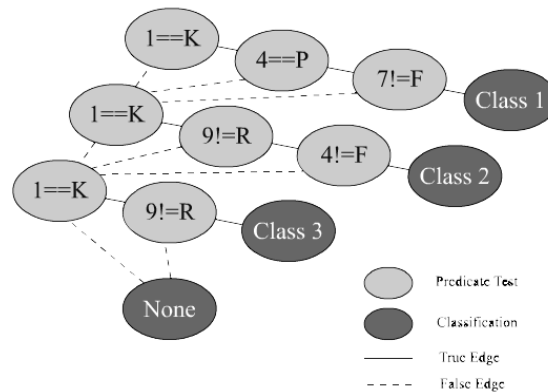


Figure 1: Filter Control Flow Graph

While the compiler optimisation techniques utilised in packet filters such as DPF and BPF+ typically eliminate a significant proportion of these redundancies, the effectiveness of optimisation is often dependent on the order in which header values are tested, which corresponds to the order of filters prior to optimisation [13]. Finding an optimum ordering of filters is thus equivalent to finding an optimum directed acyclic control flow graph, which is in turn comparable to binary decision tree [10]. As constructing an optimal binary decision tree is NP-Complete [8], finding an optimum filter permutation is a non-deterministic operation. As an example, 3 shows how the optimisation results produced from two different permutations of the filters illustrated in 2.

While a set based heuristics solution which utilises an adaptive pattern matching algorithm to find a near-optimal decision tree has been detailed



## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

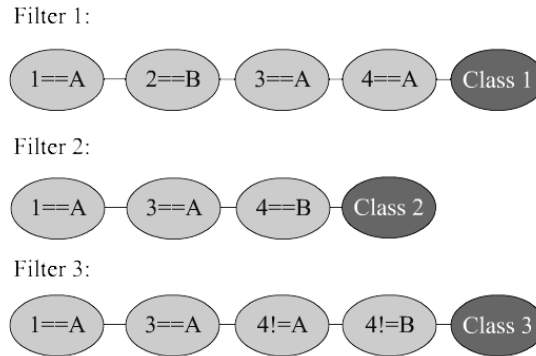


Figure 2: Filter Specification, adapted from [13].

in the literature [13], the effectiveness of the permutation optimisation is limited when the number of filters grows large. In this regard, an attractive alternative is to breed a near-optimal filter permutation using a genetic algorithm. As genetic algorithms have proven effective in NP-Complete problem spaces, including those analogous to the traveling salesman permutation problem [2], we intend to assess their effectiveness in finding an optimum filter permutation.

In this paper, we consider the feasibility of this approach by constructing a prototype simulation system to measure the effectiveness of the genetic algorithm optimisation in an abstract filter environment. As previously indicated, we are primarily interested in classification performance, as it is assumed that filter permutations will remain relatively static, with billions of packets being classified using the same control flow graph.

## 2 SIMULATION SYSTEM

This section discusses the simulation system, a rapidly developed prototype used to gauge the benefits and weaknesses of permutation optimisation using genetic algorithms.

### 2.1 Motivation

The simulation system is intended to aid in evaluating the potential for optimisation by altering filter permutation. To this end, it is necessary to specify a measure of performance that is not subject to run-time constraints, such

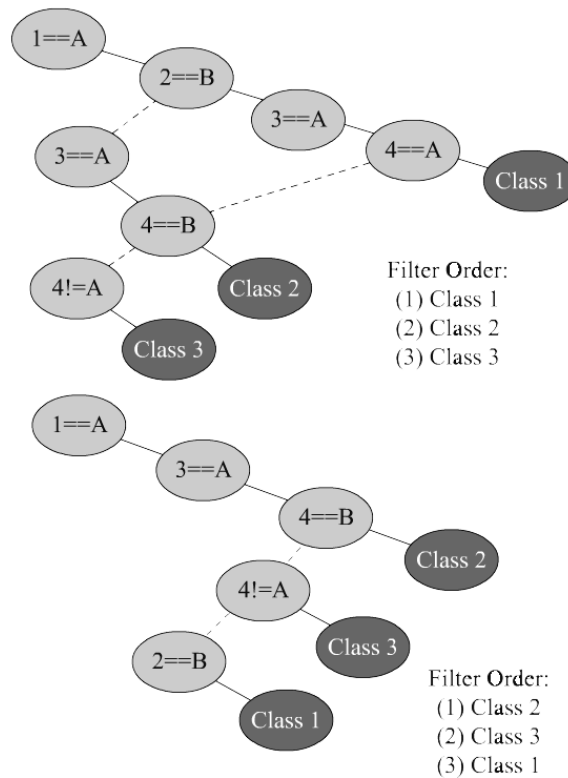


Figure 3: Control Flow Graph Reductions Using Different Permutations, adapted from [13].

as CPU clock speed or memory latency. Noting that each tree will be generated from a permutation of filters, and that the optimisation techniques used cannot create new nodes or connections, but simply remove redundant ones, we can assume that the node count of each optimised filter tree provides a satisfactory indication of the performance of that filter tree, as it indicates the absolute difference in redundant nodes eliminated by optimisation.

Using the node count as our basis for comparison, we construct a simple, abstract control flow graph generator which accepts an arbitrary permutation of a filter set as input, converts the filter permutation to a control flow graph, and reduces the resultant graph using predicate assertion propagation and static predicate prediction [4]. By comparing the node count of two trees generated from different permutations of the same filter set, where one permutation is provided by a genetic algorithm, we can infer potential performance gains without having to implement a run-time filtering process.

## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

The following sections consider the filter specification language and optimisation techniques used in generating the filter control flow graphs.

### 2.2 Filter Design

Prior to discussing the generation of filter sets in order to test optimisation, it is first necessary to elaborate on the design of the filter language used. Filters in the simulation system operate on packets containing a fixed length character array, or string. The character array is populated with random uppercase alphabetical characters, such that at any given index within the character array, there exists a random character that can be tested for equivalence against some constant character value. This forms the basis for the filter abstraction used.

Filters in the simulation system are equivalent to a chain of predicates, where each predicate compares a given packet index to a particular value, and returns true or false. In the interest of simplicity, only two comparative tests are available, namely equality and inequality. Should a predicate return true, the next predicate in the chain is evaluated until all predicates in the chain have returned true, at which time the packet is classified by the chain. If a predicate should fail, then the packet is not a member of the classification set, and is thus rejected by the filter, and processing begins on the next filter. If no filters match the packet, then the packet is not classified as a member of any set. See 1 for an illustration.

This filter design was adopted as it is both similar to typical packet filtering [13], and easy to map into a control flow graph. Furthermore, as the packets to be tested do not contain any inter-packet dependencies, in that every character in the packet is random, we are free to generate random filters without concern for relational constraints. This greatly simplifies the implementation of the simulation system, while providing for the trivial generation of random filters.

### 2.3 Automatic Filter Generation

In order to test the effectiveness of permutation optimisation in reducing the filter control flow graph, a set of filters is first required. In the interest of both generality and efficiency, we have implemented a filter generator capable of creating a filter set of arbitrary cardinality, composed of a bounded but variable number of filter predicates. In the interest of optimisation, filters

may be generated such that the indices to be tested are sorted in ascending order, improving the effectiveness of optimisation [6, 4].

In typical filtering scenarios, large volumes of packets may share common tests [6, 4], such as for TCP or IP protocols, and thus a mechanism for ensuring a specified proportion of packets contain a particular test is desirable. The filter generator facilitates these requirements, allowing for an arbitrary number of predicates to be specified and associated with an occurrence percentage value. We term these *specified predicates*. Once all specified predicates have been processed, the remainder of the chain are populated by randomly generated predicates.

The automatic filter generation component thus allows for an arbitrary set of filters to be generated, with each filter containing a number of predicates within a specified predicate-chain-length range, and a user specified degree of overlap for specific predicates.

## 2.4 Filter Optimisation

The simulation system employs a subset of typical filter optimisations, focusing in particular on the reduction of nodes within the control flow graph through a combination of predicate assertion propagation and static predicate prediction. These optimisations require the calculation of the *node dominator relationship* [1, 4] between nodes, in order to ensure accuracy. A node  $n$  is said to dominate another node  $m$  if and only if for every path to node  $m$ , node  $n$  is in that path. If node  $n$  dominates node  $m$ , then the predicate in node  $n$  is known at node  $m$  regardless of the path taken. Note that by this definition, a node implicitly dominates itself, and all nodes are dominated by the root node of the control flow graph[1]. For our purposes, a nodes dominator set may be found recursively, by finding the intersection of the dominator sets of all parent nodes.

*Predicate assertion propagation*, in its most basic form, involves the use of predecessor dominator node predicates to eliminate redundancy within in a particular path. Specifically, if an edge from a node  $n$  points to a predicate node  $m$  whose result may be determined from the dominator set of  $n$ , then the node  $m$  may be bypassed by redirecting the edge from  $n$  to the appropriate child node of  $m$  [4]. The result of this process is the minimisation of redundancy within a particular path.

*Static predicate prediction*, for the purposes of our system, is similar to pred-

## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

icate assertion propagation, in that it uses the results of dominator nodes to ascertain the result of a predicate computation without evaluating the predicate. It differs in that, while predicate assertion propagation considers the explicit computational results of a dominator predicate in optimising a path, static predicate prediction infers an implicit computational result instead [4]. Specifically, if a predicate dominator node in a path returns false, the converse of the predicate is assumed to be true, and used as an optimisation parameter in the rest of the path. Together, predicate assertion propagation and static predicate prediction provide for significant optimisation opportunities.

For instance, if a dominator node  $n$  contains the predicate “ $5==J$ ”, then predicate assertion propagation ensures that any redundant computation of this explicit predicate is removed from the path from the true edge of  $n$ . Similarly, static predicate prediction infers the implicit predicate “ $5!=J$ ”, and attempts to remove redundant computation of this predicate in the path from the false edge of the node.

### 3 GENETIC ALGORITHM STRATEGY

In this section, we discuss the particulars of the genetic algorithm employed to test our hypothesis.

#### 3.1 Introduction

Genetic algorithms are a form of adaptive algorithm modeled on natural evolution. The concept of an evolutionary algorithm was first introduced over fifty years ago as a mechanism for finding good solutions to problems within vast search spaces [3]. One such early attempt was that of an automatic programming algorithm, which attempted to evolve a binary encoded computer program capable of performing simple computational tasks, such as finding the sum of two bits [3]. Due to the lack of computational power at the time, success was somewhat limited, but subsequent technological developments and various algorithmic improvements have only supplemented the capabilities of genetic algorithms, increasing their applicability to a variety of optimisation problems.

A genetic algorithm is essentially composed of a population of individual chromosomes, where each chromosome represents, or encodes, a particular

solution to a problem. Each chromosome is assigned a fitness value, representing the efficiency of its particular solution. The initial population is typically generated randomly, and subsequent generations created by selecting two parent chromosomes from the population pool, and using them to create two new child chromosomes, each containing parts of both parents. These child chromosomes then enter the population pool, often replacing chromosomes with the lowest fitness in the process. By repeating this process for a number of generations, chromosomes with greater fitness values are slowly evolved. At some point, the process is stopped, and the best performing chromosome is selected as the solution [3]. While genetic algorithms do not guarantee an optimum solution, they are considered effective at finding near optimum solutions in relatively short time periods, making them attractive alternatives for NP-Complete problems, such as the traveling salesman problem [3].

As finding an optimum filter permutation is similar in both complexity and structure to the traveling salesman problem, we have applied a genetic algorithm to attempt to improve filter permutations such that the resultant control flow graph is minimised. In the following subsections, we discuss the specifics of the algorithm used.

### 3.2 Chromosome Representation

Before detailing the specifics of the employed genetic algorithm, it is first necessary to briefly describe our permutation representation. Chromosomes are represented as integer arrays, with a length equivalent to the total number of filters within the filter set. We then assign a unique numeric value to each filter, where each value corresponds to the filters position in the original filter set. The goal of our genetic algorithm is to permute these values into an optimum order, such that when the filters within the filter set are placed in the order of their identifiers within the chromosome, a near-minimal control flow graph is generated. Thus, the fitness of a chromosome is equal to the number of nodes eliminated from the resultant control flow graph after optimisation of the chromosomes filter permutation.

### 3.3 Selection

Chromosome selection is the process of selecting suitable parents from the current chromosome generation, in order to breed a new generation. The primary goal of the selection process is two-fold, namely improving upon current

## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

solutions, and exploring yet undiscovered solutions to a particular optimisation problem [3]. Numerous selection methods exist, from simple elitist methods which select the best performers from the chromosome population, to more sophisticated techniques such as adaptive selection and tournament selection [3]. For the purposes of our prototype, a proportional mechanism known as Roulette Wheel selection is used.

Roulette wheel selection is one of the most common selection mechanisms used today, and is considered as one of the simplest to meet the requirements of both improvement and exploration of the solution space. Simply put, roulette wheel selection is analogous to a roulette wheel, where the chance of selecting a chromosome as a parent is directly proportional to its fitness. To achieve this, the total fitness of the chromosome population is calculated by finding the sum of the fitness of each individual. We then designate a slice of this total to each chromosome, such that each slice is equivalent in size to the fitness of that chromosome. Finally, we randomly select a value between zero and the total fitness value, and determine the chromosome associated with the slice that value falls into.

While roulette wheel selection is sufficient for our purposes, more sophisticated methods may improve convergence to an optimum permutation, and the quality of the final result.

### 3.4 Crossover

The crossover operation is responsible for the re-composition of two parent chromosomes into their constituent child chromosomes. Much like selection, a myriad of crossover algorithms exist, each boasting particular strengths and weaknesses [3]. At its most simplistic, crossover involves splitting the parent chromosomes in a designated way, and then using the resultant pieces to create two child chromosomes, where each child contains pieces of both parents. For binary encoded problems, it is often sufficient to simply split each parent at a random point, creating two pieces, and then using these pieces to create the child chromosomes such that each child contains the first piece of one parent, and the second piece of the other parent. As this particular method is not well suited to permutation problems, we have opted for a more sophisticated crossover method, tailored for permutation optimisation. We detail this method below.

Recall that our chromosome representation is a simple array of unique numeric identifiers. Our first step is to compare both parent chromosomes, and

locate all those identifiers which are in the same index position within the identifier array, and copy these values to the same position within both child chromosomes. This allows for the conservation of the most beneficial permutations. This leaves a set of  $n$  identifiers, where  $n$  is less than or equal to the number of filters in the filter set. We then take the first  $\frac{n}{2}$  remaining identifiers from the first parent, and place them in order into the first  $\frac{n}{2}$  available indices of the first child, and fill the remaining indices with unused identifiers in the order they appear in the second parent. This process is repeated for the second child, with the order of parents reversed.

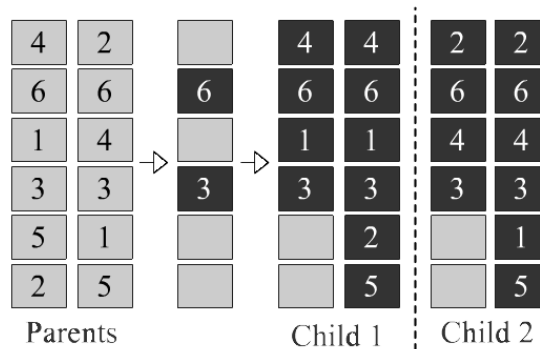


Figure 4: Crossover Operation

While crossover is of vital importance to the success of a genetic algorithm, it is often beneficial to allow a few parent chromosomes to survive intact into the next generation. To facilitate this, we use a crossover rate percentage of 70%, where the remaining 30% of crossovers result in child chromosomes identical to their respective parents.

### 3.5 Mutation

Mutation is responsible for small changes in children that are not inherited from their parents, and operates on individual components of a chromosome. Due to the purely random nature of mutation, the chance that a particular index of a chromosome is mutated, termed the mutation rate, is typically very small, to ensure that information inherited from parents is not regularly and excessively contaminated.

As mutation occurs at the component level within a chromosome, we iteratively cycle through the indices of the chromosome, allowing a 0.3% chance of



## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

mutation at each index position. This involves selecting another chromosome index at random, and swapping the filter identifiers contained within them. This ensures that no identifier occurs more than once within a chromosome, preventing corruption.

### 4 PRELIMINARY RESULTS

In this section, we discuss the preliminary findings regarding the use of a genetic algorithm to improve filter efficiency.

#### 4.1 Filter Improvement

Of primary interest, with respect to this pilot study, is the potential for increased filter efficiency through permutation optimisation alone. In this regard, preliminary findings are optimistic, with notable improvements measured in a number of test cases. To investigate the hypothesis that permutation impacts significantly on filter permutation, we generate a random filter set of a specified size and composition, and compare the node count of the resultant control flow graphs constructed using both the original and optimised filter permutation configurations. To this end, we have created three distinct test sets, each containing several results. These are enumerated below.

The first test set is conducted on ten filters, with each filter containing five to ten predicates. There is an 80% chance that a filter contains the predicate “ $2==K$ ”. Five tests were run with the predicates in index order, with the other five in random order. Results are shown in figure 5. In almost all test cases, the genetic algorithm reduced the standard reduction node count by over 20%. Note that in the second trial, the genetic algorithm was unable to find a better permutation solution than that of the standard permutation, making it the best known solution.

The second test set is intended to illustrate performance over a large number of longer filters. Results, provided in figure 6, show considerable improvement in several trials, at the expense of increased computation time.

Finally, we consider a complex filter environment, lacking any explicit redundancy. Furthermore, both population size and generation count are increased, to obtain high quality solutions. While the processing cost was significant, resulting from the need to construct 125 000 relative complex

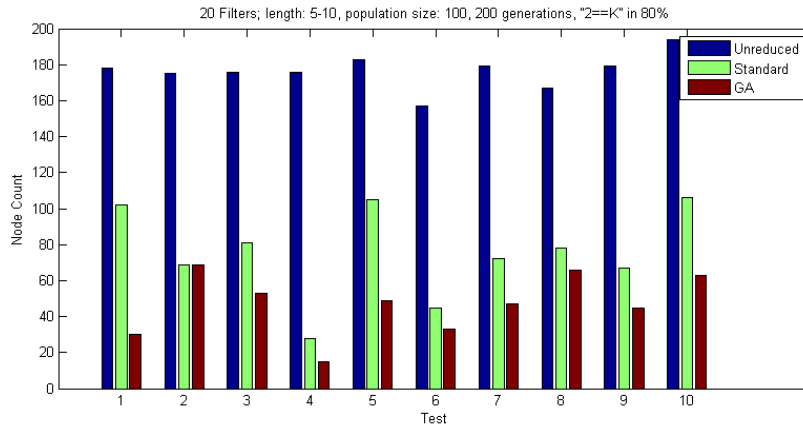


Figure 5: Test Set 1: 20 filters; length: 5-10; population size: 100; 200 generations; “ $2=K$ ” in 80%

trees, as opposed to the 20 000 trees required by the algorithm in the second test set, considerable improvement is noted in several trial cases, as illustrated in figure 7. This implies that the algorithm performs well in complex environments, given sufficient computational resources.

## 4.2 Genetic Algorithm Performance Considerations

The genetic algorithm has shown promise in filter optimisation. However, the computation time necessary is roughly proportional to both the complexity of the filter environment, and number of independent chromosomes in the genetic algorithm, as these correspond to the time necessary to reduce a single tree, and the number of such trees that need to be constructed respectively. If the chromosome population size is  $m$  and the algorithm runs for  $n$  generations, then a total of  $nm$  trees need to be reduced in order to calculate node count. Thus, we may reduce the computational time necessary to complete permutation optimisation in two distinct areas, namely the time spent optimizing an individual graph and counting its nodes, and the number of chromosome evaluations performed before a suitable solution is presumed to be found. We consider these briefly.

By improving the efficiency of the tree reduction and counting mechanisms of the control flow graph, we may reduce the number of calculations by roughly  $kmn$ , where  $k$  represents the average reduction in graph optimisation and node counting cost.

## Investigating the Effect of Genetic Algorithms on Filter Optimisation within Fast Packet Classifiers

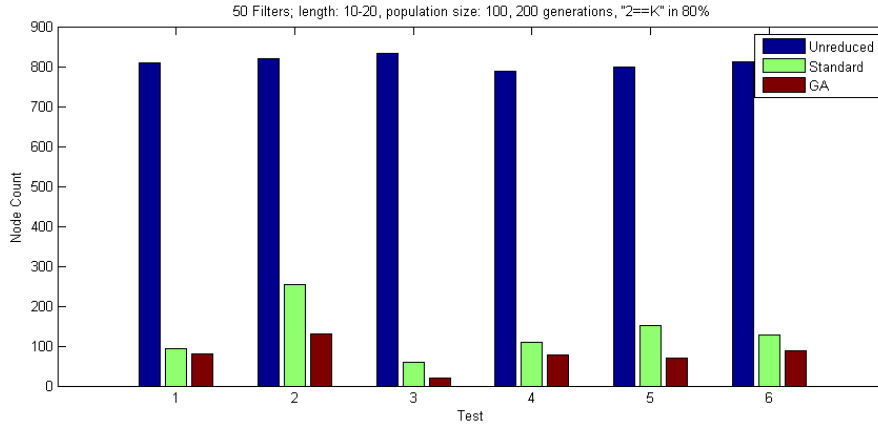


Figure 6: Test Set 2: 50 filters; length: 10-20; population size: 100; 200 generations; "2==K" in 80%

In order to reduce the number chromosome evaluations performed, we need to improve upon the values  $n$  and  $m$ . Firstly, the use of chromosome operators better suited to the task at hand is warranted. By utilising operators tailored to this problem, the rate of convergence to an optimum solution may be increased, reducing the requirements placed on both population size and generation count [3]. Specifically, Fuzzy Adaptive Genetic Algorithms (FAGAs) have shown significant potential in similar problem spaces, as they adapt breeding parameters dynamically in order to improve results [7]. This is, however, beyond the scope of this paper. Secondly, as genetic algorithms are parallel in nature [3], an implementation targeted at a parallel architecture such as multicore GPUs may reduce breeding time by a factor of  $m$ , as the entire population may be computed concurrently, spread over the number of cores available. An added benefit of this is that the population size may be increased to the number of cores available, without incurring significant delay.

While minimising filter generation time is important to some degree, rapid generation is not imperative, given its intended purpose as an offline packet classifier. Thus, we consider a generation time of several hours to be undesirable, but acceptable.

### 4.3 Limitations of Findings

As this paper represents a pilot study into the applicability of genetic algorithms to filter permutation optimisation, several limitations are evident.

Proceedings of ISSA 2009

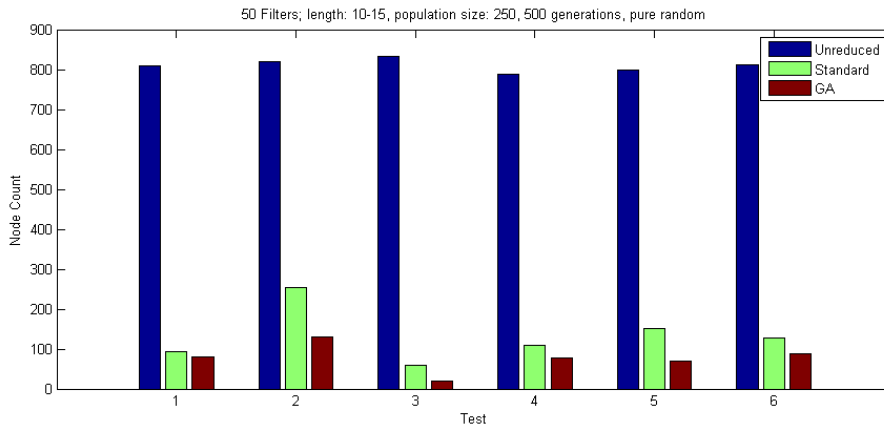


Figure 7: Test Set 3: 50 filters; length: 10-15; population size: 250; 500 generations; pure random

Firstly, we have considered the final node count within a control flow graph as the only measure of chromosome fitness. While a reduced final node count is an acceptable indicator of improvement, such improvement is not guaranteed. Numerous factors affect control flow graph efficiency, including the average path length, and the composition of incoming packets. While we have not used these measures to gauge fitness within our pilot genetic algorithm, such metrics may be incorporated into a more sophisticated implementation.

Secondly, due to the simplicity of the implemented filter system, results only indicate an approximate potential for improvement. Given that an actual packet filtering system relies upon numerous and diverse predicate and computational operators which may ultimately influence the level of success attainable by optimising filter permutation, our results do not guarantee similar performance in an actual filtering system, but simply indicate that such performance improvements are conceivably possible.

Finally, we note the limitations of the simple filtering system implemented. As the generation of filters is performed at random, the possibility of generating overlapping definitions, or unreachable classifications, is not only possible, but highly probable in large filter sets, given the limitations on indices, comparison operators, and character values. This further implies that a change in permutation may ultimately change the classification of a packet, if two similar filters have their order reversed. While such instances are of concern, in an actual filtering system they may be mitigated through the use of both detection functions, and the ability to enforced ordering of filters.

Investigating the Effect of Genetic Algorithms on  
Filter Optimisation within Fast Packet Classifiers

## 5 CONCLUSION AND FUTURE WORK

The simulation system discussed in this paper, while limited in many respects, demonstrates the possibility for significant filter efficiency improvement through the application of a well tailored evolutionary permutation optimisation approach. The simple genetic algorithm employed to test this hypothesis produced numerous control flow graphs containing less nodes than their unoptimised counterparts, illustrating the potential of such an approach in a real packet classification system. Given the breeding overhead required by genetic algorithms, such techniques may not be beneficial in dynamic filter environments, but is well suited to those in static environments. We thus intend to apply this knowledge to the development of a packet filter architecture which efficiently leverages genetic algorithms in unison with GPU processing, with the express goal of improving offline packet classification performance in complex filter environments.

### References

- [1] AHO, A. V., LAM, M. S., SETHI, R., AND ULLMAN, J. D. *Compilers: Principles, Techniques, and Tools (2nd Edition)*. Addison Wesley, August 2006.
- [2] BACK, T., AND HOFFMEISTER, F. Adaptive search by evolutionary algorithms, 1992.
- [3] BCK, T. Evolutionary algorithms in theory and practice, February 1994.
- [4] BEGEL, A., MCCANNE, S., AND GRAHAM, S. L. Bpf+: exploiting global data-flow optimization in a generalized packet filter architecture. *SIGCOMM Comput. Commun. Rev.* 29, 4 (1999), 123–134.
- [5] BOS, H., BRUIJN, W. D., CRISTEA, M., NGUYEN, T., AND PORTOKALIDIS, G. Ffpf: Fairly fast packet filters. In *In Proceedings of OSDI04* (2004), pp. 347–363.
- [6] ENGLER, D. R., AND KAASHOEK, M. F. Dpf: fast, flexible message demultiplexing using dynamic code generation. In *SIGCOMM '96: Conference proceedings on Applications, technologies, architectures, and protocols for computer communications* (New York, NY, USA, 1996), ACM, pp. 53–59.

Proceedings of ISSA 2009

- [7] HERRERA, F., AND LOZANO, M. Fuzzy adaptive genetic algorithms: design, taxonomy, and future directions. *Soft Computing - A Fusion of Foundations, Methodologies and Applications* 7, 8 (August 2003), 545–562.
- [8] HYAFIL, L., AND RIVEST, R. Constructing optimal binary decision trees is np-complete. *Information Processing Letters* 5 (1976), 15–17.
- [9] IOANNIDIS, S., AND ANAGNOSTAKIS, K. G. xpf: packet filtering for low-cost network monitoring. In *In Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR)* (2002), pp. 121–126.
- [10] MCCANNE, S., AND JACOBSON, V. The bsd packet filter: A new architecture for user-level packet capture. pp. 259–269.
- [11] MCMURCHIE, L., AND EBELING, C. Pathfinder: A negotiation-based performance-driven router for FPGAs. In *FPGA* (1995), pp. 111–117.
- [12] TAYLOR, D. E. Survey and taxonomy of packet classification techniques. *ACM Comput. Surv.* 37, 3 (2005), 238–275.
- [13] TONGAONKAR, A. S. Fast pattern-matching techniques for packet filtering. Tech. rep., 2004.
- [14] VASILIADIS, G., ANTONATOS, S., POLYCHRONAKIS, M., MARKATOS, E. P., AND IOANNIDIS, S. Gnort: High performance network intrusion detection using graphics processors. In *RAID '08: Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection* (Berlin, Heidelberg, 2008), Springer-Verlag, pp. 116–134.
- [15] WU, Z., XIE, M., AND WANG, H. Swift: a fast dynamic packet filter. In *NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation* (Berkeley, CA, USA, 2008), USENIX Association, pp. 279–292.
- [16] YUHARA, M., BERSHAD, B. N., MAEDA, C., ELIOT, J., AND MOSS, B. Efficient packet demultiplexing for multiple endpoints and large messages. In *In Proceedings of the 1994 Winter USENIX Conference* (1994), pp. 153–165.

Help Us! We Want To Be 'E-Secured': Digital Banking  
Customers' Security Needs in South Africa

# HELP US! WE WANT TO BE 'E-SECURED': DIGITAL BANKING CUSTOMERS' SECURITY NEEDS IN SOUTH AFRICA

Arthur Goldstuck<sup>1</sup>, Rabelani Dagada<sup>2</sup>

<sup>1</sup> World Wide Worx,

<sup>2</sup> University of the Witwatersrand

<sup>1</sup>[arthurg@internet.org.za](mailto:arthurg@internet.org.za),

<sup>2</sup>[Rabelani.Dagada@wits.ac.za](mailto:Rabelani.Dagada@wits.ac.za)

## ABSTRACT

In the context of this paper digital banking refers to online, mobile, and Automated Teller Machine (ATM) banking. Digital banking, particularly online and mobile banking, is growing rapidly in South Africa. This is happening despite heightened security concerns, created in part by the media. The 2008 World Wide Worx and Wits Business School Digital Banking Research found that the level of sophistication related to the electronic related crime in the banking sector is extraordinary. The aforesaid research revealed that most of the digital banking crime affect online banking and ATM. The media captured the crime phenomenon by using catchy headlines. The 2008 World Wide Worx and Wits Business School Digital Banking Research employed both qualitative research approaches. Quantitative data collection method was employed at an elementary level to capture relevant statistics. Purposive sampling was used to select the participating banks. Researchers deliberately targeted the biggest banks in South Africa - Standard Bank, ABSA, Nedbank, and Investec. Although the First National Bank did not participate in the 2008 study, researchers made deductions based on previous engagement with the bank. The research findings reflect various types of digital banking related crimes and some of the measures taken by the banks. These

Proceedings of ISSA 2009

include SIM [Subscriber Identity Module] swop fraud, phishing, ATM bombings, card swapping, and card skimming.

Seeing that customers are extremely concerned about the digital banking crime, the banks are reacting to the crime swiftly with a lot of sophistication. The phishing websites are removed and suspicious emails blocked. The spoof site can be knocked off the web within 48 hours whilst the fraudsters are tracked down speedily. With the assistance of the South African Police Services, banks have managed to bring down the frequency of the ATM bombings. Some of the methods employed by the banks to combat e-crime are very controversial. For example, some of the banks hire their own hackers and bomb their own ATMs. Banks also have dedicated e-crime units and invest huge financial resources on customer education. These initiatives are yielding good results. In the medium to long term, the success of countermeasures to crime in digital banking increases client confidence. Interestingly, this study found that some banking customers did not have fears regarding mobile banking as a delivery channel.

#### KEY WORDS

Digital banking crimes, e-security, methods to fight crime, client confidence



## Help Us! We Want To Be 'E-Secured': Digital Banking Customers' Security Needs in South Africa

### 1 INTRODUCTION

The Digital Banking in this study refers to the online, mobile banking, and Automated Teller Machines (ATMs). Online Banking refers to the use of the Internet for banking transacting purposes whilst mobile banking is defined as the employment mobile devices such as cell phones to conduct banking activities. According to the 2008 World Wide Worx and Wits Business School Digital Banking Research (Goldstuck and Dagada, 2009), Online and Mobile Banking were launched in South in or around 1996 and 2000 respectively. The subscriber base for Digital Banking in South Africa reached 5719280 mark by December 2008. 3642340 of this number represented the Online Banking users, whilst Mobile Banking customers are 2076940 (Goldstuck and Dagada, 2009). This is a drastic development when one reflects on the 2006 Online Banking Report (Goldstuck, 2006). According to the aforesaid report, "Online Banking reached the one million mark in South Africa for the first time at the end of 2003, grew to 1,4-million in 2004 and 1,7-million in 2005. According to Goldstuck and Dagada (2009), the number of Digital Banking accounts has grown rapidly since 2005. The growth in Digital Banking has been happening despite security concerns by both the bankers and customers.

Other than focusing on the growth of the Digital Banking, the 2008 World Wide Worx and Wits Business School Digital Banking Research paid attention to the factors that affect the adoption of the Digital Banking services. These included the usefulness, ease-of-use, experience of the user, enjoyment, trial-ability, availability of information, self efficacy, and security. These factors were derived from the theories that deal with technology adoption. These include Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and Innovation Diffusion Theory. For the purpose of this paper, authors would mainly focus on security as a factor that affects the adoption of Digital Banking channels.

## 2 THE CRISIS OF 2003<sup>1</sup>

On 12 May 2003, Katja Hiller-Staal, the manager of the Digteby Guest House in Ridgeworth, a suburb of Bellville in the Western Cape, discovered that R30 000 was missing from her bank account with Absa. She reported the matter to the bank, and then to the police. On 27 June 2003, Helene van Tonder, a bookkeeper from Bellville, visited an ATM to draw money from her account. Her salary of R15 000 had just been paid in. But when she called up her balance, the whole amount had disappeared. Within weeks, these two women would discover they had played a role in the most tense drama in the history of online banking in South Africa. Their losses set in motion a series of events that would first appear to be a lethal blow to the industry, but would culminate in a quiet vote of confidence from the public. Van Tonder also contacted her bank, Absa, who advised her to lay a charge with the police. She was reimbursed but, on being told that somebody had gained access to her account via the Internet, she cancelled her Internet account with the bank. And both the bank and the police drew her into an intensive investigation.

On Sunday, 20 July 2003, the Sunday Times carried the news of South Africa's first case of money stolen through online banking. According to the report, the Police Commercial Crimes Unit had confirmed that week it was investigating nine cases involving thefts from Absa accounts. It appeared that the perpetrator used "spyware" to gain access to the personal computers of the victims. Internet banking information found on the computers was then used to transfer money out of their accounts. Police had confirmed total losses of R230 000 reported to them, but on Friday 18 July attorney Harry de Villiers found R300 000 had gone missing from one of his trust accounts when he went to check his statements. He said the bank had only alerted him to R10 000 that was transferred into one of his accounts earlier in the week. Absa described the crimes as "identity fraud", which they said had been "committed by a person who had gained access to clients' accounts through their own personal computers using the Internet". Group information security officer Richard Peasy pointed out that the bank's "security systems and processes

---

<sup>1</sup> This section has been adopted from the World Wide Worx's Online Banking Report in South Africa. The research report was composed by Arthur Goldstuck who is the co-author of this paper.

Help Us! We Want To Be 'E-Secured': Digital Banking  
Customers' Security Needs in South Africa

had alerted the bank to suspicious activity before these clients knew about it. The transactions were frozen and the process for dealing with potentially fraudulent transactions was instituted". However, according to Harry de Villiers, the bank had only alerted him to R10 000 that was mysteriously transferred into one of his accounts earlier in the week. When he checked his accounts more closely later, he discovered that amounts of R227 000 and R93 000 had been transferred to another account. Upon further inquiry, it emerged that the person had bought 15 laptop computers by transferring some of the money into the account of the computer company and the rest into an account at a different bank. Peasey pointed out: "As with other banking channels, no fraud can take place on Internet banking accounts without the fraudster obtaining the client's Internet banking access account number and PIN number." He said it appeared the fraudster had sent unsuspecting clients an e-mail, which, when it was opened, installed software that recorded information. "It is a new trend called spyware. This has got nothing to do with the bank. It records keystrokes, like your account and PIN number, and then it e-mails the information to a Hotmail mailbox."

Absa told Finance24 that it would repay money stolen via the Internet from the accounts of three clients, but only if an investigation by an auditor confirmed that the money had, in fact, disappear in this manner. On Monday, July 21, Banking Council spokeswoman Claire Gerbhardt-Mann announced that hackers could be using home computers to steal money from Absa Bank clients, but that they were not breaking into the systems of the bank itself: "Because they are finding it increasingly difficult to breach the banks' own security systems, they are beginning to turn to weaker links outside of these systems, for example, Internet service providers or the customers' own PCs. "In this specific instance, it appears that the loophole was not in the banks' system but that home computers are being compromised." The Banking Council advised the public to make sure that no one had unauthorised access to their computers, to install the latest anti-virus applications on their computers, exercise control over the shared folders, keep their PIN secret and to never disclose their PIN to anyone, including bank staff. On Tuesday, 22 July, after officials from the four major banks held talks in Johannesburg, Richard Peasey issued the following statement: "We took the initiative in convening the meeting to share information about this new crime with the other banks. Each of the

Proceedings of ISSA 2009

banks will use the information provided to the benefit of their own customers. Absa and the rest of the banking industry have come together to combat this new crime... Our focus is on educating and sharing information to ensure peace of mind for consumers." All four banks issued statements assuring customers of the safety of online banking, with Absa and Standard Bank launching major campaigns to make anti-virus software and firewalls available at no cost, and FNB offering a money-back guarantee. Only Nedcor did not amend its existing strategy, announcing that it had implemented additional security measures a year earlier in anticipation of precisely this kind of fraud. The very next day, ironically, on 23 July, African Bank confirmed that its web site, [www.africanbank.co.za](http://www.africanbank.co.za), had been hacked into by an unknown party on the Sunday on which the online banking fraud was first revealed. However, no permanent damage had been done, with only the home page defaced. It was replaced within a few hours.

Finance24 reported that the site, which was purely for information purposes and not used for any transactions, shared a server at an off-site service provider with other websites. "Client information is not housed by the Internet service provider and has, in no way, been impacted by the accessing of the African Bank website," the bank said in a statement. African Bank IT Executive Mike King added: "Our client records and loan data were not compromised as they reside in a completely different environment" (SABCnews.com). And then, on Thursday, 24 July, the police made their arrest. According to the chief of the Western Cape's detective services, assistant commissioner Andre du Toit, a man in his 30s had been arrested at a guest house in the province after several people had been questioned. The suspect was found with five laptops, other computer equipment and documents. The following day, Johannes Jacobus Fourie, a 35-year-old Belville man, was charged with 10 counts of fraud and theft amounting to R609 714. It was revealed that the crimes had occurred between May 12 and July 18. The money was transferred into various accounts, including those of a computer company, as payment for 15 laptop computers, and allegedly into Fourie's own account to the tune of R76 025. Western Cape provincial head of detective services Andre du Toit told a media briefing on 27 July that there had been 10 complaints between May 12 and July 18 of illegal transactions from savings, personal and other Absa accounts from Durbanville, Montagu, Stellenbosch and

Help Us! We Want To Be 'E-Secured': Digital Banking  
Customers' Security Needs in South Africa

Paarl. The value of withdrawals ranged from R2 000 to R320 000. Fourie appeared briefly in the Bellville Magistrate's Court on Monday 28 July and remanded to August 4. It then emerged that Fourie had been employed at the Digteby Guest House, which was owned by his mother. When Absa's forensic officials examined guest house manager Katja Hiller-Staal's computer, they found a joke e-mail entitled J J Fourie on it. It appears that this e-mail was linked to the sending of an e-mail message which unleashed "spyware" onto Katja Hiller-Staal's computer, allowing bank account holders' account information to be stolen and money transferred from their accounts. The case was postponed from August 4 to August 11, then to August 12 and eventually to September 16, for further investigation. Finally, on 7 October, he was released on R10 000 bail – but the number of charges he faced were increased to 55. Prosecutor Anthony Stephen told the court he opposed bail on the grounds that Fourie had continued hacking after police caught up with him, and that he might attempt to evade trial. Stephen said that charges 37 to 55 had been committed after Fourie received a warning statement on June 26 from the police, saying that they were investigating him.

Within this context, the research question was formulated as follows:

**How does the perceived risk of online and mobile delivery channels affect the likelihood of the adoption of the Digital Banking in South Africa?**

In order to answer the research question, it was necessary to answer the following sub-questions:

What kind of the Digital Banking related crimes are experienced in South African banking environment?

How does the perceived credibility of online and mobile delivery channels affect the intention to adopt Digital banking?

Which technical measures are banks employing to address online/mobile banking risks and crime?

What other measures are banks employing to deal with the risk and crime related to mobile/online banking?

What are banks doing regarding the ATM bombings?

### **3 RESEARCH METHODOLOGY**

This study on which this paper is based on employed a qualitative approach, with individual interviews, key informant interviews, and document analysis being conducted. The reason for using the qualitative approach was that respondents could constitute a rich and valuable source of information. The study went beyond the numbers and statistics.

The participants in the study were four South African banks – Investec, Nedbank, Standard Bank, and ABSA. Although the First National Bank and Wizzit did participate in the interviews, information related to these banks was obtained from their websites and public documents. According to Meulenberg-Buskens (1997:114), sampling is imperative because the researcher cannot “study everyone everywhere doing everything”. In this study purposive sampling was used; participants in this study were chosen in regard to the contribution that they could make. Other than the professionals in the banking sector, other experts were also interviewed. These include a senior lecturer in security studies, a researcher attached to security institute, an Information Technology lawyer, and a financial journalist. Some interviewees requested that their identity should not be revealed since this could harm their careers. Pseudonyms have been used against extracts of their interviews.

The study used generic techniques for qualitative data collection and analysis. The study satisfied the principle of triangulation by employing multiple data-gathering methods and sources. Data-gathering methods include interviews, documents analysis, and observation.

Data gained from interviews was analysed using open coding. A frequent comparative method was applied to analyse data within and between interviews. Content analysis was also applied to analyse the content of interviews. The process involved the instantaneous coding of raw data and the construction of categories. Data was analysed with the intention to distinguish common patterns and to put together categories; these were weighed against the literature and collected documents from the banks. These categories were used to answer all the research

questions. Data collected through document analysis was analysed through content analysis.

## 4 FINDINGS OF THE STUDY

Due to space constraints, this paper will only focus on the findings obtained through the interviews.

### 4.1 There are several types of Digital Banking related types in South Africa

#### 4.1.1 Skimming

Fraudsters use skimming devices to harvest the credentials of the cheque or credit card owner. Skimming “usually happens in restaurants and hotels, the cashier or waitress would take your card away to process the payment behind the counter. Your card would then be swiped through the device and thus your User ID and password would be extracted improperly. Alternatively, both sides of your card may be photocopied.”<sup>2</sup> The criminal downloads the gathered information from the device into a computer. The next step would be to use the downloaded information to produce a fraudulent card. “But in actual effect, the criminal can use the photocopied information successfully without necessarily manufacturing another card.” These kind of crimes have made South African banking system to be more smart and superior compared to their counterparts worldwide: “the vendor machine that enables a customer to pay their bills in their tables without giving away their cards was initiated in South Africa to thwart crime.”<sup>3</sup>

#### 4.1.2 SIM card swop

The *SIM [Subscriber Identity Module] card swop* fraud is referred to as “*SIM card swapping or cell phone hijacking*”. In this particular crime, criminals would ask the victim’s cell phone service provider to transfer the existing cell phone number onto a new SIM card by pretending to act on the victim’s behalf. “*Criminals would find ways to get a copy of your authentic or falsified ID. This would convince the Vodacom, MTN, or Cell*

---

<sup>2</sup> Interview with the finance journalist

<sup>3</sup> Interview with researcher in a security institute



*C that the request is legitimate.”<sup>4</sup> By the time criminals swap the SIM card, they already have the victim’s Online Banking User ID and password. The only thing they needed would be the OTP [One Time Password] which is transmitted via the cell phone when the account holder logs in. “The possession of the swapped SIM card would enable the fraudsters to create new recipients within the online banking account of the victim. They will then transfer the victim’s money onto the fraudulently created recipients’ accounts. The fraudsters have in the past also used the OTP to increase the credit limit of the victim’s account.” When all these fraudulent transactions are taking place, the bank would be sending records of transaction to the victim’s cell phone; unfortunately the victim would not receive the alert SMS because his/her cell number has been swapped.*

After realising that cell phones were contributing to the commission of criminal activities, the Parliament of South Africa established the ‘Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002’. Amongst other things, this Act requires that the buyers of the pre-paid SIM cards should be registered by cell phones network operators so that the law enforcement agencies could identify them if and when their cell numbers are used to plan or to commit crime. A legal expert indicated that: *“the Department of Justice will announce a date in which the registration of the people who buy SIM cards commences. The delay in implementing this requirement is not justifiable, especially when you consider the fact that the Act was passed in 2002.”<sup>5</sup>*

#### **4.1.3 Keystroke logging**

Criminals would capture the computer keystrokes of the victim. *“They would do this by either deploying a piece of hardware or some software that would harvest sensitive online banking user identity of the victim. The hardware can be installed illegally into the victim’s computer whilst the software can be sent via an email as an attachment.”<sup>6</sup> The hardware or software would be recalled and the victim’s User ID and password would*

---

<sup>4</sup> Interview with a manager of Interne Banking

<sup>5</sup> Interview with a lawyer

<sup>6</sup> Interview with the researcher in a security institute



## Help Us! We Want To Be 'E-Secured': Digital Banking Customers' Security Needs in South Africa

be retrieved. Criminals will then use the harvested information to gain access into the victim's online bank account and defraud him/her.

### 4.1.4 Deposit slip scams

The criminals would deposit a cheque into the victim's account. In this instance, the victim is a merchant who is selling goods and the criminals are prospective customers who intend to purchase the goods. The copy of the deposit slip with the official bank stamp is faxed though and the victim realises the goods to criminals. *"In fact the merchant will receive the SMS from the bank alerting her that a certain amount has been deposited into her trading bank account. The criminals usually deposit the cheque on a Saturday. When the cheque is discovered on Monday to be fraudulent, the deposit to the merchant is reversed, leaving the victim out of budget."*<sup>7</sup> Alternatively, the criminals would deposit a cheque which reflects more money 'by mistake' than the actual value of the goods. This would compel the merchant to give the buyer a refund.

### 4.1.5 Spyware

The criminal put the software in the victim's computer mysteriously. This may be done either by an email attachment or *"the victim may gullibly download the spyware from the Internet. Once the spyware is in your machine, personal sensitive information will be harvested and sent back to the criminals"*<sup>8</sup>. This kind of crime happens regularly in the South African online banking environment.

### 4.1.6 Phishing and spoofing

Criminals would conduct this crime over the phone or via the Internet or as an urgent email purporting to be from the informing victims that their account information should be updated urgently. The email would contain a hyperlink, which would direct the victim to a site that appears to be genuine, *"but in fact it has been set up by cyber-criminals to gather information provided by gullible victims."*<sup>9</sup> The stolen information would allow the criminals to access the online banking accounting of the victim. Another digital banking crime which is more or less similar to *pharming* is

---

<sup>7</sup> Interview with the finance journalist

<sup>8</sup> Interview with the manager of Internet banking

<sup>9</sup> Interview with security senior lecturer

spoofing “*wherein a website that resembles the official website is developed to mislead the victims into volunteering their online banking credentials*”.

#### **4.1.7 ATM bombings**

The study on which this paper is based on found that the number of ATM bombings in South Africa had increased by a startling 3000 percent since 2005. This is new crime phenomenon in South Africa, and has surpassed world record. The criminals bomb the ATM into pieces and then collect the bank notes. During the interviews in participating banks, officials revealed that explosives stolen in mines were being used to destroy the ATMs so that criminals could gain access to cash once the machine has been broken into pieces. A researcher in a security institute claimed that the explosives illegally obtained from the gold mines are “*sold in a black market for up to 1100 times the normal price because the demand for these devices is very high. The situation is getting worse; you now have about 10 cases of the ATM bombings reported in a weekly basis. The ATM bombings have become a common crime.*”<sup>10</sup> Although all banks have had their ATMs bombed, Standard Bank claims to be the most affected: “*We have more ATMs than any other bank in South Africa and thus we are mostly affected.*”<sup>11</sup>

#### **4.1.8 ATMs do not give the right amount of money**

Some bank clients have claimed that banks robbed their money by dispensing fewer amounts than requested. A finance journalist who specialises with money matters claimed to have “*noted lots of complaints from consumers regarding this matter; this usually happens in ATMs that are found in the supermarket.*” The problem is that when clients call their banks to complain and request reimbursement, the bank refuses because the bank journal will confirm that the right amount was dispensed: “*It does not mean that banks are deliberately robbing the clients but the problem is more technical and banks have to do something about this. The rollers on the dispensing system do not push the money out adequately and thus some bank notes get stuck before they are completely out of the machine.*”

---

<sup>10</sup> Interview with a researcher in a security institute

<sup>11</sup> Interview with Itumeleng Monale, Director of Self Service Banking in Standard Bank

## Help Us! We Want To Be 'E-Secured': Digital Banking Customers' Security Needs in South Africa

During the course of the interviews for this study, banks officials refused to confirm that some of the ATMs cash dispensing problems have something to do with the criminals. Actually, they also declined to confirm that rollers in the dispensing system of some ATMs were causing problems. However, a senior lecturer in the field of security indicated that *“criminals put Card Reader (in) the ATM which would scan the clients’ card information and PIN numbers. They will then proceed and manufacture their own clients’ cards”*. Nevertheless, the research in the security institute objected vehemently to the aforementioned claim: *“As far as I know, such type of the identity theft and ATM engineering has not yet been reported in South Africa.”* The researchers of this study are therefore unable to declare conclusively if this type of crime exists or not.

### **4.2 The impact of the perceived credibility of Digital Banking to the adoption of the online and mobile channels is very little**

South African banks try to avoid creating the perception that Digital Banking delivery channels (online and mobile) are risky *“because that in its own is a huge risk.”*<sup>12</sup> The image portrayed to the customers by the banks is that the aforesaid delivery channels are credible. Be that as it may, clients are made aware of the factors that enable fraud, *“this creates awareness of fraud delicacy”*<sup>13</sup>. Notwithstanding, some customers tend to become concerned about security issues, especially when it comes to the online banking delivery channels. However, as time goes on users become comfortable with the delivery channel; that is why when the online banking was launched, *“people said they never bank on the Internet – the Internet is one of the most dangerous places”*. As the delivery channels mature, users become comfortable; so the impact of security concern has very little impact in the adoption of Digital Banking delivery channels. Officials in the banking industry were at pains to explain that customers in South Africa, especially the ‘middle and upper classes’ would rather conduct banking transactions using the Internet and mobile devices rather than frequenting the ATM. Certain security expert emphasised this point: *“You’d have heard about a gang that is observing customers when they withdraw money either from the teller or ATM; if they appear to have withdrawn a huge amount, they are then followed and*

---

<sup>12</sup> Interview with Domini Takacs, Senior Channel Manager: Cellphone & Electronic Channels in Nedbank

<sup>13</sup> Interview with Lee Albertyn, Head of Virtual Channels in Nedbank

*robbed outside the shopping mall. This kind of crime drives the rich, I mean the personal bankers to the online and mobile deliver channels.”* According to Christo Very, Managing Executive of Digital Channels in Absa, customers who are not adopting the Digital Banking channels are mostly affected by accessibility and affordability of computers and the Internet rather than the perceived lack of credibility of the Digital Banking.

#### **4.2 Banks employ advanced technical measures to fight Digital Banking crimes**

South African banks have dedicated teams of information security specialists who “combat” cyber crimes. Seeing that customers are concerned with Digital Banking crime, banks are reacting to crime aggressively and with a lot of sophistication; to avert losses, especially of assets and reputation<sup>14</sup>. Amongst other measures, phishing and spoofing websites are removed and suspicious emails are blocked before they reach the customer. This statement is supported by Christo Vrey<sup>15</sup>: *“We ensure that we have got monitoring systems, behaviour pattern analysis, and early warning systems, for example, if spoofing site is picked up worldwide on the Internet or a phishing email goes out, we typically shut the site down within 45 minutes to two hours. It doesn’t matter where it sits in the world.”* Banks are also 24 hours available to assist their customers in case they suspect they are being defrauded online. They can phone the contact centre *“and there is also a button in the Internet banking that says “do you want to report a fraud incident”, press the button – they will close your account immediately.”* Banks are also making positive progress when it comes to the thwarting of the SIM swap crime. They are working with the mobile telecommunications network operators to eliminate this crime: *“As far as mobile banking is concerned, Standard Bank has spoken with Vodacom regarding the SIM swap fraud. Vodacom has implemented a process whereby a notification SMS is sent to both the old and new SIM card regarding the SIM swaps. They also marry the serial numbers of SIM card with the cell phone’s serial number.*

---

<sup>14</sup> Interview with Kobus Burger, Head of Private Bank Account in Investec

<sup>15</sup> Managing Executive of Absa Digital Channels

## Help Us! We Want To Be 'E-Secured': Digital Banking Customers' Security Needs in South Africa

*This has helped a lot in reducing and discouraging the unlawful SIM swops.*<sup>16</sup>

Some banking officials claimed that there are instances wherein they actually literally stop the money from leaving the system fraudulently: *“we actually recovered a large percentage of money. It actually gets stopped, so there are whole set of aspects that the bank does arousing facilitating secure online banking.”*<sup>17</sup> Banks ensure that online banking transactions are taking place in a secure encrypted environment. It is impossible for the criminals to intercept these kinds of transactions because of encryption. The signature by the end side of the encryption is done by certificate imbedded in systems in the bank, in browser, so whenever customers see the lock, they know they are in the genuine banking website. Other than the lock, users would also look at the URL.

Some of the methods employed by the banks to combat e-crime are very controversial. These include the fact that some of the banks hire their own hackers and bomb their own ATMs. Working very closely with the law enforcement agencies and the South African Banking Risk Information Centre, banks have managed to bring down the level of the ATMs bombings. The South African Police Service's National Intervention Unit has been in the forefront of curbing the ATMs bombings. This has been achieved by arresting and killing the criminals responsible for this crime. Some of the intended ATMs attacks were foiled by the banks working together with the police. A Director of the Standard bank Self-Service Banking claimed that: *“Due to the fact that our ATMs are mostly hit, we decide to enhance the security around the ATMs. New ATMs are less penetrable and are environmentally friendly in case they are successfully bombed. The bank has mechanisms to detect when ATM machines are being tempered with. We have worked very closely with the police and about 400 perpetrators have already been arrested.”*

### **4.3 Banks spend billions of rands to train users in security**

Customer training helps to improve the perceptions regarding the credibility of the Digital Banking delivery channels. Banks also avoid

---

<sup>16</sup> Dheena Govender, Head of Internet Banking, Self-Service in Standard Bank

<sup>17</sup> Interview with Abdul Noutcha, Webmaster of web channel for Self-Service in Standard Bank

litigation, poor adoption of cell phone and mobile delivery channels by ensuring that users are adequately trained. It is in this premise that banks have refused to pay customers money defrauded through Digital Banking crimes. Education is a priority in all the banks and thus *“there is frequent employee and customer education regarding security”*. According to Christo Vrey<sup>18</sup>: *“If we go back to 2003, where we had the incident where a client, when key logging was put onto his PC in the Eastern Cape and he was defrauded of money through cell phone engineering. The biggest criticism we faced shortly after the announcement was from the client’s point of view, “how have you kept us informed about what risks are in the Internet banking?” If I look at where we were then and where we are now, that picture has changed fundamentally; we spent many billions of rands annually as the industry around the awareness campaigns.”* Each of the four big banks posts vast security related materials on their websites. Newsletters are also sent to the clients on a quarterly basis to provide security related tips to the clients. Banks are proactive in warning the clients.

The South African banks are proactive when it comes to crime and they have got early warning mechanisms that enable to see what is happening globally regarding the security of their customers’ accounts. The aforesaid mechanisms put the South African banks in a position to be informed of security threats before they actual manifest. On the other hand, if the crime happens, affected clients are informed speedily. Information security intelligence provided to the customers has increased drastically since the first famous Digital Banking crime in South Africa 2003.

#### **4.4 Banks expect clients to be responsible for their accounts’ security**

When Digital Banking related crimes were reported for the first time in South Africa in 2003, banks would reimburse the clients. However, banks currently refuse to reimburse the clients because they are doing a lot to educate and support the clients. This includes providing clients with the “freebies” to enhance their security. Christo Vrey becomes very emphatic to stress the point: *“There are the client’s responsibilities as he conducts*

---

<sup>18</sup> Managing Executive of Absa Digital Channels



Help Us! We Want To Be 'E-Secured': Digital Banking  
Customers' Security Needs in South Africa

*his life on the internet that we cannot control, we can inform him. We will give him free of charge, the best available anti-virus application off the shelf costing between R700 and R800.”* It is the responsibility of the client to ensure that the antivirus software is deployed in his/her computer. This would assist in making the computer safe. ‘For free’, banks give an SMS when a user logs into the Internet banking: *“If you get an SMS and you are not doing the Internet banking, then there’s a problem.”*<sup>19</sup> There is a telephone number contained in the SMS that banks dispatch to the client. The client can call this number the moment they become suspicious regarding security in their Digital Banking accounts. Users should ensure that they do not conduct transaction in the unsafe computing environment like the Internet cafes.

If the client decides to ignore SMSs from the bank regarding transactions that are taking place in his account, then the bank cannot be expected to be liable: *“So if the client is going to be negligent in his behaviour, he is going to have problems. So, if you can see, if he gets an SMS at two o’clock in the morning and he is not busy working on his PC and he choose to go to sleep without contacting the bank, he will lose money and the bank cannot be liable.”*<sup>20</sup> The South African banks are becoming more sophisticated in terms of ensuring that clients are more secured in the Digital Banking environment: *“You’ll notice that at Absa, we use a bit of a different approach than most banks do in South Africa. We’ve got a two stage approach to log in, so what it does is, it gives us an opportunity to go back to the client before he is fully into online banking and confirm with the client that he’s actually at the right place. We’ve created a phrase called Sure Phrase and in essence we bring to you a message that you’ve personally personalized in internet banking that tells you before you go through with the next page. You can check if that message is there. Now, if it’s not there, that means you’re on a fake site that looks like the Absa site but is actually not. There’s a lot of sophistication there that we bring from Absa point of view to our process, that’s been very successful for us and something that we continue to educate our clients on”*<sup>21</sup>. Absa is also the only bank which has a Virtual

---

<sup>19</sup> Interview with Lee Albertyn, Head of Virtual Channels in Nedbank

<sup>20</sup> Interview with Domini Takacs, Senior Channel Manager: Cellphone & Electronic Channels in Nedbank

<sup>21</sup> Interview with Christo Very, Managing Executive of Absa Digital Channels.

Keypad for the Internet banking. The Virtual Keypad makes it impossible to steal the client banking credentials through keystrokes logging.

## 5 CONCLUSION

The findings of this study appear to reveal that the adoption of the Digital banking is not adversely affected by online and mobile delivery channels security concerns. The researchers of this study found that the crime level in South Africa is actually pushing people into Digital Banking products. One would be very sceptical to go around with a lot of cash in South African streets. Even if you have a car, it can be stolen or hijacked with your money. When the authors of this paper were busy composing the report on which this paper is based on, they read an article in *The Star* (13 April 2009) which reported on the crimes committed Bank Queue Gang. It is the authors' contention that such crimes will drive more people to adopt the Digital Banking deliver channels. According to the article: "By definition, the crime occurs when a client leaves a bank, is followed and robbed. The victims are often tradesmen, who draw large amounts of cash on a Thursday to pay their casual labourers the following day. The linchpin of the gang is the "spotter". Spotters blend in, wait in bank queues and look for a target. Sometimes, they don't even need to see the money; they hear it. They will listen for the noise of the cash machine counting out money. To make themselves appear legitimate, spotters will deposit small amounts of cash or ask a teller for change. Using a cellphone, the spotter will then quickly pass on information. They will describe what their target is wearing and sometimes even inform the "shooters" outside in which pocket the money is being held. Outside, the shooters will pick up the target and begin following on foot or by car. The actual hit is quick and sometimes the gang is violent. Bank customers are not just followed. Sometimes the robbers strike as they head to the bank to deposit money. The challenge here is the fact that this type of crime is traditionally underreported and therefore there is no sufficient data to benchmark against. Bank staff also advise clients of alternative banking products, such as electronic transfers, and warn them of the dangers of carrying large sums of money when assisting them with transactions involving large cash withdrawals." Another driver to the Internet and mobile banking is the ATM bombings. ATMs users are concerned that they may become victims of the ATMs bombings.



Help Us! We Want To Be 'E-Secured': Digital Banking  
Customers' Security Needs in South Africa

The irony of this crime is that South African banking system to be the best in the world in terms of technology sophistication. Banking in South Africa includes wireless ATMs in remote areas. Wireless signals are used to link a point-of-sale credit card reader into banking system, allowing small vendors to accept credit cards. The attendant brings a mobile payment device that allows customers in a restaurant to pay bills of their meals on their tables. The waitress does not have to go behind the counter with the customer with customers' debit or credit cards; this prevents crimes such as identity fraud and *skimming*. The South African banks are far ahead of the American and European banks regarding introduction of mobile and electronic banking products.

## 6 REFERENCES

Goldstuck, A. 2006. Online Banking in South Africa. World Wide Worx: Johannesburg.

Goldstuck, A. & Dagada, R. 2009. The 2008 World Wide Worx and Wits Business School Digital Banking Research Report. World Wide Worx: Johannesburg.

Meulenberg-Buskens, I. 1997. Turtles all the way down? -on a quest for quality in qualitative research. South African Journal of Psychology, 27(2): 111-116.

Smillie, S. 2009. Beware of deadly 'bank queue gang'. *The Star*, 13 April 2009. Independent Online: Johannesburg.

Proceedings of ISSA 2009

An Examination of the Generic Memory Corruption Exploit  
Prevention Mechanisms on Apple's Leopard Operating System

**AN EXAMINATION OF THE GENERIC MEMORY  
CORRUPTION EXPLOIT PREVENTION  
MECHANISMS ON APPLE'S LEOPARD OPERATING  
SYSTEM**

**Haroon Meer**

SensePost, Rhodes University

haroon@sensepost.com

Proceedings of ISSA 2009

# **AN EXAMINATION OF THE GENERIC MEMORY CORRUPTION EXPLOIT PREVENTION MECHANISMS ON APPLE'S LEOPARD OPERATING SYSTEM**

## **ABSTRACT**

The Win32 platform has long been the whipping boy of memory corruption attacks and malware, which has forced Microsoft into implementing aggressive anti-exploitation mechanisms into their newer Operating Systems. Apple's Mac OS X (Leopard) has had a much smoother run, both in the media, and in terms of high profile attacks and the reason for this is less clear.

In light of Apple's increased market-share, a comparison between Microsoft's defences and Apple's defences is required as the number of anti-exploitation techniques increases with time. In order to produce a side-by-side comparison, an overview of memory corruption attacks is provided and the common generic anti-exploitation techniques for these attacks are enumerated and described. For each operating system, the quality and effective of each implemented defence is evaluated.

The results of the study show that Leopard trails Windows Vista in both the number of defences, as well as the quality and effectiveness of the defences that are implemented.

## **KEY WORDS**

exploit memory corruption stack heap shellcode overflow ret-2-libc

## **1 INTRODUCTION**

This paper will cover the basics of memory corruption exploits, and will then examine how Microsoft Windows Vista and Apple MacOS X Leopard combat these attacks in their default state. The intention is to examine how Apple's Leopard measures up against the automatic exploit mitigations built into Vista.

## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

In the interest of brevity and in order to remain focused, this paper will exclude comparisons between the built in firewalls, sandboxing capabilities or attacks that are not directly related to the execution of arbitrary code through memory corruption attacks. Discussion relating to the comparison of these other security features can be found in presentations and papers delivered by developers from Microsoft and Apple respectively [1, 2].

The remainder of the paper is structured as follows: Section 2 provides background on memory corruption attacks, Section 3 details and describes generic defences against memory corruption as well as attacks that bypass the defences, a comparison and analysis is provided in Section 4 and we conclude in Section 5.

### **2 MEMORY CORRUPTION ATTACKS**

Memory corruption attacks have been publicly discussed, at least since the 1988 Morris worm, which exploited a buffer overflow vulnerability in the fingerd daemon as its primary attack vector [3]. Aleph1's seminal paper *Smashing the Stack for Fun and Profit* [4] publicised such attacks and prompted the widespread development of techniques to exploit such vulnerabilities. After many years of simply asking developers to write more secure code, operating system vendors and the designers of compilers decided to make changes to make exploitation more difficult for attackers. These anti exploitation measures now ship by default in most modern operating systems [5, 6, 7, 8] with some packages offering them as after market add-ons [9].

Memory corruption exploitation refers to the class of attacks that rely on ones ability to hijack the execution flow of a program by corrupting the applications memory space through a number of different possible attack vectors. The two most popular techniques of Stack and heap based exploitation are discussed below.

## 2.1 Stack Overflow Basics

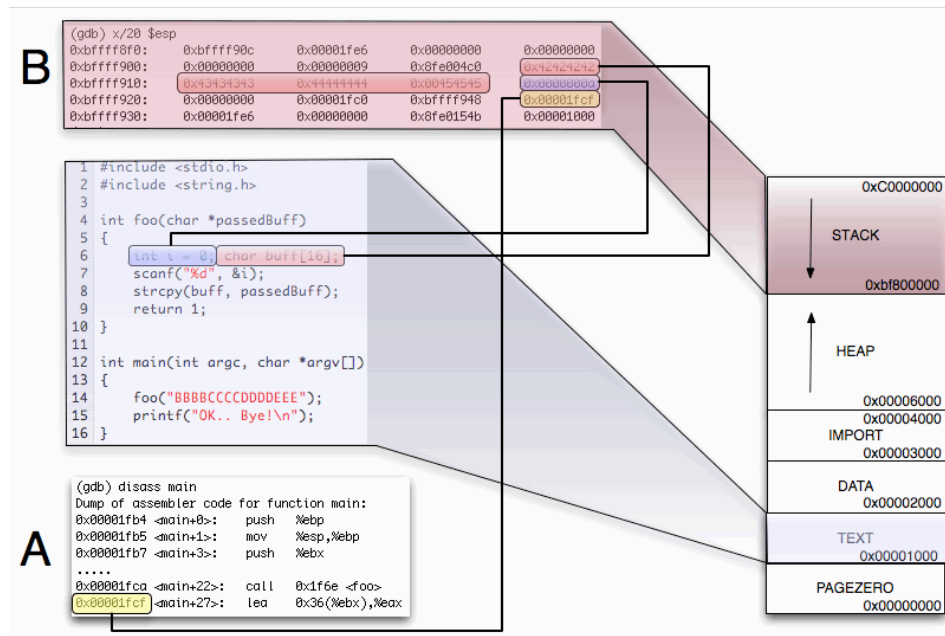


Figure 1 – Running program and its Memory Layout

The snippet of code in *Figure 1* is the canonical example of a typical stack based buffer overflow.

The disassembly of the main routine seen in the bottom left corner of the figure (labelled “A”), shows the address of the next instruction to be executed after the function `foo()` returns (`0x00001fcf`).

The top left portion of the diagram (labelled “B”) shows the state of the Stack after the `strcpy()` function has run. We see how the characters “BBBBCCCCDDDEEEE” are copied on the stack which is growing downwards towards the other local variable (`int i`) and the saved return address (`0x00001fcf`).

As can be seen from the diagram, attempting to copy a buffer of greater than 15 chars length will result in `strcpy()` copying beyond the bounds of the `buff` buffer. Enough characters and the string can continue overwriting the integer `i`, the saved frame pointer, and eventually the saved return address.

## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

Traditional stack overflow attacks aim at overwriting the saved return address on the stack. The plan would be to place executable code somewhere reachable in memory (possibly within the overflowed buffer). The address of this code is then used to overwrite the saved return address on the stack. When the function terminates, the overwritten address is popped off the stack, and execution returns to that location in memory.

### 2.2 Heap Overflow Basics

Heap overflows operate on a similar assumption to the traditional stack overflow, i.e. that the attacker has the ability to write beyond the bounds of a buffer. The major differentiator is that the heap does not hold a saved instruction pointer to overwrite, and is generally harder to tame. The overwriting of a saved function pointer on the heap [10] or overwriting of security sensitive values [11] are easy to understand and fairly commonly exploited but does not lend itself to a generic attack class.

A classic attack pattern relating to the heap however is known as “the arbitrary 4 byte overwrite”. Heap allocations (and de-allocations) are managed by maintaining a doubly linked list. Each heap chunk that is allocated includes meta-data used for heap management. The information we care about for the purposes of exploitation is traditionally referred to as the flink and blink pointers (*ptr->next* and *ptr->previous*).

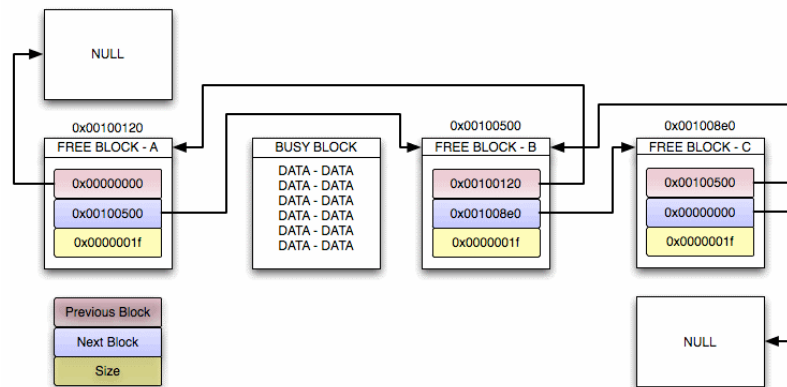


Figure 2 – The Free-List Linked List

Figure 2 is an example of the Free-List linked list, which maintains the chain of free heap memory on an OS X machine.

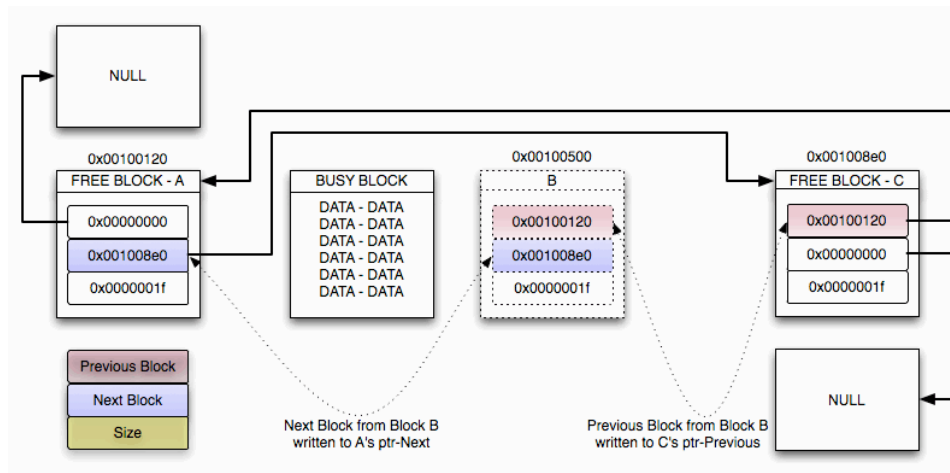


Figure 3 – The effects of an UNLINK operation

Figure 3 demonstrates what happens during a normal unlink operation, when a heap chunk is allocated. When FREE BLOCK-B is unlinked and removed from the free list, the unlink operation updates the *ptr->next* record of its *ptr->previous* block (FREE BLOCK-A) with its own *ptr->next* value (0x001008e0) and updates the *ptr->previous* record of the block pointed to by its *ptr->next* block (FREE BLOCK-C) with its own *ptr->previous* value (0x00100120).

Clearly an overflow in chunk-BUSY\_BLOCK would allow an attacker to overwrite the meta-information of FREE BLOCK-B (0x00100500) including the *ptr->next* and *ptr->previous* pointers. Controlling these pointers means that we are able to write an arbitrary 4-byte value (taken from B's *ptr->next*) to an arbitrary location (pointed to by B's *ptr->previous*) in memory.

This attack vector is fairly well understood and explored in the Win32 and Linux worlds.



## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

### 3 GENERIC DEFENCES (AND THEIR BYPASSES)

While specific defensive coding techniques are necessary to completely address vulnerabilities in code, several generic defenses have been introduced into most operating systems over the past few years. The most popular of these are discussed below.

#### 3.1 Non Executable Stack

Although quickly worked around by researchers like Rafal Wojtczuk [12] and John McDonald [13], one of the first generic defences against memory corruption attacks was the introduction of the non-executable stack [14]. This protection (as implied by its name) aims to ensure that even if an attacker is able to redirect execution flow into his attacker controlled buffer (traditionally stored on the stack), the code would not execute, since the stack would be marked non-executable.

Today the Windows Family (XP, Vista, Win2k3) and Mac OS X (Leopard) operating systems make use of modern processor advances (NX bit) [15] to mark the STACK segment as non-executable. This can be tested fairly easily. To illustrate this, one can copy shellcode [16] to a locally declared buffer that is stored on the stack and make use of a function pointer to execute this code. The code can be seen below in *figure 4*.

```

1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4
5 /* osx_ia32_bind - LPORT=4444 Size=112 Encoder=PexFnstenvSub http://metasploit.com */
6 unsigned char scode[] =
7 "\x31\xc9\x83\xe9\xea\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\xf1"
8 "\x77\x06\x47\xb0\x71\xa0\xc6\x89\x4b\x7d\x76\x8a\xaf\x12\xe8\x59";
9
10 int main(int argc, char *argv[])
11 {
12     void (*f)();
13     char stack_shellcode[113];
14     memcpy(stack_shellcode, scode, sizeof(scode));
15     f = (void (*)()) stack_shellcode;
16     f();
17 }

```

*Figure 4 – Executing code from the Stack through a function pointer*

Running the code in *Figure 4* causes a Segmentation Fault, and examining the program in a debugger yields the following error:

```
(gdb) run
Starting program: /Users/haroon/stuff/research/issa09/code/stack-exec
Reading symbols for shared libraries ++. done

Program received signal EXC_BAD_ACCESS, Could not access memory.
Reason: KERN_PROTECTION_FAILURE at address: 0xbffff8bb
0xbffff8bb in ?? ()
```

*Figure 5 – Kernel Failure when attempting to execute code from the stack*

One can tell clearly that OS X has thrown an `EXC_BAD_ACCESS` error while trying to execute code at `0xbffff8bb` (an address on the stack).

### **3.2 Bypassing the Non-Executable Stack**

Ret-2-libc (return to libc), another widely known attack pattern, evolved quickly to deal with non-executable stacks [17]. This pattern relies on the fact that even if the stack is marked as non-executable, library code is reachable within the processes memory space and is marked as executable. In its most common variant, the attacker will aim to overwrite saved EIP (Execution Instruction Pointer) with the location of the system command (which traditionally resides in libc, explaining its name), while preparing a fake stack frame containing the arguments to be passed to the system call. (In the canonical ret-2-libc attack, the attacker passes “/bin/sh” as the parameter to system, in order to launch a shell).

With enough creativity, multiple fake frames can be constructed with chained return-2-libc calls which can be used to devastating effect. In 2007 it was a ret-2-libc attack that did the heavy lifting of jail-breaking the iPhone after the initial libtiff vulnerability [18] was exploited [19].

### **3.3 Non Executable Heap**

With the stack being off-limits as a destination for attacker supplied code, the next logical target is the process heap. Several innovative techniques sprung up to cater for this with one of the most impactful being the Heap Spraying technique described by Skylined [20]. Realising that calls to create or concatenate JavaScript strings result in these strings being created on the heap, Skylined made use of a simple loop construct to create multiple copies of his string (encoded shellcode) on the heap. He

## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

then redirected execution to the heap where his shellcode would run. (The technique is called “spraying” since, in the absence of knowing the exact location of the shellcode on the heap, the attacker creates multiple copies of the shellcode on the heap (preceded by large NOP sleds) in order to increase the likelihood that a jump to the heap would result in code execution.)

Skylined’s heap spraying attack targeted Internet Explorer but subsequent attacks have applied the same technique to Adobe Acrobat Reader [21] and SQL Server [22]. In 2006 Alexander Sotirov took this vector to a new level with a paper titled *Heap Feng Shui in JavaScript* [23], which refined the use of JavaScript to give surgical accuracy over the Heap for such attacks.

Starting with Windows XP-SP2, the heap is also marked as non-executable, to some degree mitigating this problem (unless a process specifically marks the page as executable instead.) While *vmmstat* on OS X reports the heap as non-executable, it appears as if the processors NX capability is not utilized to protect this area, allowing code to be executed on the heap. Sample code to validate this (which executes with no error) is shown in Figure 6.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

/* osx_ia32_bind - LPORT=4444 Size=112 Encoder=PexFnstenvSub http://metasploit.com */
unsigned char scode[] =
"\x31\xc9\x83\xe9\xea\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x1f"
"\x77\x06\x47\xb0\x71\xa0\xc6\x89\x4b\x7d\x76\x8a\xaf\x12\xe8\x59";

int main(int argc, char *argv[])
{
    void (*f)();
    char *heap_shellcode = malloc(sizeof(scode));
    memcpy(heap_shellcode, scode, sizeof(scode));
    f = (void (*)()) heap_shellcode;
    f();
}
```

Figure 6 – Code to execute shellcode from the heap

### 3.4 Safe un-linking of Heap Chunks

With XP-SP2 Microsoft introduced the concept of safe unlinking during memory management [24]. Before using the *flink* and *blink* pointers (discussed earlier), the heap allocator checks to ensure that *flink->blink* and *blink->flink* both point at the current block. This prevents an attacker from using the unlink operation to perform an arbitrary 4-byte overwrite. With XP-SP2, Microsoft also includes a single byte cookie in the heap metadata which is checked during unlink [25]. An incorrect cookie value indicates that heap corruption has taken place. Vista takes this protection further by encrypting important metadata (XORing the metadata with a random 32bit value) and decrypting it before use. At the time of writing no such protection exists within OS X Leopard.

### 3.5 Address Space Layout Randomization (ASLR)

All of the attacks discussed above rely on the attacker being able to predictably locate objects in memory. Without this ability, most remote execution attacks (resulting from memory corruption) can be mitigated down to process crashes. Following from the pioneering work on the PAX project [26], researcher Matt Miller released *WehnTrust* [27], which offered full address space layout randomization on the Windows platform, and Microsoft introduced ASLR with the release of Windows Vista. Early versions of the implementation suffered from flaws and extensive work was done by Ollie Whitehouse to examine the amount of randomness in the Vista ASLR implementation [28]. Today Windows XP, Vista and Server 2003 boast an ASLR implementation that poses a significant hurdle to an attacker who is un-aided by a supplementary bug that leaks memory layout information.

Apple's implementation of ASLR however leaves a lot to be desired and in its current incarnation has been dubbed by some researchers as Partial Library Randomization [29]. Leopard only randomizes the addresses of most libraries within the process memory space. This ignores the randomization of the stack, the heap, the image itself or even the address of some key libraries in a race where a single predictable location can result in the race being lost. In addition to this the current random locations are documented in the world readable file `/var/db/dyld/dyld_shared_cache_i386.map` allowing system local attackers the full knowledge necessary to carry out an attack [29].

## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

### 3.6 Compiler Level Protections

Crispin Cowan first introduced *Stack Guard* in 1998 [30]. A compile time protection, Stack Guard worked by placing a virtual canary on the stack in front of the saved return address. Any attempt to overwrite the return address would also result in altering the canary which is checked when the function returns. Microsoft independently created the `/GS` (Guard Stack) compiler flag to obtain the same results [31]. This protection has come under fire several times and Microsoft's '`/GS`' implementation has been through several iterations, until finally arriving at today's version which includes advanced heuristics at compile time to re-order variables on the stack. This means that in the example application shown in *Figure 1*, the compiler would have re-ordered the variables so that *buff* would not have been able to overflow the *i* integer.)

Although not as advanced in all respects as its `/GS` counterpart, Leopard ships with a version of GCC that supports stack protection through the *ProPolice* project and the `-fstack-protection` compile time option. While researchers like Whitehouse [28] and Maynor [32] have released tools to identify which binaries on a Vista machine are not compiled with `/GS` protection, the situation on Leopard is almost perfectly reversed, with the majority of applications on Leopard having not been compiled with this kind of protection enabled.

### 3.7 Caveat

We have ignored an entire attack pattern by failing to discuss the class of attacks directed against Structure Exception Handlers (SEH). The Windows OS makes use of a SEH routine that leaves the platform uniquely vulnerable to an attack pattern, which aims at replacing the structured exception handler with an address of our choosing, before causing an exception. Vista makes use of a new protection mechanism called SEHOP [33] to protect against such attacks. OS X like most Unix derivatives make use of signals as opposed to a default exception handler making Leopard not vulnerable to this class of attacks by default.

#### 4 COMPARISONS

The findings so far are documented in *Table 1*, below.

*Table 1 – Comparisons between Vista and Leopard*

Attack Pattern	Windows Vista	OS X Leopard
Non-Executable Stack	YES	YES
Non-Executable Heap	YES	NO
Safe Heap Unlinking	YES	NO
A.S.L.R	FULL	Partial
Compiled with Stack Protection	Partial	Partial
S.E.H exploit protection	SEHOP	Not Applicable

It is fairly clear from *Table 1* that Apple lags significantly behind its Windows counterpart when it comes to generic anti-exploitation defences. What is unclear is why the lack of said defences has not led to some of the large scale attacks (like *Slammer*, or *Code-Red*), that have been witnessed against Windows machines in the past [34, 35].

A market share that is too small to attract real malevolence is an argument that is often made, but this does not stand up to the counterpoint of the literally hundreds of vulnerabilities reported weekly in obscure, relatively unused code-bases [36]. The argument that Apple simply makes less exploitable mistakes in their code is also untenable as researchers have had no difficulty exploiting OS X in public contests, when the need arose [37].

It is our belief that one of the explanations is that the client operating system OS X is being compared to the server operating systems in the Windows family. Both systems have different natural adversaries and so have different risk profiles. It can be postulated that OS X currently sits in an unusual niche, staying off the radar of server-attackers while below the threshold to make it an attractive target for attackers wishing to capture large volumes of desktop computers (for botnets or similar activities).

## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

Apple would be well advised to make good use of their time in this niche to learn from the mistakes made by those before them, because as their market share steadily rises, they steadily inch closer to moving out of this protected space. They currently have a narrow window in which they can refine their defences. This would include a more robust ASLR implementation and can enforce the mandatory use of compile time stack protection to raise the bar on the requirements for a successful attack against the system.

### **5 CONCLUSION**

We have demonstrated the basics of memory corruption exploits, and have examined how Microsoft Windows Vista and Apple's MacOS X Leopard combat these attacks in their default state. In this analysis OS X has been weighed and measured, and has come up wanting.

The next release of OS X, named Snow Leopard is currently in Beta and promises to improve the security posture of the system. It remains to be seen if the controls mentioned in this paper have been implemented or improved upon at all.

We hope that Apple is able to make the necessary improvements before it too is forced into altering its views on generic OS protection mechanisms through the media frenzy that follows public security breaches.

## 6 REFERENCES

- [1] Rafal Lukawiecki. “Windows Vista Security”.  
<http://download.microsoft.com/download/7/0/5/7058e678-6151-448e-a53b-43b83b5d309e/Windows%20Vista%20Security.ppt> (2006)
- [2] Jordan Hubbard. “OS X, From the Server Room to Your Pocket”. In proceedings of the 22<sup>nd</sup> Large Installation System Administration Conference. (12 November 2008)
- [3] E. H. Spafford. “Crisis and aftermath”. In Communications of the ACM archive, Volume 32 , Issue 6 (June 1989) (Pages: 678 – 687)
- [4] Aleph One. “Smashing the stack for fun and Profit”. Phrack Magazine 7, 49 (Fall 1997); <http://www.phrack.com/issues.html?issue=49&id=14>.
- [5] “x86: Solaris Supports the no execute Bit”. Solaris10 Release Notes.  
[http://docs.sun.com/app/docs/doc/817-0552/6mgb4fgg?l=en&a=view&q=PROT\\_EXEC](http://docs.sun.com/app/docs/doc/817-0552/6mgb4fgg?l=en&a=view&q=PROT_EXEC) (2006)
- [6] Theo de Raadt. “Exploit Mitigation Techniques (in OpenBSD).”  
<http://www.openbsd.org/papers/auug04/index.html> (2004).
- [7] “Data Execution Prevention”, Microsoft Technet,  
<http://technet.microsoft.com/en-us/library/cc738483.aspx> (2009)
- [8] Arjan van de Ven. “New Security Enhancements in Red Hat Enterprise Linux v.3, update 3”. (August 2004).
- [9] “PaX”. <http://pax.grsecurity.net/>
- [10] Solar Designer. “Bugtraq: Linux SuperProbe exploit”.  
<http://seclists.org/bugtraq/1997/Mar/0011.html> (05 Mar 1997).
- [11] “Microsoft IIS HTR Chunked Encoding heap overflow allows arbitrary code “.Symantec security response center. (12 Jun 2002).  
[http://www.symantec.com/security\\_response/vulnerability.jsp?bid=2033](http://www.symantec.com/security_response/vulnerability.jsp?bid=2033).
- [12] Rafal Wojtczuk. “Defeating Solar Designer's Non-executable Stack Patch”. (30 January 1998). <http://insecure.org/spl0its/non-executable.stack.problems.html>.
- [13] John McDonald. “Bugtraq: Defeating Solaris/SPARC Non-Executable Stack Protection”. (03 Mar 1999).  
<http://seclists.org/bugtraq/1999/Mar/0004.html>.
- [14] Solar Designer. “Non-Executable User Stack”.  
<http://www.false.com/security/linux-stack/>.
- [15] [http://en.wikipedia.org/wiki/NX\\_bit](http://en.wikipedia.org/wiki/NX_bit)
- [16] <http://en.wikipedia.org/wiki/Shellcode>



## An Examination of the Generic Memory Corruption Exploit Prevention Mechanisms on Apple's Leopard Operating System

- [17] Solar Designer. "lpr LIBC RETURN exploit". (10 Aug 1997)  
<http://insecure.org/sploits/linux.libc.return.lpr.sploit.html>.
- [18] "About the security content of iPhone v1.1.2 and iPod touch v1.1.2 Updates". <http://support.apple.com/kb/HT2170>. (2007).
- [19] Niacin, "iTouch/iPhone exploit source code released",  
<http://toc2rta.com/?q=node/30>. (21 Oct 2007)
- [20] Berend-Jan Wever (SkyLined). "Internet Exploiter 3: Technical details". (01 Dec 2004).  
[http://skypher.com/wiki/index.php?title=Www.edup.tudelft.nl/~bjwever/details\\_msie\\_ani.html.php](http://skypher.com/wiki/index.php?title=Www.edup.tudelft.nl/~bjwever/details_msie_ani.html.php).
- [21] Security Updates available for Adobe Reader and Acrobat versions 9 and earlier. (19 Feb 2009).  
<http://www.adobe.com/support/security/advisories/apsa09-01.html>
- [22] Bernhard Mueller (SEC Consult Vulnerability Lab). "Microsoft SQL Server sp\_replwritetovarbin limited memory overwrite vulnerability". (09 Dec 2008). [https://www.sec-consult.com/files/20081209\\_mssql-sp\\_replwritetovarbin\\_memwrite.txt](https://www.sec-consult.com/files/20081209_mssql-sp_replwritetovarbin_memwrite.txt).
- [23] Sotirov, A. "Heap Feng Shui in JavaScript". Blackhat Europe 2007.  
<http://www.phreedom.org/research/heap-feng-shui/>
- [24] "A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2". (26 Sep 2006).  
<http://support.microsoft.com/kb/875352>.
- [25] Johnson, R. "Windows Vista Exploitation Countermeasure". (29 Sep 2006). <http://www.authorstream.com/presentation/Mentor-6833-rjohnson-Windows-Vista-Exploitation-Countermeasure-windows-vista-exploitation-countermeasures-ppt-powerpoint>.
- [26] "PaX". <http://pax.grsecurity.net/>
- [27] "WehnTrust, Host Intrusion Prevention System for Win2000, XP and Win2003". <http://www.codeplex.com/wehntrust>
- [28] Ollie Whitehouse, "An Analysis of Address Space Layout Randomization on Windows Vista". (2007).  
<http://www.blackhat.com/presentations/bh-dc-07/Whitehouse/Presentation/bh-dc-07-Whitehouse.pdf>.
- [29] Charlie Miller, Dino Dai Zovi, "The Mac Hackers Handbook", (2009). Wiley Publishing.
- [30] C. Cowan, C. Pu, D. Maier, H. Hinton, P. Bakke, S. Beat-tie, A. Grier, P. Wagle, Q. Zhang, "StackGuard: Automatic Adaptive Detection and

Proceedings of ISSA 2009

- Prevention of Buffer-Overflow Attacks". (1998). Proceedings of the 7th USENIX Security Conference.
- [31] Brandon Bray, Visual Studio Team. "Compiler Security Checks In Depth". (Feb 2002). <http://msdn.microsoft.com/en-us/library/aa290051.aspx>.
- [32] Maynor D. "Looking Glass". (10 Apr 2004). <http://www.erratasec.com/lookingglass.html>.
- [33] "Windows Vista Service Pack 1 and Windows Server 2008 now include support for Structured Exception Handling Overwrite Protection (SEHOP)". (28 Jan 2009). <http://support.microsoft.com/kb/956607/en-us>.
- [34] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. "Inside the Slammer Worm". IEEE Security & Privacy Magazine. (2003)
- [35] David Moore, Colleen Shannon, Jeffery Brown. "Code-Red: a case study on the spread and victims of an Internet worm". Presented at the Internet Measurement Workshop (IMW). (2002)
- [36] United States Computer Emergency Readiness Team (US-CERT). "Cyber Security Vulnerability Summaries per Week". <http://www.us-cert.gov/cas/bulletins/>.
- [37] Matt Hines. "Mac Hacked Via Safari Browser in Pwn-2-Own Contest". [http://securitywatch.eweek.com/apple/mac\\_hacked\\_via\\_safari\\_browser\\_in\\_pwn2own\\_contest.html](http://securitywatch.eweek.com/apple/mac_hacked_via_safari_browser_in_pwn2own_contest.html). (20 Apr 2007)

A Framework for Web Services Security Policy Negotiation

## **A FRAMEWORK FOR WEB SERVICES SECURITY POLICY NEGOTIATION**

**Tristan Lavarack<sup>1</sup> and Marijke Coetzee<sup>2</sup>**

Academy for Information Technology  
University of Johannesburg  
South Africa

<sup>1</sup>200506397@student.uj.ac.za

<sup>2</sup>marijkec@uj.ac.za

### **ABSTRACT**

In today's business environment, the use of web services technology is becoming more popular. This growth has been met with an increase of security related attacks, which has caused web services providers to adopt stricter security policies. As not all web service consumers can implement the security requirements of web services providers, they may turn to use the services of other providers. In order to address this problem, this paper introduces a framework for a web services security policy negotiation system that web services consumers and providers can use to negotiate a customised security contract. The framework is defined over current web services technology, to be used by business-to-business (B2B) web services collaborations. The inflexibility of current security policy specification languages for negotiation is overcome, by incorporating human intuitiveness supported by an intelligent negotiation support system.

### **KEY WORDS**

Web Service, NSS, Negotiation, Security, Security Policy

## **A FRAMEWORK FOR WEB SERVICES SECURITY**

### **POLICY NEGOTIATION**

#### **1 INTRODUCTION**

A web service is an autonomous, well-defined, standards-based component that is accessed via web-based protocols. Such services enable the dynamic assembly of B2B (business-to-business) functionality, across loosely coupled heterogeneous platforms. The increased usage of web services technology has led to a growing number of malicious attacks in this environment [1]. This aspect, coupled with the importance of web services as an integration technology, has led to concerns over their security [2].

To protect themselves from attack, web services providers define security policies that describe their capabilities and requirements such as identification and data integrity. Web services providers may expect of all web services consumers to adhere to these security policies to be able to use the web service's functionality. If web services consumers cannot apply all stipulated security policy requirements, they will have to search for alternative web services providers. In such a case, a web services provider loses these consumers, and may rather decide to negotiate some aspects of its security policy requirements so that interaction can take place. This paper highlights important requirements for a security policy negotiation system, designed to fit into the current web services architecture [3].

The remainder of this paper is organized as follows. The next section provides a background on web services and web services security. Section 3 discusses related work on negotiation. Section 4 examines a list of requirements for a web services negotiation system. Section 5 provides a framework for the web services negotiation system. The paper ends with a conclusion and a brief look at future work.

## 2 BACKGROUND

The web services architecture [4] identifies web services providers and web services consumers as two endpoints of communication. A web services provider can be seen as the machine that holds the web services implementation, which the web services consumer utilises. Web services support interoperable machine-to-machine interaction over a network [4]. They have an interface described in WSDL [5] and consumers interact with the web service via SOAP messages. WSDL represents a valuable tool for the description of functionality but not for security capabilities and requirements. Therefore, secure interoperability requires additional mechanisms. Security capabilities and requirements of a web services provider are stored in policy documents. Such documents are attached to specific services and are made available to web service consumers, to allow them to consume the web service successfully. There are many different policy languages that can be used to define security policies such as WS-Policy [6], WS-Security Specification [7], WSPL [8] and WS-Agreement [9]. For semantic web services, KAoS [10], [11] can be used.

Web services that are used in business-to-business (B2B) transactions have high requirements for security. Consequently, it is more complex for large numbers of web service consumers, each having his/her own set of security requirements, to apply to the full set of security requirements of a web services provider. The problem can be described as follows: a web service provider's security policy requires that consumers perform authentication with certificates, encryption with AES, data integrity with MD5, and roles for access control. If a web service consumer uses username-password combinations for authentication, and does not support AES or roles, the web service consumer will either have to change its security mechanisms, or search for an alternative web services provider. To solve this, web services security policy negotiation can be used to negotiate over these security requirements, by taking into account the needs and limitations of each party. The result of the policy negotiation is a security contract where encryption with DES, data integrity with MD5, and roles for access control are agreed to, but a compromise is made to use username-password combinations for authentication, as the consumer has a good reputation.

The security contract is thus an agreed upon set of security clauses between the web services provider and web services consumer, whereas a security policy is a set of security requirements of a single party. Such a security contract can be used to monitor the interactions between the web service and the web service consumer, to enable service governance. Even though it may be more costly, the ability to customise web services security contracts gives web services providers more flexibility to be able to attract potential consumers.

In the next section, recent research on web services security policy negotiation is discussed.

### **3 RELATED WORK**

There is a large body of research on negotiation [12], [13], [14], [15], [16]. Negotiation can be defined as a decentralised decision-making process by at least two parties. It is performed until an agreement is reached, or the process is terminated without reaching an agreement [17], [18]. For web services, related research in this field has addressed the negotiation of Service-Level Agreements (SLA) in the Grid environment [19], WS-Negotiation [18] focusing on negotiation of business parameters, and negotiation of privacy policies [20].

The negotiation of policies such as security and privacy has been identified as an important research focus for web services [21]. Security policy negotiation refers to the adjustment in security requirements and capabilities, to accommodate needs of both consumers and providers and their environmental conditions. To date, no industry solution has been defined for this difficult problem, with little research addressing negotiation using current web services standards such as WS-Policy [6]. A prototype developed by Korba and Yee [1] is representative of the most recent research on this topic, and is discussed next.

The prototype implements a semi-automated security policy negotiation system, based on a peer-to-peer architecture. It enables an Internet service, which does not necessarily have to be a web service, and its clients, who may be human, to contact each other and hold a negotiation session across the Internet. Both the Internet service and the client have their security requirements in a security policy document. The

## A Framework for Web Services Security Policy Negotiation

negotiation system evaluates both the Internet service's and the client's security policies. Where the security requirements are the same, a match is made and no changes are necessary. Where the security requirements do not match, negotiation has to be performed. As part of the semi-automated approach, the administrator of the Internet service and the owner of the client are given the opportunity to edit their security policies to create a new security policy in order to accommodate each other. Policies are exchanged, re-evaluated, and the process continues until an agreement is reached or until either the Internet service or client terminates the negotiation process. As it is difficult to evaluate security policies, either party can ask the system for help. The help module provides a human located at each party, with a history of past choices that have been made by many others in similar situations. This is done to help them understand which security requirements were preferred before, and how many times each has been used. The help system thus provides "best practice" to its users.

Limitations of the prototype are that it is not specifically designed for B2B web services interactions; the help module does not provide any information on how decisions affect each other, policy decisions are inflexible as a match is made or not, and the prototype does not consider the role that the state of the environment, and type of relationship between parties, play in the negotiation process.

Next, the requirements for a web service security policy negotiation system, with the aim of extending this prototype are discussed.

### **4 WEB SERVICES SECURITY POLICY NEGOTIATION REQUIREMENTS**

The ability to negotiate security contracts is an important feature to be addressed for secure and flexible B2B web services interactions. Requirements for such a system need to consider the type of negotiation strategy, as a fully automated process may not be practical since security is a high risk. There is a need for an intelligent support system for administrators to assist them with decision-making. To be able to define such a system, the following seven requirements have been identified by this research:

Proceedings of ISSA 2009

1. Standards-based implementation
2. Standards-based security policy specification language
3. Standards-based negotiation protocol
4. Semi-automated negotiation strategy
5. Negotiation support system
6. Collaborative decision-making
7. Consideration of environmental influences

These requirements are next discussed in greater detail.

#### **4.1 Standards-based implementation**

B2B web services interactions, in which business relationships change regularly require a highly flexible security framework based on approval and universal acceptance of standards. This allows business partners to avoid interoperability problems among their disparate information systems. The adoption of web services standards is thus important. As no current standard directly addresses policy negotiation, a solution needs to be found to cater for this need without affecting interoperability. The requirement for a standards-based implementation influences choices to be made with respect to the policy specification language, negotiation protocol, negotiation strategy and decision-making, discussed next.

#### **4.2 Standards-based security policy specification language**

The choice of the policy specification language has a far-reaching effect on the web services policy negotiation system, and needs to be carefully considered. A major consideration is that security policies should be based on standard technologies, so that runtime platforms can read, interpret and enforce the security policy.

As mentioned, there are a number of languages that can be used such as WS-Policy, WS-SecurityPolicy, XACML, WSPL and WS-Agreement, where WSPL and WS-Agreement provide some support for negotiation. XACML is used to specify access control policies and can be used to support the negotiation of privacy policies [20]. For the specification of general security policies, XACML has a limitation in that its rules cannot be used to define application-dependent concepts such as types of



## A Framework for Web Services Security Policy Negotiation

encryption algorithms. As its policy combinators are implemented subjectively by programmers, the concepts of policy and mechanism become intertwined, which could lead to ambiguities. WSPL is a subset of XACML and can thus support negotiation of mutually acceptable policies by their intersection using combining algorithms. Unfortunately, WSPL has not become a standard.

As the focus of this research is on standard technologies supported by current runtime platforms, this research does not consider more sophisticated languages for negotiation such as WSPL, WS-Agreement, or semantic web policy languages. For B2B web services interactions, it is important to consider WS-Policy and its related specifications, as it is a W3C recommendation since September 2007. Advantages of the WS-Policy framework are that it is flexible and extensible. Policies can be defined inside a WSDL file or defined generically and referenced by any number of WSDL files by making use of reusability mechanisms such as inclusion and grouping of policies. From the perspective of more sophisticated languages, WS-Policy lacks formalisation. Thus, the merging of service consumer and provider policies as means of negotiating an agreed upon security contract is dependent on domain specifications. Such specifications have been defined successfully, but the definition of policy merging and intersection mechanisms needs to be clarified better. WS-Policy is natively supported by common development and runtime platforms.

The negotiation protocol, discussed next, is used to exchange and negotiate a security policy. It should similarly be based on standard technologies to ensure platform interoperability.

### **4.3 Standards-based negotiation protocol**

A negotiation protocol is a series of descriptions on how the negotiation is conducted. It is formatted as a set of rules about the interaction manners among the negotiating parties [22]. Generally, automated negotiations can be separated into three main phases [23], namely pre-negotiation, negotiation and post-negotiation.

The pre-negotiation stage begins by starting a new negotiation between two partners. Here, the security policies of partners are

exchanged automatically by the system. The next phase supports the negotiation of the security policy. The two negotiation parties exchange offers and counter-offers for all the security requirements that are being negotiated. Finally, the negotiation process is completed by the creation of the security contract, using the newly negotiated security requirements.

A web services security policy negotiation protocol needs to address rules governing messages, vocabulary, and synchronisation of communication, so that they can be understood by communicating parties. WS-MetaDataExchange [24], [25] defines request-response interactions to exchange policies and other metadata. It has potential to support policy negotiation exchanges using the WS-Policy framework. It is a vendor-independent mechanism for locating and retrieving metadata of a service. For this research, the security policy negotiation system ensures platform interoperability by exchanging standardised security policy documents with a partner until an agreement is reached or the negotiation is aborted. Minimal extensions to this protocol may be required to indicate the status of a security policy document in the negotiation process.

Next, the negotiation strategy is discussed.

#### **4.4 Semi-automated negotiation strategy**

The traditional form of web services security policy negotiation is performed out-of-band via face-to-face meetings or with e-mail [26]. The disadvantages are that the process is static and time consuming. In a fully automated negotiation process, agents set up, carry-out and finalise the negotiation without any human involvement [20]. As all interactions are machine-based, semantic web technology plays an important role. This approach saves time, and makes the negotiation process very dynamic. For security policy negotiation, this can be risky, as agents are not intuitive and cannot take rational decisions as humans do. The semi-automated approach has the benefits of both the previous strategies in that it is dynamic, uses humans to control some of the decision making, saves time and can be implemented using current web services standards. In a semi-automated negotiation process, agents handle all communications and some decision making. Where conflicts arise, it is resolved by humans who are supported by an intelligent negotiation support system.

## A Framework for Web Services Security Policy Negotiation

For web services security policy negotiation, a semi-automated approach would best match the risk involved and the constraints of the standards-based implementation. Practically, a negotiation process needs to be encapsulated in a negotiation system that incorporates human involvement, which is discussed next.

### **4.5 Negotiation support system**

Negotiation Support Systems (NSS) [27] [28] [29] [30] involving humans emerged in the 1980s [31], but were rarely used in practise. NSS normally assist negotiators to weigh up situations, generate and evaluate options, and implement decisions. [32]. There are two main types of NSS. Process-oriented NSS focus on improving the negotiation process, while outcome-oriented NSS help to improve the outcome of the negotiation. For this research, the outcome-oriented NSS is considered, as it supports a negotiation protocol and negotiation help system.

An outcome-oriented NSS utilises the semi-automated negotiation strategy for communication, supported by a negotiation protocol. For the help function, the NSS provides support by structuring and analysing the problem, eliciting preferences and using them to construct a utility function, determining feasible and efficient alternatives, visualising different aspects of the problem and the process [33].

A web services security policy negotiation system needs to include a NSS, possibly consisting of multiple interacting subsystems [34] such as a management subsystem for the negotiation process, a decision support subsystem to advise negotiators, a trust manager to analyse relationships between the negotiators and their respective environments, a conflict resolution subsystem and a contract definition subsystem.

For any negotiation system to be successful it needs to be guided by a formal approach to decision-making, discussed next.

### **4.6 Collaborative decision-making**

Two main types of negotiations are distributive negotiations and integrative negotiations [18], [35]. Distributive negotiations are also known as zero-sum or competitive negotiations where negotiators try to

win the negotiation. For B2B web services security policy negotiation, the security contract is thus defined by the security requirements of the negotiator that won.

Integrative negotiations are also known as collaborative negotiations. Collaborative negotiations create a contract between parties in a win-win fashion by finding options that will satisfy both parties [36]. For web services, such negotiations are more likely to succeed, because both parties compromise on certain security policy requirements in order to create a mutually agreeable security contract. The manner in which the negotiation deviates from desired security requirements is dictated by the semi-automated negotiation strategy, characterised by human participation and an intelligent NSS. The inflexible manner in which current web services policy specification languages support policy negotiation is offset by this approach.

Generally, negotiation in e-commerce scenarios focuses on functional parameters of a service such as price, where decision-making usually refers to the process of selecting a particular action in a given situation. Decision models mainly focus on game theoretic models or AI-based models [37]. Such decision-making models do not always incorporate the relationship and influence between different negotiation issues. For example, the choice of an authentication mechanism may be influenced by the level of trust in a partner, as well as the encryption that is supported. Lowering the quality of an authentication mechanism may negatively influence the assurance of non-repudiation. To be able to make decisions that take into account all negotiations issues and their influences, an intelligent NSS, supported by fuzzy techniques needs to be defined.

For web services security policy negotiation, collaborative decision-making, supported by an intelligent NSS is thus required, in order to negotiate a security contract.

#### **4.7 Consideration of environmental influences**

The environment in which negotiation is performed has a significant influence on it. Previous research on security policy negotiation has not addressed this issue. There are a number of environmental factors to

## A Framework for Web Services Security Policy Negotiation

consider such as the trust relationship between services, and the dynamically changing context in which negotiation performed.

The level of trust in another service is essential for making rational decisions over the choice of security requirements in an open environment where interacting services often have no previous relationship. Trust relationships evolve by gathering a variety of properties and attributes of consumers, services and other parties, ranging from strong cryptographically verifiable evidence to soft evidence such as a reputation measures and unsigned declarations. An intelligent NSS needs to be supported by a trust manager to assist it with its decision-making processes. Compromises in security policy requirements may be more flexible for highly trusted partners than for strangers.

Consumers and providers should be aware of constraints stemming from a dynamically changing context, which could impact both consumer and provider security policy requirements. For example, if the service platform is under threat, as determined by firewalls and anti-virus programs, it needs a greater the level of protection for the duration of the threat. This will in turn affect decisions that are made during the negotiation. To ensure secure B2B web services interactions, a rapid reconfiguration of security requirements via a context-aware security policy negotiation is needed.

In the next section, requirements discussed here are used to create a framework for the B2B web services security policy negotiation system.

## **5 FRAMEWORK FOR WEB SERVICES SECURITY POLICY NEGOTIATION**

In order to negotiate web services security policies, a Policy Negotiation Support Point (PNSP), shown in figure 1, is introduced. The PNSP automatically manages the negotiation, but if a conflict arises, a negotiator makes a decision. The PNSP is knowledgeable about the security requirements of services that can be accessed in its environment, and the standards used by the service and its consumers. Mechanisms exist at providers and consumers to support the publication and exchange of policies. Protocols ensure that messages are sent correctly, so that they are understood by communicating parties. Policies are managed by a policy

manager to guarantee their validity and conformance to standards. The PNSP sources information from a trust manager and platform monitors. The trust manager provides the PNSP with information such as the trust level of the other party and its reputation. Platform monitors are applications such as firewalls, Intrusion Detection Systems (IDS) and anti-virus applications that observe the current environment.

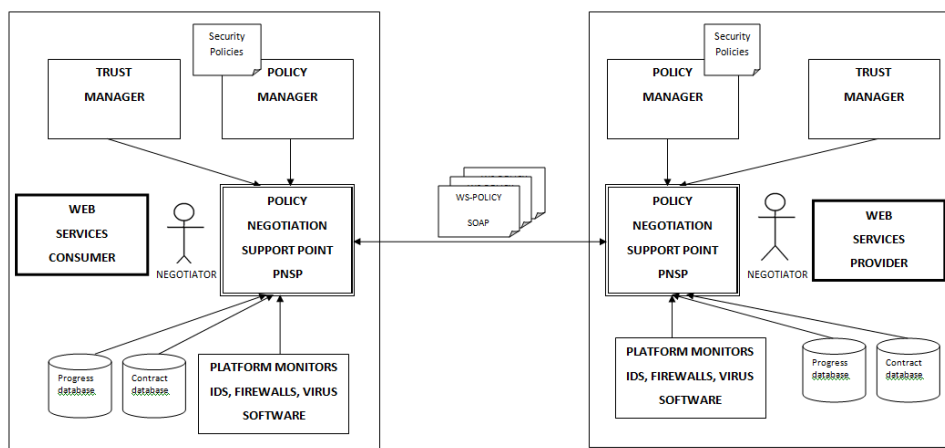


Figure 1: Web services security policy negotiation system

A contract database stores security contacts defined during the negotiation process. It contains all previous negotiated contracts, which can be used by the PNSP to make decisions and construct assistance for negotiators. The progress database stores all information about the current negotiation. This allows asynchronous distributed negotiations [13] to take place. As negotiations may take place across different time zones and countries negotiators can negotiate when it suits them.

Both consumers and providers are supported by PNSPs, as shown here. It is also possible that such a component only exists at one party. The first phase of negotiation is started by a consumer and is automatically executed. The consumer sends a request to the provider for the security policy document, defined by the WS-Policy framework. WS-MetaDataExchange request-response interactions are used for this

## A Framework for Web Services Security Policy Negotiation

purpose. The provider's PNSP intercepts the request and returns either the security policy, or a URI (Universal Resource Identifiers) that identifies its location. The consumer evaluates the security policy against its own, to determine whether it would be able to proceed. If there is a direct match of security preferences, a security contract can be agreed to and the service can be accessed without human intervention. If there is not a match, the next phase of the negotiation starts.

In this phase, the PNSP of the consumer attempts to formulate a new offer. It sources information from the trust manager and environmental monitors to determine the level to which a compromise can be made. Different policy choices are generated by the PNSP if possible, and are presented to a negotiator with explanations on how they were determined. The negotiator chooses an option and the PNSP constructs a new offer to be sent to the provider.

The provider receives the offer and if a match can be made, a security contract is created. Otherwise, the negotiation process continues back and forth until both sides agree and the negotiation is successful or one side terminates the negotiation. If the negotiation is unsuccessful, the consumer can search for another service.

## 6 CONCLUSION

Having the ability to negotiate security contracts, web services providers will have the capability to attract more consumers while keeping the security of the web service at an acceptable level. This paper has presented a novel framework for a system that allows the consumers of web services to negotiate a new security contract with the provider of a web service by incorporating environmental considerations into its decision-making.

A list of requirements for a web services security policy negotiation system was defined and analysed. To be able to use the system with current web services technologies, a standards based implementation was preferred, which affected the choice of policy language and communication protocol. The semi-automated approach to negotiation was selected to offset the inflexibility of current policy languages.

Future work aims to investigate the chosen decision model by identifying negotiation objects found in policy documents, and the



environment. Their influence on each other needs to be determined to be evaluated by making use of fuzzy techniques.

## 7 REFERENCES

1. Korba L and Yee G (2008), Security Personalization for Internet and Web Services, International Journal of Web Services Research, IGI Publishing, Volume 5, Issue 1, January-March, pp 1-23.
2. Aref W, Ghafoor A, Joshi J and Spafford E (2001), Security models for Web-based applications, Communications of the ACM, ACM New York, New York, USA, Volume 44, Number 2, pp 38-44.
3. Haas H and Orchard D (2002), Web Services Architecture Usage Scenarios, World Wide Web Consortium (W3C) Working Draft, 30 July 2002, <http://www.w3.org/TR/2002/WD-ws-arch-scenarios-20020730> Accessed: 9 June 2009.
4. Booth D, Champion M, Ferris C, Haas H, McCabe F, Newcomer E and Orchard D (2004), Web Services Architecture, World Wide Web Consortium (W3C) Working Group Note 11 February 2004, <http://www.w3.org/TR/ws-arch> Accessed: 9 June 2009.
5. Duran M and Hasan J (2006), Expert Service-Oriented Architecture in C# 2005, Second Edition, Apress, USA, p 15.
6. Boubez T, Hirsch F, Hondo M, Orchard D, Vedamuthu A, Yalcinalp U, and Yendluri P (2007), Web Services Policy 1.5 - Framework, <http://www.w3.org/TR/ws-policy> Accessed: 8 June 2009.
7. Hallam-Baker P, Kaler C, Monzillo R and Nadalin A (2004), Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard 200401, March 2004, <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf> Accessed: 9 June 2009.
8. Anderson A (2004), An Introduction to the Web Services Policy Language (WSPL), IEEE 5th International Workshop on Policies for Distributed Systems and Networks, New York, USA, 7-9 June, <http://research.sun.com/projects/xacml/Policy2004.pdf> Accessed: 8 June 2009.



A Framework for Web Services Security Policy Negotiation

9. Andrieux A, Czajkowski K, Dan A, Keahey K, Ludwig H, Nakata T, Pruyne J, Rofrano J, Tuecke S, Xu M (2007), Web Services Agreement Specification(WS-Agreement), Grid Resource Allocation Agreement Protocol (GRAAP) Working Group, <http://forge.gridforum.org/sf/go/doc14574?nav=1> Accessed: 8 June 2009.
10. Aitken S, Bradshaw J, Dalton J, Jeffers R, Johnson M, Tate A and Uszok A (2004), KAoS Policy Management for Semantic Web Services, IEEE Intelligent Systems, Volume 19, Number 4, July/August 2004, pp 32-41, <http://www.aiai.ed.ac.uk/project/ix/documents/2004/2004-ieee-is-uszok-kaos.pdf> Accessed: 9 June 2009.
11. Bradshaw J, Jeffers R, Olson L, Tonti G and Uszok A (2004), Integration of KAoS Policy Services with Semantic Web Services, 3rd International Semantic Web Conference, Hiroshima, Japan, 7-11 November, <http://iswc2004.semanticweb.org/demos/08/paper.pdf> Accessed: 9 June 2009.
12. Debenham J and Elaine L (2008), Automating Contract Negotiation, Fifth International Conference on Information Technology: New Generations, Nevada, USA, 7-8 April, pp 143-148.
13. Kersten G and Noronha S (1997), Supporting International Negotiation with a WWW-Based System, International Institute for Applied Systems Analysis (IIASA), IIASA Interim Report IR-97-049, <http://www.iiasa.ac.at/Admin/PUB/Documents/IR-97-049.pdf> Accessed: 9 June 2009.
14. Bosse T and Jonker C (2005), Human vs. Computer Behaviour in Multi-Issue Negotiation, Rational, Robust, and Secure Negotiation Mechanisms in Multi-Agent Systems, 25 July 2005, pp 11-24.
15. Cheng W, Lian-chen L, Lung N, Phil M and Wan-cheng N (2007), A Semi-automated Negotiation Process to improve the Usability for Online Marketplaces, 7th IEEE International Conference on Computer and Information Technology, Fukushima, Japan, 16-19 October, pp 253-258.
16. Jang I, Shi W and Yoo H (2008), Policy Negotiation System Architecture for Privacy Protection, 4th International Conference on Networked Computing and Advanced Information Management - Volume 02, Gyeongju, Korea, 2-4 September, pp 592-597.

Proceedings of ISSA 2009

17. Thompson L (1998), *The Mind and Heart of the Negotiator*, 1st Edition, Prentice-Hall Inc.
18. Hung P, Jeng J and Li H (2004), *WS-Negotiation: An Overview of Research Issues*, 37th Hawaii International Conference on System Sciences - Track 1 - Volume 1, Hilton Waikoloa Village, Hawaii, 5-8 January, [http://www.uu.edu/personal/hli/index\\_files/publications/WS-Negotiation.pdf](http://www.uu.edu/personal/hli/index_files/publications/WS-Negotiation.pdf) Accessed: 9 June 2009.
19. Brandic I, Buyya R, Mattess M and Venugopal S (2008), *Towards a Meta-Negotiation Architecture for SLA-Aware Grid Services*, International Workshop on Service-Oriented Engineering and Optimization, Bangalore, India, 17 December, <http://www.hpl.hp.com/india/senopt08/papers/senopt08106.pdf> Accessed: 9 June 2009.
20. Cheng V, Chiu D and Hung P (2007), *Enabling Web Service Policy Negotiation with Privacy preserved using XACML*, 40th Annual Hawaii International Conference on System Sciences, Hilton Waikoloa Village, Hawaii, 3-6 January, p 33.
21. Langendörfer P, Maaser M, Ortman S (2006), *NEPP: Negotiation Enhancements for Privacy Policies*, W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra, Italy, 17-18 October.
22. Benyoucef M, Kersten G and Wu S (2006), *INSS – A New Approach in Designing Web-based Negotiation Support Systems*, Proceedings of the Montreal Conference on e-Technologies, Montreal (Quebec), Canada, May 16-18, <http://interneg.concordia.ca/interneg/research/papers/2006/09.pdf> Accessed: 9 June 2009.
23. Kersten G and Noronha S (1999), *WWW-based Negotiation Support: Design, Implementation, and Use*, Decision Support Systems, Elsevier, Volume 25, Number 2, pp 135-154.
24. Samaranyake S (2007), *Understanding WS Metadata Exchange - Part I*, <http://wso2.org/node/2794/print> Accessed: 1 May 2009.
25. Ballinger K, Box D, Curbera F, Davanum S, Ferguson D, Graham S, Liu K, (2006), *Web Services Metadata Exchange (WS-*

A Framework for Web Services Security Policy Negotiation

MetadataExchange) Version 1.1, August 2006,  
<http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf>  
Accessed: 9 June 2009.

26. Lock R (2006), Automated negotiation for service contracts, 30th Annual international Computer Software and Applications Conference, Chicago, USA, 17-21 September, p 2.

27. Li Y and Shang W (2005), Information Exchange and Conflict Analysis in E-Business Negotiation Support System, 2nd IEEE International Conference on Services Systems and Services Management - Volume 1, Chongqing University, China, 13-15 June, pp 774-779.

28. Archer M, Rose J and Yuan Y (1998), A Web-Based Negotiation Support System, Electronic Markets, Volume 8, Number 3, Routledge, pp 13-17.

29. Dong S, Feng Y and Wang L (2007), The crucial problem of the NSS in the Ecommerce, 2007 International Conference on Intelligent Pervasive Computing, Ramada Plaza Jeju, Jeju Island, Korea, 11-13 October, pp 441-445.

30. Eustice K, Ramakrishna V and Reiher P (2007), Negotiating Agreements Using Policies in Ubiquitous Computing Scenarios, IEEE International Conference on Service-Oriented Computing and Applications, Vienna, Austria, 17-20 September, pp 180-190.

31. Jarke M, Jelassi M and Shakun M (1985), Mediator: Towards a Negotiation Support System, New York University - Department of Information, Operations, and Management Sciences, NYU Working Paper No. IS-85-36, May 1985.

32. Bui TX and Shakun MF (2004), Negotiation Support Systems minitrack, 37th Hawaii International Conference on System Sciences - Volume 1, Hilton Waikoloa Village, Hawaii, 5-8 January, <http://csdl2.computer.org/comp/proceedings/hicss/2003/1874/01/187410026.pdf> Accessed: 9 June 2009.

33. Kersten G and Lo G (2001), Negotiation support systems and software agents in e-business negotiations, First International Conference on Electronic Business, Hong Kong, China, 19-21 December.

Proceedings of ISSA 2009

34. Power D (2007), What is a negotiation support system?, Available: <http://dssresources.com/faq/index.php?action=artikel&id=137> Accessed: 15 April 2009.
35. Negotiation Types, <http://www.negotiations.com/articles/negotiation-types> Accessed: 24 April 2009.
36. Nierenburg G (1968), Gerard Nierenberg: The Art of Negotiating, Barns & Noble Books.
37. Faratin P, Jennings N, Lomuscio A, Parsons S, Sierra C and Wooldridge M (2001), Automated negotiation: prospects, methods and challenges, Group Decision and Negotiation, Springer, Volume 10, Number 2, pp 199-215, <http://www.csc.liv.ac.uk/~mjw/pubs/gdn2001.pdf> Accessed: 9 June 2009.

How Appropriate is  $K$ -Anonymity for Addressing the Conflict between  
Privacy and Information Utility in Microdata Anonymisation

**HOW APPROPRIATE IS  $K$ -ANONYMITY FOR  
ADDRESSING THE CONFLICT BETWEEN PRIVACY  
AND INFORMATION UTILITY IN MICRODATA  
ANONYMISATION**

**Marek P. Zielinski <sup>1</sup>, Martin S. Olivier <sup>2</sup>**

University of Pretoria, South Africa

1: marek.zielinski@sap.com

2: molivier@cs.up.ac.za

**ABSTRACT**

Before statistical data, such as microdata, can be released to the public, it needs to be anonymised. Anonymisation protects the privacy of the individuals whose data is released. However, as microdata is anonymised, its level of privacy increases, while its level of information utility decreases.

$K$ -anonymity is often used to address the conflict between privacy and information utility in microdata anonymisation. In this paper, we determine the extent to which  $k$ -anonymity is appropriate for addressing this conflict. We argue that the way in which  $k$ -anonymity is currently used to address this conflict does not necessarily lead to an optimum balance between privacy and information utility. We also provide recommendations for an appropriate solution for addressing the conflict between privacy and information utility.

**KEY WORDS**

Privacy, information utility,  $k$ -anonymity, microdata

# HOW APPROPRIATE IS $K$ -ANONYMITY FOR ADDRESSING THE CONFLICT BETWEEN PRIVACY AND INFORMATION UTILITY IN MICRODATA ANONYMISATION

## 1 INTRODUCTION

Microdata is one way in which statistical data can be released to the public. However, before it can be released to the public, it needs to be anonymised. Anonymisation ensures the privacy of the individuals whose data is released. As microdata is anonymised, data is removed (to some extent) from the identifying variables. As more data is removed from the identifying variables, it becomes increasingly difficult to infer sensitive data and to perform re-identification. Therefore, as microdata is anonymised, the level of privacy in the microdata increases. However, removing data from the identifying variables also reduces the accuracy and / or the completeness of the released microdata. Therefore, as microdata is anonymised, its level of information utility also decreases.

Ideally, we would like to release microdata that has high levels of privacy and information utility. However, the protection of privacy implies that we should hide and obscure data. On the other hand, releasing usable and useful data implies that we should provide data that is accurate, complete and precise (Zielinski, 2007a, 2007b). Clearly, a conflict between the needs of privacy and information utility exists. This conflict needs to be resolved before a microdata set can be released to the public.

$K$ -anonymity is often used to address the conflict between privacy and information utility in microdata anonymisation. In this paper, we determine the extent to which  $k$ -anonymity is appropriate for addressing this conflict. We argue that the way in which  $k$ -anonymity is currently used to address this conflict does not necessarily lead to an optimum balance between privacy and information utility.

## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

This paper is organised as follows. In Section 2, we provide preliminary definitions of microdata,  $k$ -anonymity, and the "optimum" balance between privacy and information utility. In Section 3, we discuss the appropriateness of the current way in which  $k$ -anonymity is used for addressing the conflict between privacy and information utility. In Section 4, we provide specific examples of how  $k$ -anonymity is used to address this conflict. In Section 5, we provide recommendations for a solution that will appropriately address the conflict between privacy and information utility. We discuss related work in Section 6 and conclude the paper in Section 7.

## 2 PRELIMINARIES

The focus of this paper is on determining the extent to which  $k$ -anonymity is appropriate for addressing the conflict between privacy and information utility in microdata anonymisation. Therefore, we will define the concepts used, namely microdata,  $k$ -anonymity, and the "optimum" balance between privacy and information utility. However, we first provide definitions for the *data owner* and the *data user*. We define the *data owner* as a person or an organization that releases microdata about individuals. For example, a data owner may be a hospital that releases microdata that contains information on its patients. We also define the *data user* as a person or an organization that requires the released microdata in order to perform specific types of data analysis.

### 2.1 Microdata

Statistical data can be disseminated in three main ways (Hundepool et al., 2007; Domingo-Ferrer, Sebe, & Solanas, 2008; Willenborg & De Waal, 2001). These include Dynamically Queryable Databases, Tabular Data, and Microdata.

Microdata is the most basic form in which statistical data can be released. It is the "raw" data from which all other statistical data outputs are derived. A microdata set may be represented as a single data matrix, where the rows correspond to the entities of the database (e.g. an individual person or a respondent) and the columns correspond to the variables of an each entity.

In the existing literature, different names for the different categories of variables of a microdata set are used by different authors. In this paper,

we shall adapt the naming conventions used by Willenborg and De Waal (2001). However, for completeness of this discussion, we also provide the alternative names used by other authors.

There are four, not necessarily disjoint, categories into which the variables of a microdata set can be classified. Before the microdata is anonymised, the data owner should determine the category of each variable.

- *Direct identifiers.* These variables are those that uniquely identify a respondent in a microdata set. A person's Passport Number, or ID Number are examples of a direct identifier. Direct identifiers are sometimes simply referred to as *Identifiers* (Ciriani et al., 2007; Hundepool et al., 2007). Before microdata is anonymised, direct identifiers are removed from the microdata set.
- *Indirect identifiers.* These variables are not necessarily unique for each respondent. However, the combination of the values of one or more indirect identifiers of a single record may create a relatively rare, or even a unique combination. Indirect identifiers are those variables on which an intruder will try to re-identify an individual respondent in a microdata set. Examples include the Date of Birth, Marital Status, or Zipcode of a person. Indirect identifiers are also sometimes referred to as *quasi-identifiers* (Samarati, 2001), or *key variables* (Hundepool et al., 2007). However, throughout this paper, we shall refer to an indirect identifier as an *identifying variable*, as has been done by Willenborg and De Waal (2001).
- *Sensitive variables.* These variables are those that contain sensitive information of a respondent. For example, a sensitive variable can be a person's disease that he sought treatment for in a hospital. These variables are also referred to as *confidential outcome variables* (Domingo-Ferrer et al., 2008; Hundepool et al., 2007), since they contain confidential information about the respondents.
- *Non-sensitive, non-identifying variables.* These variables are those that do not fall into any of the above categories. These are also referred to as *non-confidential outcome variables* (Domingo-Ferrer et al., 2008; Hundepool et al., 2007). An example of a non-sensitive, non-identifying variable may be a person's gender.



## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

However, in combination with other variables, such as the marital status, a person's gender could also be an indirect identifier. Therefore, we mentioned earlier that the four variable categories are not necessarily disjoint.

### **2.2 K-anonymity**

The concept of  $k$ -anonymity was introduced by Samarati and Sweeney (Samarati, 2001; Sweeney, 2002a, 2002b) for anonymising microdata. A microdata set satisfies the property of  $k$ -anonymity if every record in the microdata set is indistinguishable from at least  $k - 1$  other records in the same microdata set, where  $k$  is greater than 1. The inability to distinguish between different records is based on the values of the identifying variables (or quasi-identifiers - an equivalent term commonly used in the literature on  $k$ -anonymity). That is, given a record with a particular set of values for the identifying variables, the same set of values will be present in the identifying variables of at least of  $k - 1$  other records in the same microdata set.

### **2.3 The "optimum" balance between privacy and information utility**

In our research work, we regard the optimum balance between privacy and information utility as has been defined by Zielinski and Olivier (2009a). That is, the optimum balance between privacy and information utility is one in which the levels of privacy and information utility are maximised while satisfying a set of constraints that capture the data owner's and the data user's preferences. These preferences refer to the preferences that exist between each identifying variable in the microdata set, as well as the preference between the resulting levels of privacy and information utility.

The preferences between each identifying variable in the microdata set are directly related to the usefulness of the data. The usefulness of the data should be considered from both the data user's and the data owner's points of view. In the case of the data user (whose main goal is to ensure utility of data), the preferences for identifying variables should reflect the extent to which each identifying variable will be useful for the user's tasks. In the case of the data owner (whose main goal is to protect the privacy of the respondents in the microdata), the preferences are considered from a potential intruder's point of view, in terms of the perceived way in which

an intruder may use the released data to infer sensitive information. In this case, the preferences for identifying variables should reflect the extent to which we perceive that each identifying variable will be useful for the intruder in inferring sensitive data.

The preference between the resulting levels of privacy and information utility must be decided and agreed upon by the data user and the data owner. That is, it is necessary to determine if protection of privacy is considered to be equally important as providing useful data, or if privacy should assume a greater or lower importance compared to information utility. For example, if the microdata is released to only a selected group of data users, under strict confidentiality agreements made with this group, then it is certainly possible that the data owner's preference for privacy may be lower in comparison to cases where the microdata is made available to the public.

Therefore, we state our optimisation problem as follows: "Maximise privacy and information utility subject to the constraints imposed by the data user's and the data owner's preferences". In the next Section, we discuss the extent to which  $k$ -anonymity is appropriate in finding the optimum balance between privacy and information utility.

### **3 HOW APPROPRIATE IS $k$ -ANONYMITY FOR ADDRESSING THE CONFLICT BETWEEN PRIVACY AND INFORMATION UTILITY**

The use of  $k$ -anonymity is seen as a "clean way" of addressing the conflict between privacy and information utility (Domingo-Ferrer & Torra, 2005, 2008). It is seen as a "clean way" because, it is assumed that, if for a given  $k$  value,  $k$ -anonymity will provide sufficient privacy, then it allows one to concentrate on only determining how to minimise information loss (or maximise information utility) such that the given level of  $k$ -anonymity will be achieved. However, we argue that if this is assumed and if  $k$ -anonymity is used in this fashion, then it does not fully capture the objective of the optimisation problem.

First of all, it is unclear (from the literature stemming from  $k$ -anonymity) how to determine the optimum value for  $k$  that will provide "sufficient privacy" for the particular set of circumstances in which anonymisation takes place. Before we can find the optimum value for  $k$ ,

## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

we need to know what the optimum balance between privacy and information utility is for the given set of circumstances in which anonymisation takes place. Moreover, under the above assumption, when a certain  $k$  value is provided as input to anonymisation, it is provided without knowing if the given value will in fact lead to an optimal balance between privacy and information utility.

Under the above assumption, the complexity of the optimisation problem is reduced to only maximising information utility when given a certain level of privacy that needs to be achieved (i.e. a  $k$  value for  $k$ -anonymity). However, we believe that such an assumption does not take into account the whole complexity of the optimisation problem (as stated in Section 2.3). That is, such an approach does not take into account that it is *both* privacy and information utility that have to be maximised in the optimisation problem.

When the above assumption is used to solve this optimisation problem, maximising privacy is *no longer an objective function of the optimisation problem*. Instead, under the above assumption, privacy is reduced to *only a constraint under which optimisation occurs*. When privacy becomes just a constraint under which optimisation occurs, then the optimisation does not necessarily lead to a truly optimum solution. Information utility is optimised only to satisfy a given level of privacy, rather than being optimised whilst being aware of the fact that the goal of maximising information utility is in direct conflict to the goal of maximising privacy. In other words, information utility is optimised subject to a given level of privacy that is considered "sufficient".

Nevertheless, the given "sufficient" level of privacy may not necessarily be the optimum level, since the privacy level was decided upon through a means other than during the optimisation itself. This is not to say that, the optimum level of privacy will occur below the required "sufficient" or minimum level. It cannot occur below the minimum level, since otherwise the constraint of the minimum level of privacy would not be met. It is, however, possible that the *optimum* level of privacy will occur above the required minimum privacy level, but this will not be known unless privacy is optimised as well.

Note that we are not discrediting the usefulness of  $k$ -anonymisation for anonymising microdata. We are, however, stating that when  $k$ -

anonymisation is used to find the optimum balance between privacy and information utility, then the optimisation problem should be approached from both angles: the need to maximise both information utility and privacy. If this problem is approached from both these angles, then during the process of optimisation, the  $k$  value will actually be *calculated*. First, the optimum balance will be determined. Thereafter, in a second step, the optimum balance will be used to determine how the microdata should be anonymised. If  $k$ -anonymity is used as the anonymisation technique, then during the second step, the value for  $k$  will be calculated and then the microdata set will be  $k$ -anonymised with this value. In other words, the value for  $k$  will no longer be an input into the optimisation problem. The only input into the optimisation problem will be the constraints under which the optimisation should occur. These constraints are the preferences that were stated in Section 2.3.

The limitation of the way in which  $k$ -anonymity is used to address the conflict between privacy and information utility, as discussed above, relates to the objectives of the optimisation problem. Another limitation of  $k$ -anonymity, with regards to how it is currently used to address the conflict between privacy and information utility, is related to the definition of the constraints under which optimisation is performed.

In the original definition of  $k$ -anonymity, anonymisation is performed without taking into account the data user's preferences between the different identifying variables. Therefore, the anonymisation does not consider that information loss should be minimised in those identifying variables that a data user considers useful. Some enhancements of  $k$ -anonymity have addressed this shortcoming, as discussed in the next Section. In a similar way, the original definition of  $k$ -anonymity also disregards the (perceived) preferences between identifying variables that a potential intruder may have. That is, anonymisation does not necessarily ensure that the most information loss occurs in those identifying variables that we perceive to be most useful for a potential intruder. Furthermore,  $k$ -anonymity also does not take into account the preference between privacy and information utility. When we need to determine the optimum balance between privacy and information utility, these preferences should be taken into account as constraints under which the optimisation is performed. However, the original  $k$ -anonymity definition does not take these into account.

## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

To summarise, although  $k$ -anonymity shows potential as a good way to address the conflict between privacy and information utility, we argue that the way in which it is currently used is not appropriate to address this conflict. That is, the way in which  $k$ -anonymity is currently used fails to find a truly optimum balance between privacy and information utility for two main reasons. The first reason relates to the way in which the objective of the optimisation is defined. That is, the objective of the optimisation problem focuses on only maximising information utility, such that a certain level of privacy ( $k$  value) is met. To find the optimum balance between privacy and information utility, the objective of the optimisation should focus on maximising both privacy and information utility. The second reason relates to the way in which the constraints of the optimisation are defined. That is, the preferences between privacy and information utility, as well as the data user's preferences and the data owner's preferences (in terms of the perceived intruder's preferences) between identifying variables are not taken into account when optimisation is performed.

#### **4 SPECIFIC EXAMPLES OF HOW K-ANONYMITY IS USED TO ADDRESS THE CONFLICT BETWEEN PRIVACY AND INFORMATION UTILITY**

In this Section, we present a number of specific examples of how  $k$ -anonymity has been recently used to address the conflict between privacy and information utility.

Stark, Eder and Zatloukal (2006) propose a priority-driven anonymisation technique to achieve  $k$ -anonymity. The proposed technique allows specifying the degree of acceptable information loss for each variable separately. Variables that are considered useful for the data user can be protected from extensive generalization. Those variables that have been assigned low priorities are generalized first. Variables that have been assigned higher priorities are only generalized when no other solution may be found to achieve  $k$ -anonymity. Although this approach is able to take into account the user's preferences with respect to which variables will be useful to him, it is unable to take into account other constraints of the optimisation problem, namely the data owner's preferences between variables (from the perspective of a potential intruder) and also the preferences between privacy and information utility. Moreover, the

optimisation problem is addressed by considering only the need to maximise information utility such that a certain level of  $k$ -anonymity is provided.

Other utility-based anonymisation approaches were also proposed. For example, LeFevre, DeWitt, and Ramakrishnan (2006) propose algorithms that will generate anonymous data such that the utility of the data is preserved with respect to the workload for which the data will be used. Xu et al. (2006) also study the problem of utility-based anonymisation and present a framework to specify the utility of variables. Zhang, Jajodia and Brodsky (2007) propose a model and an algorithm that will guarantee safety under the assumption that the intruder knows the disclosure algorithm and the generalization sequence. Nevertheless, these works address the conflict between privacy and information utility from only one angle, namely the need to maximise information utility subject to a given  $k$  value (i.e. a level of privacy that is considered as "sufficient"). As we argued in the previous Section, considering the optimisation problem from this limited perspective does not lead to a truly optimum balance between privacy and information utility

In a more recent work, Gionis and Tassa (2009), study how to achieve  $k$ -anonymity with minimal loss of information (i.e. an optimum  $k$ -anonymisation). The authors provide an improvement on the best-known  $O(k)$ -approximation provided by Aggarwal et al. (2005) to an approximation of  $O(\ln k)$ . Nevertheless, the authors also do not consider the optimisation problem from the perspective of maximising both privacy and information utility. Instead, they aim to determine how to achieve  $k$ -anonymity with such that information utility is maximised. That is, the algorithm proposed expects that the value for  $k$  will be provided as input. However, as we argued in the previous Section, if we are to obtain a truly optimum balance between privacy and information utility, by using  $k$ -anonymisation as the anonymisation technique, then the value for  $k$  will actually be calculated during the optimisation process.

Loukides and Shao (2008) consider how a  $k$ -anonymisation can be produced with an optimum trade-off between information utility and privacy. In their paper, the needs of both privacy and information utility are considered. The optimisation problem is addressed from both these angles when an optimal anonymisation is determined. However, the

## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

proposed measure for information utility is based on the average amount of generalizations that each group of records incurs - the smaller this number, the higher the utility. This proposed measure does not consider the preferences that a specific data user may have between different identifying variables. Therefore, this measure will not be able to take into account the purpose for which the user requires the data and hence does not provide a meaningful measure for information utility. Therefore, an anonymised microdata set will not necessarily have the optimal level of information utility for a specific user and the purpose for which the data is released.

Although a number of approaches based on  $k$ -anonymity have been proposed to address the conflict between privacy and information utility, none are able to find a truly optimum balance between and information utility. The concept of  $k$ -anonymity itself is also currently being used inappropriately to address this conflict. In the next Section, we present recommendations for an appropriate solution that will ensure that the optimum balance between privacy and information utility is achieved when microdata is anonymised.

### 5 RECOMMENDATIONS FOR AN APPROPRIATE SOLUTION

When we consider the definition of the "optimum" balance between privacy and information utility provided in Section 2.3, it is clear that the way in which  $k$ -anonymity is currently used to address the conflict between privacy and information utility is not appropriate. We now provide recommendations for developing a solution that will be appropriate for determining the optimum balance between privacy and information utility.

We argue that if we are to find a truly optimal balance between privacy and information utility, then the goal of maximising *both* privacy and information utility should be regarded as *the objective function of the optimisation problem*. This stems from the fact that both privacy and information utility are desired, although they may be desired in different proportions. This is our recommendation with respect to the objective of the optimisation problem.

We also need to make recommendations that address the constraints under which optimisation should be carried out. These constraints should



reflect the preferences between privacy and information utility. The constraints should also reflect the data user's and the data owner's preferences between identifying variables. In the case of the data owner, the preferences between identifying variables should be considered from the perspective of the potential intruder (i.e. what identifying variables are considered to be most useful for an intruder in deriving sensitive data).

Therefore, a challenge exists to develop a solution that will appropriately capture the above objective and constraints and thereafter find the optimum balance between privacy and information utility. Moreover, once the optimum balance has been determined, the solution should also determine how to anonymise the microdata such that the optimum levels are achieved. Therefore, the solution should have two components: an optimisation component, in which the optimum levels of privacy and information utility are determined, and an anonymisation component, during which the microdata is anonymised.

In cases where  $k$ -anonymity is used as the anonymisation technique, the optimisation component of the solution will determine the optimum level of privacy and information utility. Thereafter, the anonymisation component of the solution will calculate the optimum value for  $k$  with which the microdata set should be  $k$ -anonymised.

## 6 RELATED WORK

Other approaches for addressing the conflict between privacy and information utility have also been proposed. In addition to  $k$ -anonymity, Domingo-Ferrer and Torra (2005) identify two other approaches. These include the *score*, and R-U confidentiality maps.

Domingo-Ferrer and Torra (2001) introduced the *score* as a way to evaluate the trade-off between information loss and disclosure risk. It was subsequently used in several other works, for example, by Medrano-Gracia et al. (2007), Nin, Herranz, and Torra (2008a, 2008b), Yancey, Winkler, and Creecy (2002). The *score* is useful in that it allows us to regard the selection of a masking technique (for microdata protection) and the parameters of the technique as an optimisation problem (Domingo-Ferrer & Torra, 2005). For example, Sebe et al. (2002) applied a masking technique to a microdata set, after which a post-masking optimisation procedure was applied to obtain an improved *score*. The main drawback of



## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

the *score*, with reference to how appropriate it is in addressing the conflict between privacy and information utility, is that it is unable to take into account the way in which the released data will be used, or the way in which we perceive the intruder to infer sensitive data. The need to take into account these preferences was one of the requirements we identified for the "optimum" balance between privacy and information utility. The *score* fails to take into account this requirement, and hence we do not consider it appropriate for finding the optimum balance between privacy and information utility.

R-U confidentiality maps (Duncan et al., 2001; Duncan, Keller-McNulty & Stokes, 2001) provide a way in which to graphically represent the conflict between disclosure risk,  $R$ , and data utility,  $U$ . After the form of the disclosure risk,  $R$ , and the data utility,  $U$ , have been specified, the task is to determine how  $R$  and  $U$  are related to the parameter values of the specific masking technique chosen to anonymise the microdata set. An R-U confidentiality map is obtained by plotting, on a two-dimensional graph, a set of paired values,  $(R, U)$ , which represent the disclosure risk and the data utility that correspond to various strategies for data release.

The graphical representation of the relationship between privacy and information utility allows one to easily determine how a particular masking technique, and its parameters, impacts the balance between privacy and information utility. It is, of course, reasonable to expect that the microdata set should be released with a level of data utility  $U$  at which the disclosure risk  $R$  will be below the maximum tolerable risk. However, by using the R-U confidentiality map alone, it is still unclear where the optimum balance between  $R$  and  $U$  occurs. One does not know if the optimum balance occurs *exactly* at the point at which  $R$  is just below the maximum tolerable risk. However, it is also quite likely that the optimum balance may, in fact, occur at a lower risk level, much lower than the maximum tolerable risk. This is certainly possible when  $(R, U)$  pairs form an exponential graph. In such cases, reducing the utility level by a small factor may result in a relatively large reduction of the disclosure risk. Hence, the optimum balance between  $R$  and  $U$  may in fact occur lower than the maximum tolerable risk, but this is not known by just examining the R-U confidentiality map.

Nevertheless, R-U confidentiality maps do not actually *determine* the optimum balance between privacy and information utility. That is, it can only *guide* the decision about how to balance the needs of privacy and information utility, by graphically representing the relationship between privacy and information utility. However, the decision where to strike the balance between privacy and information utility is still left up to the user of the R-U confidentiality map.

The research work described in this paper has been done in the context of a larger research project, the aim of which was to develop an optimal microdata anonymisation process. The recommendations provided in this paper were used as the basis for developing a solution for the optimal anonymisation of microdata. In a related paper (Zielinski & Olivier, 2009a), we use the recommendations provided here to address the optimisation aspect of the solution, where we use Economic Price Theory as the basis for determining the optimum levels of privacy and information utility that a microdata set should possess. The anonymisation aspect of the solution is addressed in another related paper (Zielinski & Olivier, 2009b), where we determine how microaggregation and  $k$ -anonymity should be used to anonymise the microdata such that the identified levels of privacy and information utility are achieved.

## 7 CONCLUSION

When microdata is anonymised, it needs to satisfy two conflicting goals: privacy and information utility. In this paper, we determined whether  $k$ -anonymity is appropriate in addressing this conflict. We have shown that the way in which  $k$ -anonymity is currently used to address this conflict is not appropriate, since it does not necessarily lead to an optimum balance between privacy and information utility. We also provided recommendations for the basis of a solution that will be appropriate for finding the optimum balance between privacy and information utility. We have subsequently used these recommendations to develop such a solution, which first determines the optimum levels of privacy and information utility (Zielinski & Olivier, 2009a) and then anonymises the microdata such that these optimum levels are achieved (Zielinski & Olivier, 2009b). This work focused on the conflict between privacy and information utility in microdata anonymisation. For future work, we aim

## How Appropriate is K-Anonymity for Addressing the Conflict between Privacy and Information Utility in Microdata Anonymisation

to explore the conflict between privacy and information utility in other forms of statistical data, such as tabular data.

### 8 ACKNOWLEDGEMENT

The work presented in this paper is part of a larger research project lead by the author at SAP Research CEC Pretoria, South Africa. The support of SAP Research and the SAP Meraka Unit for Technology Development (UTD) towards this work is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and should not necessarily be attributed to SAP Research or the SAP Meraka Unit for Technology Development (UTD).

### 9 REFERENCES

- Aggarwal, G., Feder, T., Kenthapadi, K., Motwani, R., Panigraphy, R., Thomas, D., et al. (2005). Achieving anonymity via clustering. In *Proceedings of the 10th International Conference on Database Theory*. Chicago, USA.
- Ciriani, V., De Capitani di Vimercati, S., Foresti, S., & Samarati, P. (2007). Microdata protection. In *Yu, T., Jajodia, S. (editors) Secure Data Management in Decentralized Systems* (pp. 291 - 321). Springer-Verlag.
- Domingo-Ferrer, J., Sebe, F., & Solanas, A. (2008). A polynomial-time approximation to optimal multivariate microaggregation. *Computers and Mathematics with Applications*, 55, 714 - 732.
- Domingo-Ferrer, J., & Torra, V. (2001). A quantitative comparison of disclosure control methods for microdata. In *Doyle, P., Lane J.I., Theeuwes, J.J., Zayatz, L. (editors) Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies* (pp. 111 - 134). North-Holland, Amsterdam.
- Domingo-Ferrer, J., & Torra, V. (2005). Ordinal, continuous and heterogeneous k-anonymity through microaggregation. *Data Mining and Knowledge Discovery*, 11, 195 - 212.
- Domingo-Ferrer, J., & Torra, V. (2008). A critique of k-anonymity and some of its enhancements. In *Proceedings of the 2008 Third*

Proceedings of ISSA 2009

*International Conference on Availability, Reliability and Security.*  
Barcelona, Spain.

- Duncan, G. T., Feinberg, S. E., Krishnan, R., Padman, R., & Roehrig, S. F. (2001). Disclosure limitation methods and information loss for tabular data. In *Doyle, P., Lane J.I., Theeuwes, J.J., Zayatz, L. (editors) Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies* (pp. 135 - 166). North-Holland, Amsterdam.
- Duncan, G. T., Keller-McNulty, S. A., & Stokes, S. L. (2001). Disclosure risk vs. data utility: The R-U confidentiality map. Technical Report LA-UR-01-6428, Statistical Sciences Group, Los Alamos National Laboratory, Los Alamos, USA.
- Gionis, A., & Tassa, T. (2009). k-anonymization with minimal loss of information. *IEEE Transactions on Knowledge and Data Engineering*, 21(2), 206 - 219.
- Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Lenz, R., Longhurst, J., et al. (2007). Handbook on statistical disclosure control, Version 1.01.
- LeFevre, K., DeWitt, D., & Ramakrishnan, R. (2006). Workload-aware anonymization. In *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 277 - 286). Philadelphia, USA.
- Loukides, G., & Shao, J. (2008). Data utility and privacy protection trade-off in k-anonymisation. In *Proceedings of the 2008 International workshop on Privacy and Anonymity in Information Society* (pp. 36 - 45). Nantes, France.
- Medrano-Gracia, P., Pont-Tuset, J., Nin, J., & Munes-Mulero, V. (2007). Ordered dataset vectorization for linear regression on data privacy. In *Proceedings of the 4th international conference on Modeling Decisions for Artificial Intelligence* (pp. 361 - 372). Kitakyushu, Japan.

How Appropriate is K-Anonymity for Addressing the Conflict between  
Privacy and Information Utility in Microdata Anonymisation

- Nin, J., Herranz, J., & Torra, V. (2008a). How to group attributes in multivariate microaggregation. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 161, 121 - 138.
- Nin, J., Herranz, J., & Torra, V. (2008b). On the disclosure risk of multivariate microaggregation. *Data and Knowledge Engineering*, 67(3), 399 - 412.
- Samarati, P. (2001). Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6), 1010 - 1027.
- Sebe, F., Domingo-Ferrer, J., Mateo-Sanz, J. M., & Torra, V. (2002). Post-masking optimization of the tradeoff between information loss and disclosure risk in masked microdata sets. In *Domingo-Ferrer, J. (editor) Inference Control in Statistical Databases, From Theory to Practice*, Lecture Notes in Compute Science (Vol. 2316, pp. 163 - 171). Springer-Verlag.
- Stark, K., Eder, J., & Zatloukal, K. (2006). Priority-based k-anonymity accomplished by weighted generalisation structures. In *Proceedings of the 8th International Data Warehousing and Knowledge Discovery Conference* (pp. 394 - 404). Krakow, Poland.
- Sweeney, L. (2002a). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5), 571 - 588.
- Sweeney, L. (2002b). k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5), 557 - 570.
- Willenborg, L., & De Waal, T. (2001). *Elements of Statistical Disclosure Control*. Lecture Notes in Statistics. Springer-Verlag.
- Xu, J., Wang, W., Pei, J., Wang, X., Shi, B., & Fu, A. W. (2006). Utility-based anonymization for privacy preservation with less information loss. *ACM SIGKDD Explorations*, 8(2), 21 - 30.

Proceedings of ISSA 2009

- Yancey, W. E., Winkler, W. E., & Creecy, R. H. (2002). Disclosure risk assessment in perturbative microdata protection. In *Domingo-Ferrer, J. (editor) Inference Control in Statistical Databases, From Theory to Practice*, Lecture Notes in Computer Science (Vol. 2316, pp. 135 - 152).
- Zhang, L., Jajodia, S., & Brodsky, A. (2007). Information disclosure under realistic assumptions: privacy versus optimality. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*. Alexandria, USA .
- Zielinski, M. P. (2007a). Balancing privacy and information utility in microdata anonymisation. In *Proceedings of the 2007 Digital Identity and Privacy Conference*. Maastricht, The Netherlands.
- Zielinski, M. P. (2007b). Privacy protection in eParticipation: guiding the anonymisation of microdata. In *Avdic, A., Hedstrom, K., Rose, J., Gronuld, A. (editors) Understanding eParticipation - Contemporary PhD eParticipation studies in Europe* (pp. 57 - 69). Örebro University Library, Sweden.
- Zielinski, M. P., & Olivier, M. S. (2009a). On the use of Economic Price Theory to find the optimum levels of privacy and information utility in non-perturbative microdata anonymization. (*Submitted for publication*).
- Zielinski, M. P., & Olivier, M. S. (2009b). How to determine the optimum number of records per cluster in microaggregation. (*Submitted for publication*).

## **AN ANALYSIS OF AUTHENTICATION FOR PASSIVE RFID TAGS**

**Gregory Stuart Smith<sup>1</sup> Marijke Coetzee<sup>2</sup>**

Academy for Information Technology  
University of Johannesburg  
South Africa

<sup>1</sup>Hyperionza@gmail.com  
<sup>2</sup>marijkec@uj.ac.za

### **ABSTRACT**

RFID (Radio Frequency Identification) tags have become pervasive for identifying objects, people and pets, automated payment and theft-deterrents. However, assurance of tag identity has not been built into the RFID environment. Privacy by means of encryption can prevent the data from being human readable but cannot stop a clone being created. This paper considers recent approaches that have been proposed to breach this gap. These include PUF's (Physically Unclonable Functions), cryptography, digital signatures and radio fingerprints.

This paper contributes a critical analysis of current approaches in order to identify requirements for RFID tag authentication, focusing on passive RFID tags used for product authentication.

### **KEY WORDS**

RFID tag authentication, Product authentication, PUF, RF Fingerprinting, Digital Signature, Cryptography.

## AN ANALYSIS OF AUTHENTICATION FOR PASSIVE RFID TAGS

### 1. Introduction

A basic RFID system consists of small transponders, or tags, attached to physical objects and RFID tag readers. When wirelessly challenged by a reader, the tag responds with some identifying information that may be associated with arbitrary data records. Thus, RFID systems are a type of automatic identification system, similar to optical bar codes [1], but without the requirement for active human interaction.

Throughout its development, RFID technology was considered infallible as tags and readers could not easily be copied and reproduced, as the technology was not available. Today that technology does exist [2]. Criminals with little technical knowhow and accessible RFID kits can clone tags, thereby producing counterfeit goods with seemingly authentic identifiers. Criminals who are competent in technology can use freely available, open source software [3] to copy and modify tags and reveal tag information. A clone, as used in this context, refers to the creation of an exact replica of the original.

The aim of this paper is to outline the different approaches to RFID tag authentication, both traditional and new, and to objectively lay out the weaknesses in each approach. This paper then proceeds to propose a set of requirements needed to solve the problem of authenticating RFID tags for the purpose of product authentication.

The rest of this paper is structured as follows: Section 2 outlines a case study and explains RFID tags. Section 3 defines four broad authentication models and details several implementations. Section 4 outlines criteria for comparison, tabulates the results and Section 5 briefly summarizes the table. Section 6 gives the requirements. Finally Section 7 concludes the paper.

### 2. Background

A RFID tag may claim that it is Tag X representing Manufacturer Y, identifying Object Z. Figure 1 shows Tag X, attached to an object such as a passport, representing an organization such as Home Affairs. Currently



## An Analysis of Authentication for Passive RFID Tags

the only method to verify Tag X, the RFID tag, is the unique ID embedded on Tag X itself. There is no secondary method of authenticating the tag, to support its claim to its identity and proving its authenticity.



Figure 1: RFID tags embedded in a shipping label and a passport [4].

A passive RFID tag consists of an integrated circuit (IC) that receives its power from the reader via an induction loop aerial. The aerial is also used to send and receive data. Passive RFID tags either indicate their presence, i.e. on/off, or store data between 64-bits up to 64KB [5] in length. Active tags on the other hand have their own power source, are much more powerful and have a greater read range. They can typically store up to 128KB.

Without proper authentication in order to verify that the tag being read is not a clone, an attacker can easily write fraudulent data to a fake RFID enabled passport. In such a situation no-one would be the wiser because all available information about the passport would agree to its authenticity.

To avoid ambiguity, this paper takes the term *privacy* to mean a transmission that is not in plain text. However, *privacy* cannot be taken to mean proof of *authenticity*.

How is the authenticity of a RFID tag ensured? The following section outlines four broad approaches answering this question.

### 3. State-of-the-Art Authentication Models for RFID

Authentication is defined as the process of verifying the authenticity of the RFID tag [6]. In the RFID environment there exists two main types of authentication: mutual- and product- authentication [7]. *Mutual*

*authentication* is when the tag and reader need to prove the authenticity of each other. *Product authentication* is verifying the authenticity of an object. The focus of this paper is placed on product authentication. Typically authentication is proved through at least three factors: something you are, such as the passport; something you have, such as an RFID tag, and something you know, such as some form of secret [8]. The act of authentication must be performed such that it is reliable, accurate, discrete and secure from attack [7].

In this section, four general approaches used in authenticating RFID tags are discussed. The first two of these models are traditional forms of authentication, used amongst high end RFID tags. Here, *digital signatures* and *cryptography* are discussed. The last two approaches considered are new techniques. Here, *Physical Unclonable Functions* and *radio fingerprinting* are discussed in order to determine whether it is viable to use unique device characteristics in authentication.

### **3.1.Digital Signature**

Traditionally, digital signatures [9] create a unique fingerprint of the data being transmitted. The fingerprint will differ between two users transmitting the exact same data. This provides evidence of user authenticity, guarantees data integrity and ensures non-repudiation of signed electronic data.

An approach taken [10] is to embed an immutable digital signature into the tag memory, which may be used to validate the RFID tag. The digital signature would be created using a public-key infrastructure (PKI) such as RSA [10]. The public key would be stored on the reader and the private key used to create the signature stored on the tag. The suggested minimum length of such a key is 1024-bit [11], which to the authors' knowledge, is not implemented in any RFID tag. A successful cloning attack against a digital signature transponder (DST), which does not employ an immutable digital signature, is described in [12]. The key length, which was said the vendor to be safe at the time, was 40-bits. A far cry from 1024 bits.

**Analysis:** Immutable digital signatures are vulnerable to cloning. An unchanging bit-stream is transferred between tag and reader. A bit-stream copy may be created and written to an RFID tag simulator or even a new

RFID tag. An immutable digital signature [11], fails to provide adequate security measures in authenticating RFID tags.

### 3.2. Cryptography

Traditional cryptography has some role in authentication, be it in use as part of a digital signature, as above, or merely by saying that only authorized parties have the keys necessary to decrypt the message. However, as far back as 1996 [13], 56-bit symmetric keys were being broken with regularity. In 2005 the 112-bit TrippleDES algorithm was labeled as inadequate by NIST [14]. AES, the currently recognized mainstream cryptographic standard, has a minimum key length of 128-bit [15]. However, this paper's focus is not on traditional cryptography on high-end devices, rather this section considers a selection of the cryptographic algorithms available for use in RFID tags. In this section the *One-Time-Pad* approach used by Electronic Product Code (EPC) tags is discussed. This is followed by the recently broken Mifare Classic's *Crypto-1* cipher. Lastly, a hardware implementation of the *VEST-4* stream cipher is discussed.

***One-Time-Pad:*** EPC Class 1 Generation 2 tags [16] are passive RFID tags that make use of a one-time-pad for certain commands, these being Write, Kill and Access. Authentication data is generated by the one-time-pad and transmitted in the clear. It is recommended that tags use unique passwords and that memory operations be performed in a secure location, which is not always possible.

***Crypto-1:*** Crypto-1 is a cipher using only a 48-bit key [17]. The algorithm was kept private, thus enabling security through obscurity. In 2008, a research group in the Netherlands successfully reverse engineered a Mifare Classic RFID tag [17], and conducted fraudulent transactions. The successful attack on the Crypto-1 cipher is an indication that the key lengths possible within the constraints of RFID are not sufficient to provide adequate security for either privacy or authentication for a determined attacker.

***VEST-4:*** Very Efficient Substitution-Transposition or VEST ciphers [18] are implemented in hardware with keys ranging from 80 bit and upward. VEST ciphers have, since publication in 2005 [19], till at least 2007 had a clean security record, with the fastest method of attack being a serial

brute force attack. Unfortunately, VEST ciphers exceed the specifications of more limited RFID tags.

**Analysis:** Cryptographic techniques available to RFID technology are severely limited in nature and strength. This is primarily due to cost constraints [20]. It must be pointed out that a key length of 48 bits, such as that used in Crypto-1, is less than 20% of the bits currently used in online encryption. As such cryptography should not be used in RFID for the purpose of authentication because of weak encryption (short keys), but used for weak information hiding (privacy).

The discussion to this point has been of well established models used in authentication in the electronic world. This paper now moves away from these models, changing focus to new and emergent models that focus on the inherent characteristics of devices that make them unique. Next this paper discusses *Physical Unclonable Functions* and *Radio Frequency Fingerprinting*.

### 3.3. Physical Unclonable Functions

The Integrated Circuit (IC) that contains the logic of an RFID tag has physical and electrical characteristics that exist as a result of the manufacturing process. These characteristics can ideally be used for authentication. Such characteristics are unique and it is impossible to intentionally create a duplicate. This is not to say that a duplicate may not exist as there is no control over these characteristics during the manufacturing process [21]. Characteristics are a result of material imperfections and irregularities in the doping and etching process. Recent research attempts to harness, measure, and extract these characteristics. A Physical Unclonable Function (PUF) is an implementation specific circuit that has been designed to extract these features [22] and is added into the IC of the RFID tag whose characteristics are to be measured and used in authentication. A particular drawback of this method is that each RFID tag that is manufactured would have to be tested repeatedly. This is to accommodate any electronic noise that may be present, and build a database of challenges and responses to be used for authentication. The result of the PUF is a set of fingerprints, or *challenge-response pairs* (CRP's), that are stored in the database of some relevant authority. Next

## An Analysis of Authentication for Passive RFID Tags

the *Vera X512H* RFID tag and the *FERNS* algorithm, as a means of using PUF's to determine authenticity are discussed.

***Vera X512H:*** Released late 2008, it is claimed to be unclonable [23]. The RFID tag uses PUF technology in a challenge – response environment, where recorded challenges must be matched with their recorded responses generated by the PUF circuit by processing the challenge. Each challenge – response pair may only be used once to avoid man-in-the-middle and replay attacks. The match need only be above 75% for the tag to be taken as authentic [24]. The challenge is sent through the PUF circuitry, which uses delay characteristics of various components. Verayo claims a failure rate of less than one in billion [25]. Vera X512H is based on preliminary work with delay based arbiter PUF's presented in [26], [27] and [28]

***FERNS:*** uses a different kind of PUF than Vera RFID tags. FERNS [29], is based on the transient power-on state of Static Random Access Memory (SRAM). This state, measured before the SRAM is initialized, can produce a unique set of values. However, the transient power-on states of SRAM can be affected by environmental noise. Thus, before releasing to market, the manufacturer would have to accurately map the set of values by aggregating many readings in different environmental conditions. A major flaw for use in authentication is that its output is a static digital response, and as such is susceptible to replay attacks. There is no dynamically generated challenge to prevent such an attack.

***Analysis:*** As Karsten Nohl points out in [22] the designers of PUF's cannot anticipate the output, given an arbitrary input, merely by looking at the design. As he terms it, it is security-by-obscurity par excellence. There is no guarantee that the characteristics of the electronics will be unique. Transmitting the PUF results insecurely open the approach up to man-in-the-middle as well as replay attacks, as only a limited number of challenge-response pairs are recorded and used. Whilst PUF's are secure from creating intentional clones on other tags, it is not secure from a device capable of simulating a RFID tag, assuming the attacker has unlimited contact time with the tag.

### 3.4. Radio Frequency Fingerprinting

Using unique characteristics to identify electronics is an area undergoing staunch research. Some success [30], [31] in measuring, and subsequently

using the characteristics of wireless and wired network cards and their transmissions over their respective mediums, for device identification has been observed. This shows that, for a small environment, devices that transmit data over wires or radio frequency, have a unique way of doing it. Applying this to authentication is trivial. If each device, such as an RFID tag, that transmits data has a unique way of doing so, then it is logical to assume that two transmissions would then come from the same RFID tag if their transmission characteristics match.

As with PUF's, this model uses the unintentional characteristics created in a circuit during manufacture in an attempt to uniquely identify the circuit and prove its authenticity. However, as opposed to measuring these characteristics on the tag itself, the reader measures the effect they have on the transmissions and radio spectrum [32]. A patent exists [33] to match this approach. However further details, of its implementation regarding RFID tags, is not available. There is very little literature regarding this approach.

*Analysis:* Each radio transponder has different characteristics associated with it, also called transients. These transmission characteristics can sometimes be used to identify a particular transmitter. Unfortunately it is not reliable [34] as not all the fingerprints created by the transmission characteristics will be unique enough to prove an identity.

Having completed a discussion on each of the four different models available to the task of authenticating RFID tags, this paper now draws a comparison of the approaches discussed to determine the best approach for RFID product authentication.

#### **4. Comparison of Authentication Models**

The resource constrained nature of the RFID environment, used for product authentication, is the focus of the comparison. This paper addresses a RFID system, both tag and reader, with no form of authentication or privacy built into it. The purpose is to show the change required from such a system using both traditional and new approaches, to have a common point of comparison. The terms of comparison used in Table 1 are:

#### **4.1.Implementation**

Broken up into several criteria, this section focuses on the characteristics of the various implementations of the four models.

- Privacy or Authentication: is the model better suited to hiding of information (privacy), as opposed to proving a products authenticity?
- Cost Effectiveness: this shows how cost effective an implementation would be were it to be implemented.
- Resource Consumption: will the approach use a “High”, “Average”, “Low” or “None” amount of resources available to the tag to complete its function?
- Reliability: how reliable is the implementation regarding read errors and mismatches? Unfortunately not all models have data regarding this.
- Strength: how much difficulty must an attacker go to, to create a duplicate RFID tag or RFID simulation device?
- Speed: how many RFID tags may be read per second?

#### **4.2.Compatibility**

Compatibility refers to two possible states, either forwards compatibility or backwards compatibility.

- Forwards: given a vendor who has implemented a RFID solution prior to the authentication model being implemented, would the old implemented system be capable of reading the new model RFID tags without unreasonable modification.
- Backwards: given a vendor who implements a RFID solution after the implementation of the authentication model, would it still be capable of reading old RFID tags that have not implemented the new authentication model.

Under either circumstance of compatibility, authentication is not possible. The hardware or firmware required to perform authentication activities would not be present. The implemented system would only be able to identify the RFID tag being queried and not authenticate it.



#### 4.3. Stage most affected by change

This refers to the stage of production, design or manufacture, which would be most affected, in terms of time, should the authentication model become standard.

#### 4.4. Change required from base technology

This refers to the change that is required by the new model with respect to the reader / writer devices and the RFID tag itself. The categories by which these will be laid out are as follows. “Significant” - a major change would be incurred. “Some” - a degree of change is necessary. “Minor” - a small addition either of a circuit or programming would be incurred. And finally “None” - no change to the tag or reader would be incurred at all.

### 5. Analysis

The analysis of Table 1 briefly highlights issues that stem from the traditional and recent approaches to authentication in passive RFID tags.

**Traditional:** Both *digital signatures* and *cryptography*, save for the *one-time-pad*, have a fairly high cost in terms of resources within the RFID tag. The lack of resources available in passive RFID tags has led to all the traditional forms of authenticating RFID tags having been broken. To add the necessary resources would increase the cost of the tags beyond the reasonable point. These approaches are clearly not suited to authentication of passive RFID tags.

Next, a critical analysis is performed of more recent approaches.

**Recent:** *PUF's* and *Radio Fingerprinting* (RFF) are both the result of inherent, unintentional characteristics within the circuitry caused as a result of the manufacturing process. PUF's rely on a digital state to generate their fingerprints and would require a small additional circuit built into the RFID tag to monitor and measure these functions. RFF would require no additional circuitry on the RFID tag itself, but requires a greater addition to the reader, neither of which affects the current operation of a RFID tag, rather extending it. This ensures both *forwards-* and *backwards- compatibility*. Neither PUF's nor RFF are reported to have been broken, which would indicate a high level of resilience against



Table 1. Comparison of discussed authentication models. **An Analysis of Authentication for Passive RFID Tags**

		Digital Signatures		Cryptography			Physical Unclonable Functions		Radio Fingerprint
		Digital Signature	DST	One-Time-Pad	Crypto-1 Hitag-2	Vest	Vera X512H	FERNS	
<b>Implementation</b>	<b>Privacy</b>			X	X	X		X	
	<b>Authentication</b>	X	X				X		X
	<b>Cost Effectiveness</b>	Poor	Average	Good	Average	Poor	Average	Average	Good
	<b>Resource Consumption</b>	High	Average	Low	Average	High	Low	Low	None
	<b>Reliability</b>	Good	Good	Poor	Good	Good	Good	Poor	Poor
	<b>Strength</b>	Low	Low	Low	Average	High	High	Average	High
	<b>Speed</b>	Unknown	Unknown	Fast	Unknown	Fast	Fast	Fast	Unknown
<b>Compatibility</b>	<b>Forwards</b>	No	No	No	No	No	Yes	Yes	Yes
	<b>Backwards</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Stage affected by change most</b>	<b>Design</b>	X	X	X	X	X			
	<b>Manufacture</b>						X	X	X
<b>Change required from base technology.</b>	<b>Reader / Writer</b>	Significant	Significant	Significant	Significant	Significant	Some	Some	Significant
	<b>Tag</b>	Significant	Significant	Significant	Significant	Significant	Minor	Minor	None
<b>Implemented</b>		No	Yes	Yes	Yes	Experimental	Yes	Experimental	Experimental
<b>Broken</b>		No	Yes	Yes	Yes	No	No	No	No

attack. Evidence of this resilience lies in that there is no published report about current implementations, of these technologies being broken. This makes them good candidates for authenticating resource constrained passive RFID tags. To refer back to the definitions differentiating *privacy* from *authentication*, it becomes obvious as to why PUF and RFF technology is better suited to authentication as opposed to privacy. At no point in time do these technologies perform any cryptographic or other data obscuring operations, except, as in the case of PUF, on the authentication data itself.

Next, the proposed requirements for an authentication model for passive RFID tags are laid out.

## 6. Requirements for Passive RFID Authentication

To supply the definition of authentication again: Authentication is defined as the process of verifying the authenticity of the RFID tag [6]. The focus of this paper has been specifically on *product authentication* with regards to passive RFID tags. The following requirements are now proposed, which match and extend the definition of authentication as given in Section 3:

- Resource consumption: the approach should not rely overly much on the resources provided by the passive RFID tag, these are few and costly.
- Strength: should be such that the attacker needs put a substantial amount of effort towards breaking the approach, making it not worth their while. The approach should also consider that an attacker may not have limited time with a captured passive RFID tag.
- Speed: in today's fast paced lifestyle, seconds matter, anything too slow, becomes cumbersome to use, and oft times finds itself discarded on the wayside.
- Reliability: read errors, false negatives and false positives breed frustration for the end user and should be limited.
- Cost effectiveness: the approach should be such that RFID remains a feasible solution, especially for product authentication in which the number of passive RFID tags is no longer trivial.

## An Analysis of Authentication for Passive RFID Tags

- **Compatibility:** the aim of a new approach should be of maintaining functional compatibility with existing systems. Instead of changing technology, the new approach should extend current technology. Thereby including markets with previous systems without forcing a change.
- **Stage of production:** to minimize cost and contact time with the manufacturers, the stage affected most by implementing an approach should ideally be the design stage.

The authors believe that PUF's are a viable model for use in authenticating passive RFID tags. PUF's meet most of the requirements as laid out above. However, the very nature of the unpredictability of a PUF should be cause for concern. The entire set of possible CRP's cannot possibly be stored and the single-use policy of a CRP indicates that a periodic update would be necessary to avoid re-using a CRP. Future research would need to discover a way of avoiding this inconvenience. Next, the conclusion of this paper.

### **7. Conclusion**

This paper introduces the problem of authentication in a resource constrained environment, such as passive RFID tags, providing background and examples. It then discusses four broad models and several implementations of these models in order to uncover issues involved with authenticating passive RFID tags. After this discussion this paper performs a critical analysis of the implementations, the results of which are tabulated and highlighted. The main contribution of this paper is that it identifies a set of requirements that a passive RFID tag should implement when considering authentication.

Future research will be performed in order to identify an approach to passive RFID authentication whose nature is predictable and controllable, without the need to be measured, that meets the requirements set out in this paper.

### **Bibliography**

- [1] Weis, S. A. (2006). RFID (Radio Frequency Identification): Principles and Applications.

Proceedings of ISSA 2009

- [2] Trossen Robotics. (Accessed 16/04/2009). RFID Catalogue Home. <http://www.trossenrobotics.com/store/c/2784-RFID.aspx>.
- [3] RFIDIOT. (2008). <http://rfididiot.org/>.
- [4] [www.gadgettastic.com](http://www.gadgettastic.com). (2008). [rfid\\_passport](http://www.gadgettastic.com/wp-content/2008/08/rfid_passport.jpg). [http://www.gadgettastic.com/wp-content/2008/08/rfid\\_passport.jpg](http://www.gadgettastic.com/wp-content/2008/08/rfid_passport.jpg).
- [5] Williams, D. H. (2004). RFID - Hot Technology with wide ranging applications.
- [6] Office of Information Dissemination Program Development Service. (2005). Authentication. Washington, D.C.: U.S. Government Printing Office.
- [7] Soon, T. J., & Tieyan, L. (2008). RFID Security. Information Technology Standards Committee.
- [8] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2007). Fourth-Factor Authentication: Somebody You Know.
- [9] Arx. (2009). Digital Signatures FAQ. <http://www.arx.com/digital-signatures-faq.php>.
- [10] Texas Instruments Incorporated. (2006). Increasing Security in the Supply Chain with Electronic Security Markers.
- [11] Texas Instruments Incorporated. (2005). Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies.
- [12] Bono, S. C., Green, M., Stubblefield, A., Juels, A., Rubin, A. D., & Szydlo, M. (2005). Security Analysis of a Cryptographically-Enabled.
- [13] Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., et al. (1996). Minimal Key Lengths for Symetric Ciphers to Provide Adequate Commercial Security. <http://www.crypto.com/papers/keylength.txt>.
- [14] Department of Commerce. (2005). Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS)46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard and FIPS 81, DES Modes of Operation. In N. I. Technology, Fedeal Register (Vol. 70).

An Analysis of Authentication for Passive RFID Tags

- [15] National Institute of Standards and Technology. (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards.
- [16] EPCglobal Inc. (2008). EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0.
- [17] Garcia, F. D., de Koning Gans, G., Muijrs, R., van Rossum, P., Verdult, R., Wichers Schreur, R., et al. (2008). Dismantling MIFARE Classic. Nijmegen: Radboud Universiteit Nijmegen.
- [18] O'Neil, S., Gittins, B., & Landman, H. A. (2006). VEST Ciphers (eStream Phase 2). [www.vestciphers.com](http://www.vestciphers.com).
- [19] Synaptic Laboratories Limited. (2007). VEST Enhanced Smart Cards. [www.vestciphers.com](http://www.vestciphers.com).
- [20] Jain, V. (2006). Radio Frequency Identification: The Current and Future Solutions for Privacy and Authentication.
- [21] Radio Comms. (2008). Electronic DNA enables unclonable RFID chips. <http://www.radiocomms.com.au/articles/27871-Electronic-DNA-enables-unclonable-RFID-chips>.
- [22] Nohl, K. (2008). Bold Security Claims about PUFs on RFID.
- [23] Verayo. (2008). Vera X512H Unclonable RFID IC.
- [24] RFID Journal. (2008). PUF Technology Catches Clones.
- [25] Verayo. (2009). Physical Unclonable Functions: Performance and reliability. <http://www.verayo.com/technology/technology.html>.
- [26] Gassend, B., Clarke, D., van Dijk, M., & Devadas, S. (2002). Silicon Physical Random Functions. Computer and Communication Security Conference.
- [27] Gassend, B., Lim, D., Clarke, D., van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits.
- [28] Suh, G. E., & Devadas, S. (2007). Physical Unclonable Functions for Device Authentications and Secret Key Generation.

Proceedings of ISSA 2009

- [29] Holcomb, D. E., Bureson, W. P., & Fu, K. (2007). Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID tags.
- [30] Franklin, J. e. (2006). Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting.
- [31] Gerdes, R. M., Daniels, T. E., & Russell, S. F. (2006). Device Identification via Analog Signal Fingerprinting.
- [32] Hall, J., Barbeau, M., & Kranakis, E. (2003). Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase.
- [33] Clarke, J. B. (2006). RADIO FREQUENCY FINGERPRINTING TO DETECT FRAUDULENT RADIO FREQUENCY IDENTIFICATION TAGS. <http://www.wipo.int/pctdb/images4/PCT-PAGES/2006/322006/06083468/06083468.pdf>.
- [34] Ellis, K. J., & Serinken, N. (2001). Characteristics of radio transmitter fingerprints.

An Introduction to Emerging Threats and  
Vulnerabilities to Create User Awareness

## **AN INTRODUCTION TO EMERGING THREATS AND VULNERABILITIES TO CREATE USER AWARENESS**

**N Veerasamy & B Taute**

Council for Scientific and Industrial Research (CSIR)

[nveerasamy@csir.co.za](mailto:nveerasamy@csir.co.za)

+27 841 2893

PO Box 395

Pretoria 0002

### **ABSTRACT**

With technological change and advancement, attackers are increasingly becoming more sophisticated in their attack strategies and techniques. Other global factors and developments also impact the line of attack. This paper provides an introduction to the most current, pertinent attack strategies and trends. It aims to create an awareness of emerging areas that should be better studied and understood. The paper addresses the blurring lines of cyber crime, information warfare and cyber terror to indicate the key concerns at a national, commercial, governmental and individual level. Thus, the paper proposes and discusses topical security threats to elucidate their methodology and gauge their impact such that further strategic, operational and technical measures can be taken

### **KEY WORDS**

Cyber crime, cyberterror, Information Warfare, security, threats

## **AN INTRODUCTION TO EMERGING THREATS AND VULNERABILITIES TO CREATE USER AWARENESS**

### **1 INTRODUCTION**

ICT networks are regularly the target of various exploits. However, due to poor user awareness the ease and impact of attacks is missed. This paper attempts to clarify the current perspectives of information security exploitation by providing an introduction to emerging threats.

Enormous investment is put into tools, personnel and procedures to better protect systems. Technical evaluations and analysis can identify security threats, but by instilling good security awareness many mistakes can be prevented upfront.

In addition, by looking at threats from a higher-level perspective, understanding can be gained into the underlying motives and areas of impact. This view is given in the framework proposed in Section 2. It is also important to take note of the influence of global trends and issues that impact the development of new attack techniques. Thus, by studying attack trends, knowledge can be gained into more effective protective techniques and emerging areas that should not be overlooked. This will be addressed in the discussion of top exploits in Section 3.

### **2 FRAMEWORK**

As a preliminary introduction to information security threats and vulnerabilities a framework is presented that depicts the current state of the various perspectives of technological information exploitation. The framework (Figure 1) commences with the different perspectives of perpetrators, then their underlying motives which is enabled by information security exploits through the portals of Information Communication and Technology (ICT) networks and leaves on impact of different domains. A brief discussion of the framework follows.

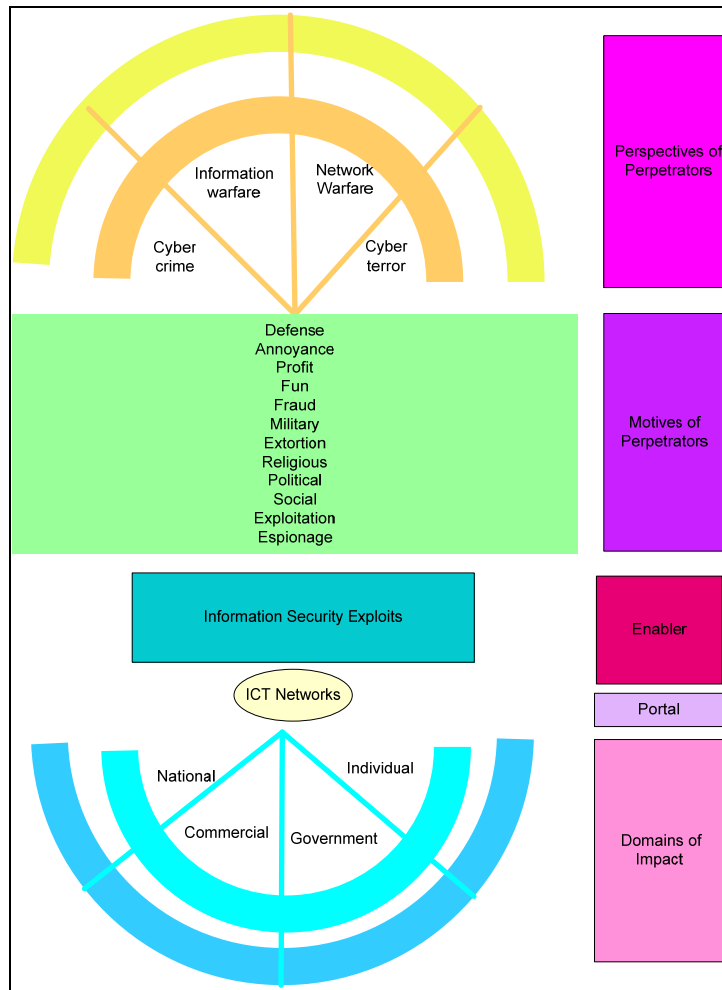
#### **2.1 Perspectives of Perpetrators**

When an attack takes place on a network or computer, the media often labels it as an act of cyber terror or a hacking incident. However, much misconception exists over whether an attack on the network is information



An Introduction to Emerging Threats and Vulnerabilities to Create User Awareness

warfare, cybercrime, or cyberterror. A brief discussion follows to place these concepts into perspective (Figure 1).



*Figure 1: High-level Framework of Current State of Information Security*

Symantec defines cybercrime as criminal activities using a computer, network or hardware device where the computer or device may be the agent, facilitator or target of the crime [9]. Information warfare implies a range of measures intending to protect, exploit, deny or destroy information and resources to gain a significant advantage over the adversary (Alger in [5]). Thus information warfare addresses both

offensive and defensive areas whereas cyber crime largely looks at attack activities. Network warfare can be seen as an enabling component of Information Warfare which sees conflict in the networked forms of communication. Thomas argues that the core of computer Network Warfare is to disrupt the layers in which information is processed with the objective of seizing and maintaining control of network space [17].

Cyberterror addresses unlawful attacks and threats against computers, networks, and information done to intimidate the government or its people to further certain political or social objectives and thus cause violence or enough harm to generate fear [10]. Cyberterror can thus form part of both information warfare, network warfare and cyber crime. Cyber terror largely operates from political, religious or social motives and thus when invasive illegal activities are committed, it can be considered as cybercrime. Furthermore, hacking describes activities to break into systems covertly and exploit vulnerabilities. Thus, hacking relates to techniques to carry out cyber crime, information warfare and cyberterror. Another aspect of cybercrime linked to cyberterror is that hackivists, who will engage in hacking activities from a political standpoint [19].

From the discussion, a key distinguishing factor will be the motive that will determine whether an attack is cyberterror, cybercrime, or information warfare and is discussed next.

## **2.2 Motives of Perpetrators**

The outcome of security exploitation is to have a beneficial result for the perpetrator: be it financial reward or the satisfaction gained from causing inconvenience. Some typical motivating factors follow:

- Cyberterror: social, religious, political, philosophical [8][6][15][7]
- Cybercrime: fraud, espionage, sabotage, extortion [11]
- Information warfare and network warfare: exploitation, military, defense [3]
- Hackivists : hacking for political reasons [19]
- Hacking: fun, profit, cyberterror, cybercrime, information warfare, hackivism[14]

Some motivating factors cross categories. For example, exploitation is applicable to cybercrime, network warfare and information warfare. Thus, the lines are quite blurred and a closer inspection of the target can shed light on the intended impact. The discussion therefore moves to the domains of security exploitation which looks at the target areas.

### **2.3 Domains of Impact**

Information security exploitation can have an impact at four typical levels. This includes National, Governmental, Commercial and Individual:

Denning states that serious attacks against critical infrastructures would be acts of cyberterrorism, depending on their impact [10]. If we were to look at cyberterrorism, cyberterrorists would typically launch attacks at targets of national and governmental importance as this would have the biggest impact. However, victims of cybercrime and actors of information warfare can be found across all four domains. Cybercriminals attack various individuals and companies and defensive strategies of information security are also applied across government, industry and personal systems.

### **2.4 Summary of Framework**

ICT networks are the portals through which information security exploitation is taking place. Information security can be classified as cybercrime, information warfare or cyberterror depending on the underlying motive. However, in many instances activities are blurred and clear boundaries cannot be established. Nevertheless, the combination of various threats, vulnerabilities and risks enable information security exploitation. Thus the focus shifts to exploits to look at emerging trends and create user awareness.

## **3 TOP EXPLOITS TO ALL DOMAINS OF IMPACT**

Currently the most common and critical threats facing users: Trojans, phishing with custom malware and web application vulnerabilities [13]. A discussion of each of these areas follows.

### **3.1 Trojans**

A Trojan is code that hides inside a program and performs a disguised function [16]. Trojans provide the ability to control a machine and thus monitor activity and download information. In the Symantec Global

Internet Threat Report, Trojans made up 71% of the volume of the top 50 malicious code samples [18]. The type of information that can be gained access to include: trade secrets (Commercial domain), classified data like strategy and policy documentation (National domain), identification or voting records (Governmental domain) and email or Internet banking records (Individual domain).

Thus, the impact of Trojans is felt across the board from national to individual level. Typical types of Trojans as listed by the IBM X-Force study include Infostealers (keyloggers, password stealers) and Clickers (provide revenue through malicious traffic generation) [1].

### **3.2 Phishing with Custom Malware**

Users are often sent emails requesting an update of personal details by clicking on an embedded link. The spoofed sender is typically shown as banks and other reputable vendors. According to IBM, 82% of targets in 2008 were financial institutions [1]. Users are actually redirected to a malicious site where they are prompted to enter personnel information which is then harvested for other fraudulent activities. Users could also be installing rootkits and other malware when clicking on links, thus providing control of machines to the perpetrators.

Other emerging scams include scareware and ransomware. With scareware, false security warnings are displayed encouraging users to download a named security tool [4]. The user's clicks are redirected to a malicious site whereby malware is downloaded. Thus, users are tricked into installing harmful software.

Ransomware occurs when data is kidnapped and encrypted. The attackers demand payment in return for the decryption key. This form of extortion originated in Russia but has since surfaced around the world [4].

### **3.3 Web Application Vulnerabilities**

SQL injection takes place when there is improper validation of user input. According to IBM, SQL injection vulnerabilities increased a staggering 134% from 2007 [1]. This indicates that even though this vulnerability is not a new exploit, its application is still wide-spread. With SQL injection, access to sensitive information in databases can be gained and thus the integrity of information on web sites and in transactions could be in

jeopardy if data is deleted or modified. New attacks could also be embedded in the database and thus be used against other visitors to the site. Examples would be to redirect visitors to a vulnerable web site or manipulate a feedback form by generating a query to select and modify supplier details through cleverly crafted SQL statements.

Cross-site scripting also takes advantage of improper validation of user input and can utilise cookie theft to hijack sessions, gain access to sensitive information, manipulate fields and commit fraudulent transactions [18]. Another manipulation technique is to embed vulnerabilities or scripts to steal information

Thus, various techniques exist to trick users into downloading malicious software and these types of attack will continue to fool users unless some awareness is created on the topic. In addition, other trends stemming from global issues also emerge and are discussed next.

#### **4 THE NEW FACE OF THREATS**

Whilst not new, spam continues to be a thorn in the side of many network administrators. The economic crisis could also see new avenues of exploitation as people try to make the quick buck. However, a crucial area of exploitation will be sites like Facebook and Myspace. Another area that is often overlooked is the spreading of infections on storage devices like USB and flash drives. In addition, the underground server economy provides an extensive black market for malicious exploits and other resources. A brief discussion on each of these issues follows.

##### **4.1 Spam**

In previous years, spam made up 71% of monitored email traffic [18]. Phishing scams can also be distributed using spam. As a consequence, with poor user awareness, an ignorant or ill-informed user could be enticed or manipulated into believing that a received link is a genuine message from a bank or vendor.

Spam trends are changing in terms of delivery methods like pdf, random text and image spam (complex images, random pixels and borders to disguise intention) [1]. Users are attracted to a range of services being offered from handbags to watches. The implications include the storage resources, engagement in unnecessary services and resource wastage. The

impact of bringing down one of the key spamming role-players was felt when the spam host McColo Corporation had the plug pulled out on them in November 2008. McColo is believed to have been responsible for up to 60% of worldwide spam [12].

#### **4.2 Economic Crisis**

With the current downturn in the economy and unemployment at such a high rate, the negative situation could be further exploited through the exploitation of people's fears and quest for financial stability. McAfee predicts that 2009 will see many fake web sites and services being hosted [12]. Examples include transactional services, investment firms and legal services. Phishing scams could also utilise these tactics.

#### **4.3 Social Networks Exploits**

Social networks like Facebook, Hi5, Friendster and MySpace are becoming targets of spam, adware, malware and other social engineering scams. At the end of 2008, the Koobface exploit surfaced. According to the Computer Emergency Response Team (CERT) advisory, it is spread through an invitation which provides a link to a video in which users are prompted to update Adobe Flash Player [2]. When users agree to the download, it is actually malicious code being installed. These social networks provide a wealth of information in terms of personal details, tracking activities and interests. They can also be used to profile users and commit acts of identity theft, fraud, spoofing and various other exploits.

#### **4.4 Storage Devices**

The unregulated use of USB and flash memory discs can see the widespread leakage, theft, loss or infection of data across enterprises, governments, commercial companies and individual users' systems.

#### **4.5 Underground Economy Servers**

The criminal black market is a hub to advertise and trade in stolen information and services, as well as required tools and data. Typically the type of goods available on these servers includes [9]:

- Information : Government issued identification numbers, credit card numbers, credit card verification numbers, debit card numbers, PINs, user accounts, email address lists, bank accounts

- Services: Scam page hosting, job adverts to be scam developers or phishing partners
- Applications: Malware, Zero-day exploits

From a security point of view at a national level, the ability to track and shut down these sites has become an issue. However, due to the nature of these servers, they can shut down quickly and move to a new site. From an individual level, users need to be made aware of the ease and frequency of exploitation and be aware that personal information can be sold off.

#### **4.6 Defensive Strategies**

A few defensive techniques are listed to help protect against some of the described information security exploits (whilst remembering that many threats have no identified solutions as yet).

- It is advised to rather use reputable vendors instead of following the prompts from displayed warning messages.
- Be aware of suspicious sites or emails (many anti-virus software have automatic scanning of potential vulnerabilities)
- Refrain from clicking on sent URL's in emails but rather navigate to the site itself and try and find listed location
- Users need to be made aware of regularly backing up data to prevent becoming a victim to ransomware attacks
- Defensive tool like anti-virus, anti-malware and firewalls have to be regularly updated
- Remain current with patch updates (web application fixes)
- Spam filters, use of alternate email address when browsing to prevent spam being sent to main email address
- Be very cautious when disclosing personal information on social networks
- Using an assigned memory stick for external connections and routine scanning/formatting when using it on sensitive systems
- Regulation is needed to control portable drives and users need to be better educated on the sensible use of these portable devices.

## 5 CONCLUSION

A worldwide battle has emerged in the form of hacking, cybercrime, information warfare, network warfare and cyber terrorism. At the heart of these areas is information security. Threats like phishing, Trojans, and web vulnerabilities still exist but are finding new avenues of exploitation like preying on people's insecurities during the economic crisis and kidnapping data. Thus, users need to be made aware of these techniques and remain vigilant for scams and other deceptive techniques. Users should not fall into a false sense of security but be knowledgeable of the potential traps of social exploits and that disclosed personal information is not necessarily secure and private. Defensive mechanisms need to be instituted across the domains. This translates to: the establishment of a Computer Security Incident Response Team (CSIRT), in-house security awareness and maintenance programs (typically ISS at a commercial and governmental level) and personal security awareness like getting alerts from security web sites and organisations.

This paper presents a structured overview of the underlying perspectives, motivation, application areas and techniques of information security exploits so as to create an awareness of the current face of threats in the global networked space.

## 6 REFERENCES

- [1] Anonymous, "IBM Internet Security Systems X-Force 2008 Trend and Risk Report," IBM Global Technology Services, 2009.
- [2] Anonymous, "Malicious code targeting social networking site user," US Computer Emergency Readiness Team (CERT), Accessed 7 April 2009, Available online at <http://www.us-cert.gov/current/archive/2009/03/04/archive.html>.
- [3] N. Bhalla, "Is the mouse click mighty enough to bring society to its knees?" *Computer Security*, vol. 22, pp. 322-336, 2003.
- [4] G. Cluley, "Viruses and Spam 2008: A look at the current security landscape and future trends," 19 August 2008.
- [5] B. Cronin and H. Crawford, "Information warfare: Its application in military and civilian contexts," *The Information Society*, vol. 15, pp. 257-263, 1999.



An Introduction to Emerging Threats and  
Vulnerabilities to Create User Awareness

- [6] K.C. Desouza and T. Hensgen, "Semiotic emergent framework to address the reality of Cyberterrorism," *Technological Forecasting and Social Change*, vol. 70, pp. 385-396, 2003.
- [7] A. Embar-Seddon, "Cyberterrorism: Are we under siege?" *Am.Behav.Sci*, vol. 45, pp. 1033, 2002.
- [8] C. Foltz Bryan, "Cyberterrorism, computer crime, and reality," *Information Management & Computer Security*, vol. 12, pp. 154-166, 2004.
- [9] M. Fossi, E. Johson, M. Turner, J. Blackbird, D. McKinney, M.K. Low, T. Adams, M.P. Laucht and J. Gough, "Symantec Report on the underground economy," Symantec, 2008.
- [10] S. Gordon and R. Ford, "Cyberterrorism?" *Computer Security*, vol. 21, pp. 636-647, 2002.
- [11] I. Lachow, "Cyber security: A few observations," National Defense University, 2008.
- [12] McAfee Avert Labs, "2009 Threat predictions," McAfee, 2009.
- [13] H. Meer and C. van der Walt, "Cyberterrorism threats," Sensepost, Personal communications on 11 March 2009.
- [14] Nortel Networks and Aspen Institute, "The promise of global networks (Annual Review of the Institute for Information Studies)," Institute for Information Studies, 1999.
- [15] M.M. Pollitt, "Cyberterrorism - fact or fancy?" *Computer Fraud & Security*, vol. 1998, pp. 8-10, 1998.
- [16] D. Russell and G.T. Gangemi, "Computer security basics," O'Reilly Media Incorporated, 1991.
- [17] T.L. Thomas, "Chinese and American network warfare," *Joint Force Quarterly*, vol. 38, pp. 76, 2005.
- [18] D. Turner, M. Fossi, E. Johson, T. Mack, J. Blackbird, S. Entwisle, M.K. Low, D. McKinney and C. Wueest, "Symantec Global Internet Security Threat Report," Symantec, Tech. Rep. Volume XIII, 2008.
- [19] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Tech. Rep. 119, pp. 1-12, 2004.

Proceedings of ISSA 2009

# **A SURVEY OF COMPUTER CRIME AND SECURITY IN SOUTH AFRICA**

**A. Stander, A. Dunnet, J. Rizzo**

Dept Information Systems, University of Cape Town

Adrie.Stander@uct.ac.za, petitqul@gmail.com, jackalza@gmail.com

## **1 INTRODUCTION**

Computer crime has escalated considerably over recent years and has become a very serious problem that costs governments, organisations and general computer user's significant losses annually. The Internet provides endless connectivity to billions of users around the world which has greatly influenced the flow of information. As revolutionary as this has been, the associated benefits have extended to the criminal world and allowed these miscreants to take advantage of this powerful tool to commit a host of computer crimes (Jones, 2007). Organisations relying on the Internet for daily business processes face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack (Householder, Houle & Dougherty, 2002). Moreover, it has become apparent that technology and the law do not seem to go hand in hand, and instead, are grappling to find common ground (Jones, 2007).

As national computer crime statistics do not exist, the purpose of this empirical research is to produce the first South African survey on computer crime and security. By analysing the results of the national survey, a better understanding of the extent to which South African organisations are aware of and affected by computer crime can be determined. The results will also indicate the adequacy of current organisational resources, policies and procedures. South Africa's current position will be evaluated in comparison with Australia and the United States of America. Ultimately, the research aims to serve as justification for further investment in computer security technologies, as well as the

Proceedings of ISSA 2009

creation of or improved adherence to computer and information security policies and procedures.

## 2 TRENDS IN COMPUTER AND INFORMATION SECURITY

The Australian Computer Crime and Security Survey (2006) indicated that more than 90 percent of all respondents used anti-spam filters, anti-virus software, firewalls and access control technologies, which is consistent with results over the past four years. The British Chambers of Commerce Crime Survey (2008) found that approximately four-fifths of their respondents use anti-virus software and 77 percent use anti-spam filters to help combat computer crime.

Network-based attacks have been somewhat limited by the introduction of default firewalls in popular operating systems such as Microsoft Windows XP, as well as an increasing awareness of computer security threats and practices among organisations and general Internet users. As a result, network-based attacks have declined by a small percentage (Symantec Internet security threat report, 2008).

The SIEM (Security Information and Event Management) market is one of the fastest growing security markets, with a growth rate of more than 30 percent in 2007 and estimated revenue reaching more than \$800 million in 2007 (Kavanagh & Nicolette, 2008).

The Australian Computer Crime and Security Survey (2006) indicated that almost half their respondents still do not use or follow security standards. In 2005, research indicated that more than 1300 organisations have been certified under the ISO/IEC 17799 standard and many more were in the process, making the standard the most prominent standard for IS security management (Theoharidou et al., 2005).

The British Chambers of Commerce Crime Survey (2008) found that larger organisations, typically those with more than 50 staff and turnover of £1 million or more, appear to have greater resources to be able to deal with computer crime related incidents. A majority of these organisations had formal written security plans (British Chambers of Commerce, 2008).

## A Survey of Computer Crime and Security in South Africa

The CSI 2007 Computer Crime and Security Survey found that most respondents spent between 3 to 5 percent of their IT budget on security and only 9 percent of respondents spent more than 10 percent (Richardson, 2007).

### **3 METHODOLOGY**

#### **3.1 Research Strategy**

Quantitative research in the form of a survey instrument has been used to collect the data and descriptive statistics have been used to analyse and present the data. The decision to follow a quantitative research methodology was based on the fact that the results of the survey should be a representative sample of the total population. Moreover, the nature of the data required, as well as the fact that comparisons have been drawn from similar research, meant that following a qualitative research methodology would have been inappropriate and ineffective.

#### **3.2 Research Questions**

Due to the exploratory nature of the research, research questions were derived from the literature. These questions provided a basis for the research in order to investigate possible relationships or trends with the eventual intention of discovering new theories.

##### **3.2.1 Questions**

What is the level of understanding of South African organisations with regard to the origins of computer crime?

- To what extent have South African organisations implemented and utilised the necessary resources, policies and procedures to effectively prevent and mitigate computer crime?
- What corporate policies and procedures regarding the reporting of computer crime exist within South African organisations?
- What are the perceptions of South African organisations regarding law enforcement's ability to combat computer crime?
- How are South African organisations affected by computer crime?

### **3.3 Sample and Respondents**

The primary target respondent was a working professional who was aware of the various computer crime and security issues within his/her organisation. Typically, these were senior managers, IT administrators, IS professionals, CIOs, as well as any IT security consultants.

Simple random sampling was the primary sampling method used when selecting the sample for this survey. The survey was distributed directly, through e-mail requests to specific organisations, as well as indirectly through a web based questionnaire linked to a well known South African IT news website.

Generally it was found that only people interested in this field of research responded to the survey. A total of 60 complete responses were collected, the majority (66%) of which came from organisations with more than a hundred employees. As similar techniques were used to collect data in the Australian and United State's surveys, this was seen as representative enough to compare the local survey to those surveys. The survey went live on May 31, 2008 and was closed on August 12, 2008.

## **4 RESULTS AND FINDINGS**

### **4.1 Who We Asked**

Survey respondents represent a broad range of industry sectors which include organisations from both the public and private sectors. Over 14 different industry sectors are represented. The industries with the greatest representation are the Information Technology sector (33 percent); the financial sector (18 percent); and the national or provincial government sector (15 percent). In terms of employee numbers and gross annual income/expenditure, most respondents that completed the survey belong to small to medium-sized organisations.

Respondents were grouped by job description. Twenty percent of respondents were senior executives with the titles chief executive officer (CEO) (10 percent), chief information officer (CIO) (8 percent), chief security officer (CSO) (2 percent) or chief information security officer (CISO) (5 percent). The single largest category of respondents (13 percent) had the job title of security officer. An additional 12 percent of

## A Survey of Computer Crime and Security in South Africa

respondents had the title of systems administrator, 7 percent of respondents had the title of IT support, while 43 percent had various other titles

### **4.2 Readiness to Protect**

This national survey cannot measure organisations' readiness to protect their IT systems merely based on responses to a few questions about the use of security technologies, policies and procedures, IT security standards and the level of training and education of personnel responsible for managing these systems. It does, however, seek to raise awareness about some of the essential elements which may contribute to an organisation's security posture and readiness to protect their systems.

### **4.3 Security technologies used**

Respondents were asked to identify the types of security technology used by their organisations. Nearly all respondents reported the use of anti-virus software (98 percent), logins and passwords (97 percent), and firewalls (93 percent). The USA and Australian respondents matched the SA result of 98 percent for anti-virus software, yet exceeded reported usage of firewalls with 97 percent and 98 percent, respectively. In contrast, there was a significant difference in the usage of logins and passwords between SA and the two countries. Furthermore, Australian organisations place much more emphasis on access control (90 percent) compared to South Africa (57 percent). Other noticeable differences between the three countries include the reported usage vulnerability management technologies, as well as the fact that SA organisations reported the highest usage of biometrics.

### **4.4 Security evaluation**

Although organisations are implementing various security technologies, it is important to note whether or not they are verifying that these security technologies are properly in place and effective on an ongoing basis. Fifty-three percent of SA respondents and 63 percent of USA respondents reported that their organisations perform security audits conducted by their internal staff, making security audits the most popular technique in the evaluation of the effectiveness of information security. The SA percentage for each technique is less than that of the USA, with the exception of e-mail monitoring software. The use of other techniques, such as automated

tools and Web activity monitoring software, are clearly also prevalent. Regarding security audits by external organisations and penetration testing by internal staff, the USA results exceeded the SA results by 20 percent and 26 percent, respectively.

#### **4.5 Computer security policies and standards used**

Among the four Readiness to Protect factors (technologies, policies, standards and training) the most significant in terms of lack of adherence, is the proportion of organisations that use or follow various IT security related standards. There was a considerable difference between the responses of SA and Australia. SA reported a 68 percent adherence or usage of IT security related standards, with 32 percent of respondents indicating the usage of ISO/IEC 17799 standard

#### **4.6 Spending**

Respondents were asked whether their organisation has increased expenditure on computer security in the last 12 months as a result of concerns about the adequacy of computer security within their organisation. Fifty-seven percent of SA organisations increased their IT security spending in the last 12 months for these reasons, compared to 50 percent of Australian organisations. However, this should not necessarily be interpreted as meaning that 43 percent of SA organisations were satisfied with their current IT security spending levels. Approximately 35 percent of SA respondents did not know what proportion of their organisational IT budget was allocated to IT security,

#### **4.7 Outsourcing**

Respondents were asked several questions pertaining to their IT security personnel, including the extent to which the computer security function of the organisation is outsourced. Fifty percent of SA organisations reported that their security function was not outsourced, as opposed to 61 percent of USA organisations.

#### **4.8 Training and Awareness**

Regarding training, qualifications and certifications of IT security personnel, respondents were questioned on each of these aspects. In the area of IT tertiary qualifications, SA reported 57 percent of their personnel had tertiary IT qualifications and 30 percent had no formal qualifications



## A Survey of Computer Crime and Security in South Africa

but more than 5 years IT security experience. Australia reported significantly higher numbers regarding vendor IT certification and ad hoc IT security courses.

Training staff adequately in IT security is an important part of the security agenda. Respondents were asked what percentage of the total IT budget their organisations allocate to awareness training where most SA and Australian respondents indicated this was less than 1 percent. While 30 percent of SA organisations reported that their organisations do not use awareness training and a further 22 percent do not measure the effectiveness of awareness training, many reported the use of volume and type of incidents or of help desk issues as indicators. Thirty-two percent of USA organisations reported the use of mandatory written or digital tests.

### **4.9 Computer Crime, Attack and Abuse Trends**

Respondents were asked whether they had experienced one or more electronic attacks in the last 12 months. Forty-five percent of SA organisations said “Yes”. Notably, the USA and SA responses were fairly similar, yet the Australian responses differed significantly. Respondents who indicated that they had experienced one or more electronic attacks in the last 12 months were then asked to report the approximate number of these electronic attacks. Most respondents for SA, the USA and Australia reported between 1 and 5 attacks within the last 12 months. Both SA and Australian respondents reported that more attacks came from the inside as opposed to the outside.

Respondents reported their opinions regarding suspected motives for electronic attacks that harmed the confidentiality, integrity or availability of network data or systems in the last 12 months. SA respondents reported foreign government political advantage (28 percent), illicit financial gain (25 percent) and indiscriminate random acts (22 percent) as the most common suspected motives. Australian respondents suspected that illicit financial gain (27 percent) was amongst the main motives, but reported personal grievance (31 personal) and other political interest (55 percent) as more common motives of electronic attacks.

Regarding the types of electronic attack, computer crime, or computer access misuse or abuse - SA, the USA and Australia responses were mostly similar. SA organisations were most able to detect computer

facilitated fraud (60 percent), whilst the USA and Australia mostly detected a degradation of network performance associated with heavy network scanning (59 percent and 62 percent respectively).

Respondents were also asked which of these types of electronic attacks, computer crime, or computer access misuse or abuse, caused their organisations financial loss in the past 12 months. Computer facilitated financial fraud was the main cause of financial loss for both SA (53 percent) and Australian (69 percent) organisations.

#### **4.10 Cost**

In order to approximate the cost of computer crime, respondents were asked to provide estimated Rand values that their organisations lost in total due to various types of electronic attack, computer crime, computer access misuse, or abuse within the last 12 months. Bearing in mind that these figures were rough guesses, losses estimated totalled R57.8 million. Of the total estimated loss, R50.1 million was due to unauthorised access to information by insiders. Theft of other computer hardware devices, telecommunications fraud, sabotage of data or networks, laptop theft, as well as DOS attacks, all had figures which exceed R1 million.

#### **4.11 Reporting Behaviours and Attitudes**

Beyond computer crime, attack and abuse trends, respondents were asked whether they shared information on these intrusions with law enforcement and legal counsel, who they reported these incidents to, and more generally, what, the outcome was when incidents were reported. Most SA (30 percent), USA (30 percent) and Australian (69 percent) organisations chose not to report one or more incidents to anyone outside their organisations, followed closely by reporting one or more incidents to a law enforcement agency. SA respondents also indicated the reporting of incidents to legal counsel for civil remedy (23 percent), as well as to their organisations' external auditor (17 percent).

When respondents were asked about the most important reasons why their organisation chose not to report computer crime, the results yielded a strong contrast of results between Australia and the other two countries. Most SA respondents reported that civil remedy seemed best (33 percent), or that they did not believe that law enforcement agencies were capable of apprehending the perpetrators (27 percent), or merely that the incident was

## A Survey of Computer Crime and Security in South Africa

not serious enough to report (27 percent). Similarly, most Australian respondents (76 percent) did not believe that law enforcement agencies were capable of apprehending the perpetrators, yet 74 percent indicated that negative publicity was also an important reason.

In cases where the electronic attacks or other forms of computer crime were reported, SA (25 percent) and Australian (49 percent) respondents stated that the crime was investigated but the lack of evidence prevented charges being laid. Only 15 percent of SA respondents and 19 percent of Australian respondents reported that the investigations resulted in a charge/charges being laid.

## 5 CONCLUSION

As a developing country, the national economy will become increasingly reliant on IT infrastructure and e-commerce for critical activities. Future growth may be hindered by the constantly evolving threat of computer crime, and thus it imperative that South African organisations are made aware of and become more knowledgeable of the origins and consequences of computer security issues, in the hope that further investment will be made into computer and information security for improvement. Moreover, those responsible for computer and information security should be able to justify new investments in new technologies and awareness training, as well as be able to understand the economic, financial, and risk management aspects of computer security. *Risk intelligent* organisations must be able to identify changes, threats or vulnerabilities in the landscape as they become visible.

## 6 REFERENCES

*Australian computer crime and security survey*. (2006). Retrieved April 4, 2008, from <http://www.auscert.org.au/images/ACCSS2006.pdf>

British Chambers of Commerce. (2008). *The invisible crime: A business crime survey*. Retrieved April 14, 2008, from <http://www.britishchambers.org.uk/6798219243143333651/crime.html>

Proceedings of ISSA 2009

- Campbell, K., Gordon, L.A., Loeb, M.P. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11(3), 431 – 446. Retrieved April 18, 2008, from SSRN database.
- Householder, A., Houle, K. & Dougherty, C. (2002). Computer attack trends challenge Internet security. *Computer*, 35(4), 5-7. Retrieved April 10, 2008, from IEEE database.
- Jones, B. R. (2007). Comment - virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law & Criminology*, 97(2), 601-629.
- Kavanagh, K. M. & Nicolette, M. (2008). *Magic quadrant for security information and event management*. Gartner RAS Core Research Note G00156945.
- Richardson, R. (2007). *CSI computer crime and security survey*. Retrieved March 29, 2008, from [http://www.gocsi.com/forms/fbi/csi\\_fbi\\_survey.jhtml](http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml)
- Symantec Internet security threat report*. (2007). Retrieved March 31, 2008, from [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/ent-whitepaper\\_internet\\_security\\_threat\\_report\\_xii\\_09\\_2007.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf)
- Taylor, M., Haggerty, J. & Gresty, D. (2007). The legal aspects of corporate computer forensic investigations. *Computer Law & Security Report*, 23(6), 562 – 566. Retrieved April 18, 2008, from ScienceDirect database.
- Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472-484. Retrieved March 29, 2008, from ScienceDirect database.

Evaluating Information Security Controls Applied By  
Service-Oriented Architecture Governance Frameworks

**EVALUATING INFORMATION SECURITY CONTROLS  
APPLIED BY SERVICE-ORIENTED ARCHITECTURE  
GOVERNANCE FRAMEWORKS**

**Jacqui Chetty<sup>1</sup> and Marijke Coetzee<sup>2</sup>**

<sup>1</sup>Department of Business Information Technology

<sup>2</sup>The Academy for Information Technology

University of Johannesburg

<sup>1</sup>[jacquic@uj.ac.za](mailto:jacquic@uj.ac.za)  
(011) 559 1177

<sup>2</sup>[marijkec@uj.ac.za](mailto:marijkec@uj.ac.za)  
(011) 559 2907

## ABSTRACT

Ensuring a secure Service-Oriented Architecture implementation within an organisation is challenging. Without sound information security principles supporting a Service-Oriented Architecture implementation, the rate of success is low. The information security principles of identification, authentication, authorization, confidentiality, integrity, availability and accountability remain the same for Service-Oriented Architectures. However, the Service-Oriented Architecture environment consists of agile implementations, which are designed around principles that demand a different approach that can be to the detriment of information security. Unless all information security issues related specifically to Service-Oriented Architecture are taken into consideration, an organisation faces unnecessary risks. An organisation faced with these added challenges may choose to avoid confronting this architectural approach altogether. Regrettably, an organisation could also miss out on the advantages and potential value that a Service-Oriented Architecture has to offer.

In order to identify information security shortcomings regarding Service-Oriented Architecture governance frameworks, this paper evaluates two existing Service-Oriented Architecture governance frameworks against ISO/IEC 17799 (2005) controls. The paper presents an analysis and evaluation regarding the state of governance of information security for Service-Oriented Architectures, to assist managers on how this complex issue should be approached.

## KEY WORDS

Information security, Service-Oriented Architecture, governance

# **EVALUATING INFORMATION SECURITY CONTROLS APPLIED BY SERVICE-ORIENTED ARCHITECTURE GOVERNANCE FRAMEWORKS**

## **1. INTRODUCTION**

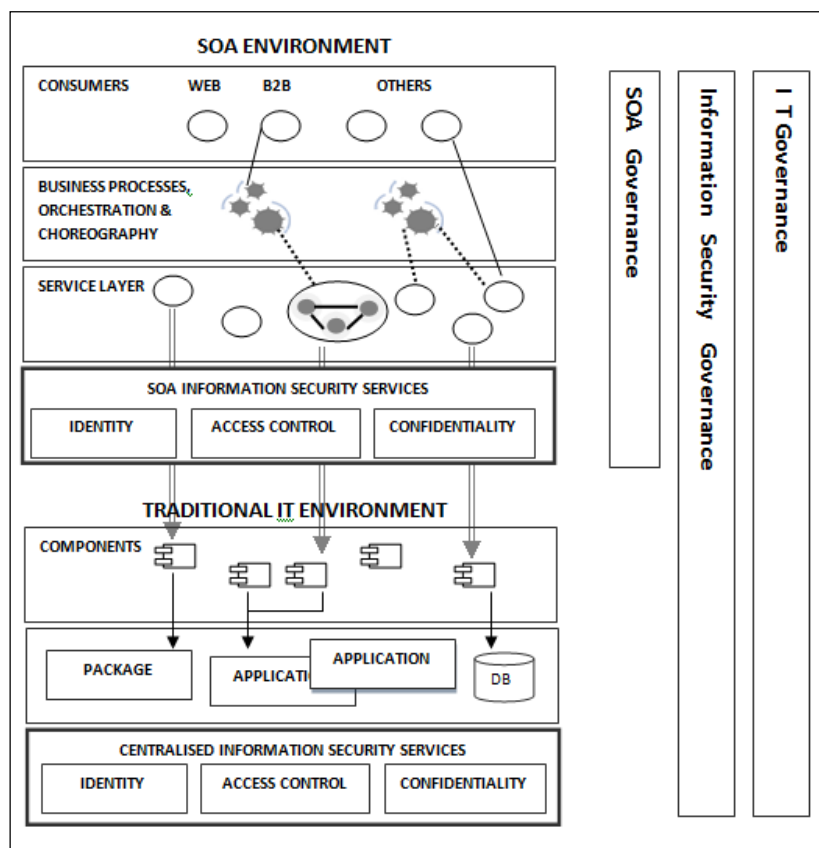
Service Oriented Architecture (SOA) (Brown, et al., 2006) is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains, and implemented using a variety of technology stacks. Although an SOA can be implemented using different technologies, web services (Champion, et al., 2002) is commonly used. Services can be shared and reused if design principles such as loose coupling, abstraction, discoverability, composition and the inclusion of a service contract are followed (Erl, 2006). Services implemented in this manner are vulnerable to information security threats, as they often expose the limitations of existing information security implementations (Buecker, et al., 2007).

SOA governance ensures that stakeholders define, implement and execute a business model and accountability framework for SOA. The main focus is to ensure that SOA policies are enforced by a policy enforcement model, which defines various policy enforcement mechanisms (Marks, 2008). Applying SOA governance in this manner may mean that information security controls are not comprehensively addressed.

The purpose of this paper is to evaluate whether existing SOA governance frameworks adequately address information security. Information security challenges for SOA are described in the following section. Section 3 evaluates two formal SOA governance frameworks. Section 4 describes ISO/IEC 17799 (2005) (ISO/IEC 17799, 2005) as a best practice for information security. Section 5 evaluates two SOA governance frameworks against ISO/IEC 17799 (2005), to illustrate which ISO/IEC 17799 (2005) controls are not adequately addressed in the frameworks. Section 6 concludes the paper.

## 2. SOA INFORMATION SECURITY CHALLENGES

Traditional IT environments are governed by IT and information security governance frameworks such as Cobit (IT Governance Institute, 2007) and ISO/IEC 17799 (2005), shown by layers on the right of Figure 1.



*Figure 1: Traditional IT and SOA environments*

Centralised information security services, shown at the bottom of Figure 1, protect this environment following a set of well-known best practises, defined by the IT and Information security governance layers. These controls



## Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks

are centralised, are characterised by human-to-machine interactions, have a fixed network perimeter to protect, address a singular information security context, and makes use of mechanisms of high assurance such as platform-dependent operating system access controls.

In contrast, an SOA environment consists of platform independent boundaries that are not fixed. Software components are exposed via service interfaces, as shown in Figure 1. Services can be composed or orchestrated into complex business processes and exposed to B2B transactions with remote partners. This complex environment needs another layer of governance, shown on the right of Figure 1, to cater for its complexity. Furthermore, service design principles such as loose coupling and composition have a detrimental effect on information security (Pulier & Taylor, 2006). Loosely coupled services do not form dependencies with other services or resources (Erl, 2008), regardless of context such as information security. Information security must be defined in a platform independent manner, to function unobtrusively to the service. The application of such security relies heavily on a policy infrastructure (Marks, 2008). When services are composed, the security context can only be determined at the time of composition. This increases the complexity of identification of service consumers, access control and accountability. Figure 1 indicates a new layer of SOA security services that make use of immature, emerging standards, are custom-built, complex, automated and policy-driven to cater for machine-to-machine interactions.

Figure 1 highlights the dilemma faced by management of SOA-enabled organisations. They may decide to govern the SOA and its security by using a SOA governance framework, as information security is generally addressed within such frameworks, and tool support is provided by vendors. Questions pertinent to address are whether SOA and information security governance frameworks are in alignment with one another? Do they function in a complementary manner to each other, or do they duplicate governance controls? Is all vital information security controls identified by these frameworks, or should new controls be identified? The following section describes SOA governance frameworks, emphasising information security.

### 3. SOA GOVERNANCE FRAMEWORKS

There is currently no standard framework that exists for SOA governance. The Generic SOA Governance Model by Niemann, Eckert and Steinmetz (Niemann, et al., 2008), referred to as NES here, has been defined by considering both vendor frameworks such as SAP AG (Brandt, 2009), Oracle (Hodgson, 2009) and IBM (Evans, 2009), and academic frameworks such as Marks/Bell (Marks & Bell, 2008) and Bieberstein, et al (2006). This framework, and the SOA Governance Reference Model by Marks (Marks, 2008) are chosen for the evaluation, due to their formal and comprehensive approach. Vendor-driven approaches are not considered, as they focus on technology and tool approaches. Table 1 describes the NES framework.

*Table 1: Generic SOA Governance Model –NES*

The model consists of two parts shown below:

- **The SOA Governance Control Cycle** – The cycle consists of four phases, namely planning, design, realisation and operation, providing a closed loop. Planning and design includes definition of policies and metrics. Realisation is where governance mechanisms such as metrics and policy enforcement are installed and processes are activated. Operation is where the SOA governance processes are evaluated and analysed for effectiveness. This ensures that the system complies with policies.
- **The SOA Governance Operational Model**
  - a. *SOA Center of Excellence (SCE)* defines and enforces guidelines and policies throughout the organisation. Information security is also considered here.
  - b. *Best Practices Catalog* stores all policy experiences, both positive and negative, to consistently improve an SOA.
  - c. *Policies* divide the policy-related topics into governance areas, including an area for information security-related policies which focuses on data and communication security, systems security and authentication and authorisation mechanisms.
  - d. *SOA Processes* defines the SOA system that needs to be governed, subject to governance policies.
  - e. *Metrics* are defined by the SCE and are applied to SOA Processes. Business, process, performance, SLA and SOA conformance metrics are defined, which correspond to specific policies like information security-related policies. The results of the metrics are fed back to the SCE for compliance.
  - f. *SOA Maturity Measurement* element describes how an SOA is adapting and operating within an organisation and contributes to monitoring policy effectiveness.

## Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks

The model uniquely considers governance of cross-organisational interaction on a technical level. Information security forms part of this framework but there is no separate, comprehensive element for information security.

Table 2 briefly highlights the MARKS model. This model is a very comprehensive, detailed model to provide a good structure for organisations that would like to implement an SOA governance framework.

*Table 2: SOA Governance Model - MARKS*

The layers of the model are grouped into four tiers. The tiers are Enterprise / Strategic Governance, SOA Operating Model Governance, SOA and Service Lifecycle Governance and Governance Enabling Technology. The Governance Enabling Technology tier applies across the other three, and is responsible for policy creation and policy enforcement, which includes information security policy control. This tier is described further, as it is the only one that addresses information security.

- **Governance Enabling Technology** – Policies are created and enforced using technology and tools across the services lifecycle. Policies should be monitored and managed to ensure that each policy is specific and that they can relate to one another. The use of policy automation through technology is encouraged. There are many tools and standards available to implement and enforce policies, namely registries, repositories, policy engines and distributed enforcement points. These tools interact with, amongst others, information security infrastructure. Implementing policy-driven SOA governance means adhering to web services standards.

This model identifies an important aspect of SOA governance, namely policy automation via technology support, to cater for agile machine-to-machine interactions. As it is very comprehensive, organisations must research it extensively before it is implemented.

The following section introduces a best practice for information security to evaluate each of these frameworks against.

#### **4. INFORMATION SECURITY BEST PRACTICE - ISO/IEC 17799**

Information security is achieved by implementing, amongst others, controls. For governance, control means to ensure that adequate measures are in place to provide assurance that objectives will be achieved and undesirable events will be prevented or detected and corrected (IT Governance Institute, 2007). Da Veiga and Eloff (2008) demonstrate that ISO/IEC 17799 (2005) addresses a comprehensive set of information security controls for governance. It is now chosen here as a baseline for the evaluation of information security of SOA governance frameworks. ISO/IEC 17799 (2005) controls are described in Table 3.

For a secure SOA, it would be imperative that these controls are comprehensively addressed. The next section evaluates the two mentioned SOA governance frameworks, with regards to information security.

#### **5. EVALUATING SOA GOVERNANCE FRAMEWORKS**

The evaluation is shown in Table 4. The first column lists ISO/IEC 17799 (2005) controls. NES and MARKS are evaluated against each control and either receives \* (not mentioned), √ (mentioned), √√√ (explicitly addressed) or ° (control should be addressed by the general information security governance of an organisation). A framework receives three ticks if it adheres to any of the following: security services are specifically mentioned, are defined as separate controls, controls are automated, or cross-organisational communication is considered.

Evaluating Information Security Controls Applied By  
Service-Oriented Architecture Governance Frameworks

*Table 3: ISO/IEC 17799 (2005) Controls*

<p><b>Security Policy</b> – An information security policy must be developed which reflects organisational objectives, management support and commitment.</p> <p><b>Organizing Information Security</b> – Management must establish a framework to initiate and control the implementation of information security. Information security must extend to external parties.</p> <p><b>Asset Management</b> – The organisational assets must receive an appropriate level of protection, an asset inventory list must be kept and ownership of assets must be classified and documented.</p> <p><b>Human Resources Security</b> – All parties, both internal and external must understand their responsibilities and roles, be aware of security threats and concerns, support the information policy and management information security must be applied throughout.</p> <p><b>Physical and Environmental Security</b> – To prevent unauthorised physical access, damage, theft and interference to organisational assets.</p> <p><b>Communications and Operations Management</b> – To ensure that the operational context is secure and to ensure that the appropriate level of information security is applied to third parties. To maintain adequate levels of information security and ensure that information is exchanged in a secure manner. Systems must be monitored and information security events recorded.</p> <p><b>Access Control</b> – To control the access to information, authorisation of user access rights and to ensure that authorised users understand their responsibilities and are co-operative both internally and externally.</p> <p><b>Information Systems Acquisition, Development and Maintenance</b> – To maintain information security throughout the systems development lifecycle. To protect the confidentiality, authenticity and integrity of information through cryptographic means.</p> <p><b>Information Security Incident Management</b> – To ensure that information security weaknesses and events are highlighted in a timely manner.</p> <p><b>Business Continuity Management</b> – To ensure that interruptions to business activities can be handled appropriately and timely.</p> <p><b>Compliance</b> – To ensure that organisations comply with legal, organisational policies and standards.</p>
---

Table 4: Evaluating SOA Governance Models against ISO/IEC 17799 (2005)

ISO/IEC 17799 (2005) CLAUSE	NES	MARKS
Security Policy	√√√	√
Organizing Information Security - Internally - Externally	* √√√	* *
Asset Management	√√√	√√√
Human Resources Security	√√√	√√√
Physical and Environmental Security	o	o
Comm. and Operations Man - Oper. procedure and 3 <sup>rd</sup> party delivery - System Planning - Software protection	√√√ * o	√√√ * o
Access Control	√√√	√√√
Information Systems Acquisition, Development and Maintenance - Maintain information security throughout SDLC - Protect the confidentiality, authenticity and integrity using cryptographic means	* *	* √√√
Information Security Incident Management	√	√
Business Continuity Management	o	o
Compliance - Legally - Policies and standards - Effectiveness of auditing process is maximised	√ √ *	√ √ *

The table reveals that SOA governance does attempt to address information security controls, shown by the number of √√√s. The number of \*s and √s indicates that information security is not addressed holistically.

## Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks

A closer look reveals that:

- Information security is not addressed holistically, as there is no information security framework that specifically addresses how to initiate and control the implementation of information security across all layers of an organisation;
- Information security for external parties, which may be pertinent to secure cross-organisational interactions, is not always considered;
- Information security controls are not always applied across the systems development lifecycle;
- Not all security services such as encryption are explicitly mentioned;
- Considering the automated manner in which service interaction is performed, a concern is that auditing, which can validate the existence and persistence of SOA information security enforcement, is not comprehensively addressed.
- In line with the previous concern, auditable records of compliance that are automated does not form part of the frameworks;

Management and governance methodologies such as Cobit and ISO/IEC 17799 (2005), applied to the traditional IT environment as shown in Figure 1, are robust and mature. The evaluation of SOA governance frameworks with ISO/IEC 17799 (2005) is valuable as it indicates that SOA environments, rich with technology and having a different focus on application design and implementation, requires a different focus to how it is controlled. Generally, ISO/IEC 17799 (2005) does not address SOA or any other application development methodology directly. It does highlight that information security controls such as security policies, access controls and compliance to security policies are vital to SOA service delivery. The high level of complexity present in an SOA requires that its information security controls must address agile services that are policy driven; control dynamically changing security contexts; and have centrally controlled governance that is extensible and interoperable between domains. Principles like loose coupling, composition and discoverability, while attractive for business solutions, require stringent information security and governance.

Proceedings of ISSA 2009

The specific information security controls used in traditional IT environments do not cover these issues. It is important that the concepts and features of ISO/IEC 17799 (2005) controls are followed when specific information security controls are defined, to protect SOAs more comprehensively. The process of correlating SOA governance frameworks with ISO/IEC 17799 (2005) controls is a complex undertaking.

The following list provides some suggestions to enhance information security controls for SOA governance. It should be noted that this list is by no means complete.

- A separate, comprehensive SOA information security framework is needed to initiate and control the implementation of information security for services. This is to ensure that organisations do not overlook the complexity of information security that is embedded into an SOA governance framework.
- A Plan, Do, Act, Check (PDCA) model should be used to ensure a closed loop, SOA governance control cycle.
- A SOA governing body such as the SOA Centre of Excellence should include an information security committee, to liaise with that of the organisation to ensure that information security is addressed holistically, and that controls are not duplicated or left out.
- Cross-organisational Centres of Excellence are needed to ensure that cross-organisational cooperation is governed by information security policies, where possible.
- An automated policy framework is needed to control, enforce and monitor automated service interactions.
- The auditing of dynamically changing service interactions, to ensure that the information security policy is consistently being applied across all security contexts, is needed.



## Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks

- As services are machine-to-machine interactions, automated mechanisms, not requiring human intervention are needed to ensure that policy specification, enforcement and monitoring are effectively applied.
- The use of standards such as WS-Trust (Nadalin, et al., 2007), WS-Provisioning (Schwartz, 2006), WS-Policy (Bajaj, et al., 2006) and XACML (Moses, 2005) is imperative to ensure that web services-based information security services can be integrated across platforms.

From this list it is clear that current information security controls needs to be extended for the purpose of information security for SOA governance. Figure 1 shows this, as SOA governance, which includes an information security component, is defined over IT governance, and Information Security governance.

For example, a Cobit control such as DS5 “ensure systems security” is addressed by ISO/IEC 17799 (2005) controls such as the definition of formal access control policies. This control needs to be extended for SOA to the definition of machine-readable access control policies, to be used by SOA specific access control services. The difficult task facing an organisation is ensuring that these frameworks are aligned with each other. This can only be achieved if comprehensive information security architecture is developed. The following section provides a conclusion and future work.

## 6. CONCLUSION AND FUTURE WORK

Governance has made an impact on information security and organisations. Consequently, organisations need to relook their information security frameworks. SOAs are not immune to these developments. A governance standard such as ISO/IEC 17799 (2005) was used to evaluate the extent to which information security is addressed in SOA governance frameworks. It has been identified that information security is not holistically addressed for SOA governance frameworks and adequate controls are not in place. It is important that information security is integrated into such a framework and

Proceedings of ISSA 2009

forms part of all activities related to the framework. Future work will focus on evaluating other standards such as Cobit and ISO/IEC 27000, to develop a comprehensive information security model that can be embedded into SOA governance frameworks.

## 7. REFERENCES

Bajaj, S., Box, D., Chappell, D., Curbera, F., Daniels, G., Hallam-Baker, P., Hondo, M., Kaler, C., Langworthy, D., Nadalin, A., Nagaratnam, N., Prafullchandra, H., von Riegen, C., Roth, D., Schlimmer (Editor), J., Sharp, C., Shewchuk, J., Vedamuthu, A., Yalçinalp, U. & Orchard, D. (2006). *Web Services Policy 1.2 - Framework (WS-Policy)*. Available from: <http://www.w3.org/Submission/WS-Policy>. (Accessed 6 June 2008).

Beucker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S. & Readshaw, N. (2007), *Understanding SOA Security Design and Implementation IBM*. Redbooks

Bieberstein, N., Bose, S., Fiammante, M., Jones, K., Shah, R.: (2006) Service-Oriented Architecture (SOA) Compass - Business Value, Planning, and Enterprise Roadmap. IBM developerWorks

Brandt, N. (2009). *Bauer, Conergy, Infineon, Post, SAP AG: German Equity Preview*. Available from: <http://www.bloomberg.com/apps/news?pid=20601100&sid=a1RiMsNUcbtk&refer=germany>. (Accessed 12 April 2009).

Carter, S. (2007). *The new language of business: SOA and Web 2.0*. IBM Press.

Champion, M., Ferris, C., Newcomer, E. & Orchard, D. (Editors) (2002) *Web Services Architecture*. Available from: <http://www.w3.org/TR/2002/WD-ws-arch-20021114/>. (Accessed 24 March 2009).

Christensen, E., Curbera, F., Meredith, G. & Weerawarana, S. (2001). *Web Services Description Language (WSDL) Version 1.1*. Available from: <http://www.w3.org/TR/wsdl>. (Accessed 14 November 2007).

Da Veiga, A, & Eloff, J.H.P. (2007). *An Information Security Governance Framework*. Information Systems Management, 24:361-372

## Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks

- Eloff, J.H.P. & Eloff, M. (2005). *Integrated Information Security Architecture*, Computer Fraud and Security, 2005 (11), 10-16.
- Erl, T. (2006), *Service Oriented Architecture: Concepts, Technology, and Design*. New York: Prentice Hall
- Erl, T. (2008). *SOA Principles of Service Design*. Indiana:Prentice Hall
- Evans, B. (2009). *IBM CFO: We Had 62 Unix Competitive Displacements In Q1*. Available from: [http://www.informationweek.com/blog/main/archives/2009/04/ibm\\_cfo\\_we\\_had.htm](http://www.informationweek.com/blog/main/archives/2009/04/ibm_cfo_we_had.htm) . (Accessed 19 April 2009).
- Hodgson, J. (2009). *With Sun, Oracle May Be Serious About Hardware*. Available from: <http://online.wsj.com/article/BT-CO-20090427-714253.html>. (Accessed 27 March 2009).
- ISO/IEC 17799 (2005). Information technology. Security techniques. Code of practice for information security management, South Africa.
- IT Governance Institute. (2007). *Cobit 4.1*. Illinois: IT Governance Institute.
- Kanneganti, R. & Chodavarapu, P. (2006). *SOA Security in Action*. Manning (unedited draft)
- Marks, E.A. & Bell, M. (2006), *Service-oriented Architecture A Planning and Implementation Guide for Business and Technology*. Wiley
- Marks, Eric A. (2008), *Service-Oriented Architecture Governance for the Services Driven Enterprise*. Wiley
- Moses, T. (2005). *eXtensible Access Control Markup Language 3 (XACML) Version 2.0*. Available from : [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf). (Accessed 17 March 2009).
- Nadalin, A., Goodner, M., Gudgin, M., Barbir, A. & Granqvist, H. (Editors) (2007). *WS-Trust 1.3*. Available from: <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html>. (Accessed 12 February 2009).

Proceedings of ISSA 2009

Niemann, M. (2008). *Governance for Service-oriented Architectures: An Implementation Approach*. Available from: [http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-374/I-ESA2008\\_MichaelNiemann.pdf](http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-374/I-ESA2008_MichaelNiemann.pdf). (Accessed 5 January 2009).

Niemann, M., Eckert, J. & Steinmetz, R. (2008). *Towards a Generic Governance Model for Service-Oriented Architectures*. Available from: Americas Conference on Information Systems (AMCIS), AMCIS 2008 Proceedings, <http://aisel.aisnet.org/amcis2008/361>. (Accessed 4 February 2009).

Pulier, E. & Taylor, H. (2006). *Security in a Loosely Coupled SOA Environment*. Available from: [http://www.developer.com/design/print.php/10925\\_3605836\\_1](http://www.developer.com/design/print.php/10925_3605836_1). (Accessed 2 March 2009).

Rahaman, M. A., Schaad, A. & Rits, M. (2006). *Towards Secure SOAP Message Exchange in a SOA*. Available from: ACM 1-59593-546-0/06/0011

Schwartz, M. (2006). *Web Services Gets SPML 2.0 Boost*. Available from: <http://esj.com/articles/2006/05/02/web-services-gets-spml-20-boost.aspx>. (Accessed 8 April 2009).

SDA India (2008). *IT Audit and Information Security*. Available from: <http://iaudit.blogspot.com/2008/03/soa-mitigate-compliance-and-security.html> (Accessed 27 January 2009).

Von Solms, H. & Eloff, Jan H.P. (2004). *Information Security*. RAU

Von Solms, S.H. & Von Solms, (2006). *Information Security Governance*. Unpublished draft.

Weill, P. & Ross, J. (2004): *IT Governance*. Harvard Business School Press

Whitman M. E. & Mattord H. J. (2009). *Principles of Information Security*. Course Technology

Automated Firewall Rule Set Generation Through Passive Traffic Inspection

# AUTOMATED FIREWALL RULE SET GENERATION THROUGH PASSIVE TRAFFIC INSPECTION

Georg-Christian Pranschke<sup>1</sup>, Barry Irwin<sup>2</sup> and Richard Barnett<sup>3</sup>

Security and Networks Research Group  
Computer Science Department  
Rhodes University  
Grahamstown, South Africa

<sup>1</sup>g05p3292@campus.ru.ac.za, <sup>2</sup>b.irwin@ru.ac.za,  
<sup>3</sup>barnettrj@acm.org

## ABSTRACT

Introducing firewalls and other choke point controls in existing networks is often problematic, because in the majority of cases there is already production traffic in place that cannot be interrupted. This often necessitates the time consuming manual analysis of network traffic in order to ensure that when a new system is installed, there is no disruption to legitimate flows.

To improve upon this situation it is proposed that a system facilitating network traffic analysis and firewall rule set generation is developed. A high level overview of the implementation of the components of such a system is presented. The system makes use of a third party package, named *Firewall Builder* which provides firewall rule sets for a wide variety of firewalling solutions. Additions to the system are scoring metrics which may assist the administrator to optimise the rule sets for the most efficient matching of flows, based on traffic volume, frequency or packet count.

## KEY WORDS

firewall, choke point control, automatic configuration, network traffic analyser, pcap, netflow

# AUTOMATED FIREWALL RULE SET GENERATION THROUGH PASSIVE TRAFFIC INSPECTION

## 1 INTRODUCTION

In order for firewalls to serve their intended purpose, it is imperative that they are correctly configured. This is because each individual network setup is different and if the firewall is to become an integral part of a network's infrastructure it has to cater for the individual properties of the network it is deployed in. A misconfigured firewall will, almost certainly, only provide the illusion of network security [15]. While configuring host based firewalls and firewalling solutions protecting small networks and correctly documented networks may be a relatively straight forward task for an experienced network administrator, it does become a very much harder task when dealing with poorly documented legacy and organically developed networks.

This research is focused on the feasibility of automatically generating the configuration for a rule set generator called *Firewall Builder* [5], to further automate the process of configuring and deploying firewalling solutions.

The remainder of this paper is structured as follows. After a brief problem statement in section 2, in which we describe in what situations and setups the system is to be employed, we turn to a high level design overview of the proposed system in section 3. Each component of the components that make up the system is individually highlighted in sections 3.1, 3.2, 3.3 respectively. Section 3.4 deals with *Firewall Builder*, a third party product upon which the system relies. Section 4 describes possible future extensions to the system and section 5 concludes the paper.

## 2 PROBLEM STATEMENT

A firewall is rarely a single piece of hardware or software [12] and, therefore, combining the various technologies involved into a well configured firewalling solution is often a non trivial task in itself. The process of configuring and deploying a firewalling solution is further complicated when a firewall is to be introduced into a network segment that previously did not have any choke

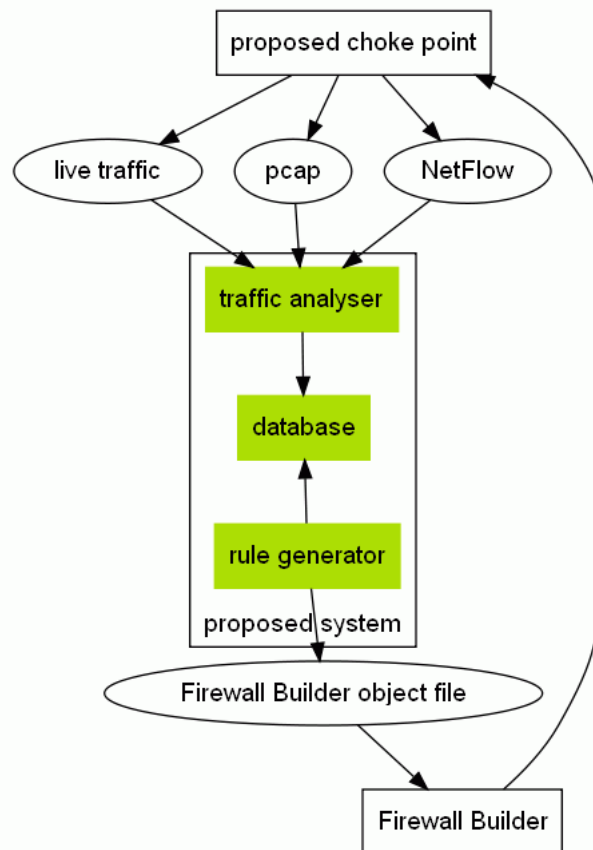
## Automated Firewall Rule Set Generation Through Passive Traffic Inspection

point controls. This is often the case in growing network infrastructures where it might be desirable to introduce choke point controls at a node that previously had no such system. Because the flows passing through the node might not be known to their full extent and because an unintended interruption of production traffic is surely undesirable, it is often necessary to inspect the traffic flows at the node manually and then to derive firewall policies for the particular firewalling solution proposed at the node. While there are many traffic analysers available, ranging from propriety commercial products, that cost up to 25,000 USD, to free and open source solutions [9]; that perform traffic flow analysis, there is no product that specifically caters for the configuration of firewalls.

### 3 PROPOSED SOLUTION

To alleviate this situation the authors are currently developing a system, which specifically aims to automate as much of the firewall configuration process as possible. This shall be achieved by firstly building upon automation solutions already available, specifically *Firewall Builder* [1], and secondly by taking a flow based traffic analysis approach utilising portions of Cisco's *NetFlow* format [9]. The system shall consist of two distinct modules, one for analysing the traffic at the proposed choke point and one for generating a rule set to match the observed traffic. The traffic analyser should be capable of analysing either live traffic at the node or trace files recorded at the node, in *pcap* [4] or *NetFlow* format.

The output of the traffic analysis shall be in a format similar to that of *NetFlow*, as this has a high information density, which is desirable for all consecutive steps in the configuration process. The resulting flows shall be stored in a database upon which the GUI-based rule generator can act. The rule generator shall then, in turn, propose a set of rules based on the observed flows and allow the administrator to review and refine these rules from within a GUI. The refined rules shall then be exported to a format understood by *Firewall Builder*, which is capable of deploying these rules to a wide variety of firewalling solutions. Thus *Firewall Builder* shall act as the backend of the configuration process. A graphical representation of how the components interact is given in figure 1. Because it is unusual for a dedicated firewall machine to have windowing capabilities, this modular approach enables the traffic analyser to run on these machines on the command line, whereas the rule generator can be run on a remote desktop machine.



*Figure 1: Overview of the high level design of the proposed system and its position in the configuration process.*

It is expected that this solution will speed up the process of configuring and deploying firewalls considerably because the administrator does not need to concern himself with a tedious manual traffic analysis, or the intrinsic details of writing firewall policies for a particular firewalling solution.

As most network infrastructures are inherently heterogeneous, the project puts a strong emphasis on cross platform portability and the use of free and open source tools and libraries.

### 3.1 Traffic Analyser

The traffic analyser's primary task is to create or extract traffic flows from its input data and to consequently store these flows in a database. Working with



## Automated Firewall Rule Set Generation Through Passive Traffic Inspection

flows is advantageous because of their high information density, and because they contain stateful information about the prevalent network connections. The three supported types of input data are *NetFlow* flow records, live traffic and *pcap* dump files.

### 3.1.1 NetFlow

NetFlow is both a format and a technology. Initially developed in-house at Cisco, it has quickly become the *de facto* standard for network analysis and is used for a variety of purposes including, but not limited to, billing, network planning, traffic engineering and the detection and analysis of security incidents [8, 9]. *NetFlow* enabled devices can export flow data via a UDP based protocol to a *NetFlow collector*, which then files, filters and stores the flow data. Ideally the traffic analyser should be capable of processing both the UDP exported flows and *NetFlow collector* files.

Flows are created by continuously analysing IP packets and categorizing them into IP flows. A packet is either categorized into an existing flow or creates a new flow. Finished or expired flows are then exported to the *NetFlow collector* via UDP. A flow is defined by seven key fields, namely, source IP, destination IP, source port, destination port, protocol, type of service and input interface. Any two packets sharing the same entries for all seven fields belong to the same flow [7]. There are several versions of *NetFlow*, some of which are more commonly used than others, namely versions 1, 5, 7, 8 and 9 that incrementally improve upon another and provide a richer feature set with more detailed flow records [8].

The traffic analyser only requires a subset of the information provided by *NetFlow* and shall extract the relevant bits for its operation into a custom flow format and discard the rest.

### 3.1.2 Live Traffic and *pcap* Trace Files

The traffic analyser uses *libpcap* [4, 11] (*WinPcap* [6] on Windows) to handle both, live traffic and *pcap* dump files. The processing of these two types of input is nearly identical. The strategy to obtain the same custom flows that are extracted from *NetFlow*, is to screen the packet data for three way handshakes and TCP FIN and RST packets.

The ACK packets involved in the three way handshake can be determined through the packets' sequence numbers [14]. This establishes the sources and destinations and hence the direction of the traffic flows. The difference in the timestamps between these packets allows for an estimation of the duration of any given connection. The packets that are neither SYN nor FIN are matched to one of the existing flows and their payloads added to the total volume of traffic in the flow. Their occurrence is also recorded in the packet count of the flow. Because packets might arrive out of order, care must be taken when reconstructing the flows to not disregard valuable information, meaning that non SYN or FIN packets without a corresponding flow do create their own flow so that it is possible to reconstruct them later or at least take them into consideration when generating the rules at a later stage.

The flow information is then stored in a database for later analysis by the rule generator. The database table that records the traffic flows should feature fields for a flow identifier number, the flows type of service, the timestamp of the SYN - ACK packet, the timestamp of the FIN - ACK packet, the total packet count in the flow, the total volume of traffic transferred in the flow so far, the flows source address and port and the flows destination address and port.

### 3.2 Database

Currently the project uses the embedded SQL database engine *SQLite* [3, 13] to record the flows, which has various advantages over other more sophisticated database solutions. From a performance perspective, this in-process library is simply much faster than any networked database solutions could ever be. Because *SQLite* is serverless, self-contained and requires no configuration it also increases the ease of use of the system. *SQLite* stores its databases in a file, in a format that is consistent across all platforms, thus its database files lend themselves as the perfect format for information exchange between the traffic analyser and the rule generator, especially across different platforms [13, 3]. An added advantage is that the database files can be efficiently compressed and are therefore ideal to be sent across the network.

### 3.3 Rule Generator

The rule generator then uses the database file to propose matching firewall rule sets. The user interface of the rule generator shall provide an integrated terminal so that the user does not have to leave the GUI to start and control

## Automated Firewall Rule Set Generation Through Passive Traffic Inspection

the traffic analyser on the remote site. A facility to perform custom SQL queries against the database shall also be provided. The flows recorded in the database shall be visualized in a table like structure for close inspection by the user. The security policies are visible in another tab and all changes made from anywhere within the system should be immediately reflected here. At the end of the review and refinement process the user should be able to export the policies into a *Firewall Builder* network object file or alternatively invoke one of *Firewall Builder's* policy compilers directly.

The basic strategy to automatically generate a rule set is to divide the network into an 'inside the wall' and an 'outside the wall' part. Initially both sides start off with the least possible privileges (deny all). Then all incoming flows targeted at commonly known services are permitted. Flows targeting high port numbers are only allowed as a response to outgoing flows. The presence of services that are commonly considered outdated such as Telnet is pointed out to the user and a suggestion for their replacement made. This quite lax basic configuration can then be refined by the administrator by either individually allowing or denying flows or by specifying wildcards on IP, protocol or port level.

By default ICMP rules will be generated from a template. The user can then activate or deactivate the desired subtypes. A facility for reverse DNS lookup shall be provided, so that unwanted sites can be blocked at the discretion of the user.

### 3.4 Firewall Builder

Firewall Builder is a GUI-based firewall configuration and management tool that supports *iptables* (netfilter), *ipfilter*, *pf*, *ipfw*, *Cisco PIX* (FWSM, ASA) and *Cisco routers extended access lists* [1]. It features a set of policy compilers that compile the rule sets created from within its GUI, from xml based object files, into, firewalling solution specific, firewall rule sets. The policy compilers do also create automatic deployment scripts, that allow the firewall to be brought up remotely and to roll back the installation if necessary. *Firewall Builder* also ensures that the SSH connection between the configuring host and the firewall will never accidentally be interrupted. Because Firewall Builder's GUI is built upon *Qt* [2, 10] it is capable of running on a wide variety of target platforms, such as Linux, FreeBSD, OpenBSD, Mac OS X and Windows [5]. All of the above mentioned features make *Firewall Builder* the ideal backend for the project.

## 4 POSSIBLE FUTURE EXTENSIONS

Since the proposed system is considered a proof of concept, most future extensions considered at this time are related to adding features that will make it a stable production release. A very obvious one is adding IPv6 support, which should be relatively straight forward. Furthermore the traffic analyser could be extended to generate additional scoring metrics that can help to further optimize the generated rule sets. The inclusion of an intrusion detection and prevention system such as *snort* and in turn its automatic configuration and deployment would certainly result in a more powerful and complete firewalling solution. At a later stage, the option of customizing and integrating *Firewall Builder's* policy compilers into the rule generator might prove desirable, to increase ease of use and lessen the dependency on this third party package.

## 5 CONCLUSION

Although this research is still at a very early stage, it is anticipated that the approach of automatic firewall rule set generation by means of passive traffic inspection will prove feasible and that a working prototype can be developed within the given timeframe. It is hoped that the proposed system will not only be quicker and more convenient than manual configuration, but possibly prove to be more accurate and allow for faster turnaround in the deployment of new firewalling solutions. This should result in decreased risk and cost for organisations deploying such solutions.

## ACKNOWLEDGEMENT

The authors would like to acknowledge the support by Telkom SA, Comverse, Tellabs, Stortech, Mars Technologies, Amatole Telecommunication Services, Bright Ideas Project 39, THRIP and the NRF through the Telkom Centre of Excellence in the Department of Computer Science at Rhodes University.

## References

- [1] Firewall builder cookbook. Online: <http://www.fwbuilder.org/guides/>.

## Automated Firewall Rule Set Generation Through Passive Traffic Inspection

- [2] Qt - a cross-platform application and ui framework. Online: <http://www.qtsoftware.com>.
- [3] Sqlite. Online: <http://www.sqlite.org>.
- [4] Tcpdump/libpcap public repository. Online: <http://www.tcpdump.org>.
- [5] What is firewall builder. Online: <http://fwbuilder.org/about.html>.
- [6] Winpcap: The windows packet capture library. Online: <http://winpcap.org>.
- [7] Cisco ios ipsec accounting with cisco ios netflow. Tech. rep., Cisco Systems, 2004.
- [8] Cisco cns netflow collection engine user guide, 5.0.3. Tech. rep., Cisco Systems, 2005.
- [9] Introduction to cisco ios netflow - a technical overview. Tech. rep., Cisco Systems, 2007.
- [10] BLANCHETTE, J., AND SUMMERFIELD, M. *C++ GUI Programming with Qt 4*. Prentice Hall, 2006.
- [11] GARCIA, L. M. Programming with libpcap - sniffing the network from our own application. *hackin9 3* (2008), 39.
- [12] OGLETREE, T. *practical firewalls*. Que, 2000.
- [13] OWENS, M. *The Definitive Guide to SQLite*. Apress, 2006.
- [14] SIYAN, K. S., AND PARKER, T. *TCP Unleashed*. SAMS Publishing, 2002.
- [15] ZWICKY, E. D., COOPER, S., AND CHAPMAN, D. B. *Building Internet Firewalls*. O'Reilly, 2000.

Proceedings of ISSA 2009

## **PHISHING: HOW AN ORGANISATION CAN PROTECT ITSELF**

**Edwin Donald Frauenstein<sup>1</sup> and Rossouw von Solms<sup>2</sup>**

<sup>1,2</sup>Nelson Mandela Metropolitan University, South Africa

<sup>1</sup>efrauenstein@wsu.ac.za, (+27)72 144 2751, East London, 5247

<sup>2</sup>rossouw@nmmu.ac.za, (+27)41 5043669, PO Box 77000, Port Elizabeth,  
6000

### **ABSTRACT**

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to address all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. Most research in this area has shown that only certain dimensions used to combat phishing attacks, in an organization, are addressed in isolation and not holistically. Anti-phishing research literature studied has either focused on algorithms for detecting phishing attacks in web browsers (Egelman, 2008; Fette, 2007; Garera, 2007; Patel, 2007) or on evaluating the user interfaces of anti-phishing web browser toolbars (Wu, 2006). From research studied, there has been little work conducted on preventing users from falling for phishing email messages. It has been proven that phishing does indeed pose an ongoing threat to an organization through its employees. Therefore, a suitable solution to this problem should be devised. This paper attempts to present such a holistic solution in the form of a model.

### **KEY WORDS**

Phishing, social engineering, information security model, e-mail scams, spoof-websites

# **PHISHING: HOW AN ORGANIZATION CAN PROTECT ITSELF**

## **1 INTRODUCTION**

Information in the modern electronic world can be viewed as the most important asset in a global market. Individuals, businesses, organizations and governments depend on information to be embedded in secure, private and trustworthy IT infrastructures ([http://www.thedacs.com/techs/enhanced\\_life\\_cycles/](http://www.thedacs.com/techs/enhanced_life_cycles/)). Individuals within an organizational environment often tend to rely on an organization to take responsibility and have these well defined controls to protect the integrity and availability (ICT Standards Board, 2007) of their personal data from unauthorized access, use, disclosure, disruption, modification or destruction (IBM Business Consulting Services, 2006). However, these controls alone cannot avert information security threats. An alternative technique of gaining unauthorized access of information, apart from the common procedure of hacking, is *Phishing*.

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to include all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. This paper also addresses, from research studied, the problems that phishing poses to individuals and organizations (Orgill, 2004).

## **2 BACKGROUND TO THE PROBLEM OF PHISHING**

There is much evidence in literature that proves that phishing is a growing problem in the current global industry and poses an ongoing threat that may affect every individual in an organization (Ohaya, 2006; Orgill, 2004; Safecode, 2008; Threat Insight Quarterly, 2005). Phishing is a social engineering technique through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity (Kumaraguru, 2007). Today, phishing has become much more sophisticated in techniques using technology, advantageously,



## Phishing: How an Organisation can Protect Itself

as a tool through a combination of spoofed emails, Internet Relay Chat (IRC) and instant messengers (IM's) to lure individuals (Ohaya, 2006).

Since most organizations are conducting business transactions through the Internet, Information Technology is rapidly changing the world through information and communication technology (Alkadi, 2004). Today most communication occurs through electronic mail. According to Badra (2007), there are many various forms of phishing attacks however, common phishing schemes mostly use spoofed e-mails to lure users to fake websites designed to capture their confidential information (Ohaya, 2006). The spoofed- email normally tends to have a slightly threatening message or tone to increase the effectiveness of luring the victim to avoid any further consequence. An example of this technique could be that the user's bank account details would be terminated if they fail to respond to the email. Phishing is not only based on obtaining user account details, but includes access to all personal and financial data. When individuals respond to such messages, they are putting themselves and their respective organizations at risk. This is caused primarily due to a lack of knowledge in information security protocols and carelessness regarding the consequences which may follow.

Recently, social attraction networks (e.g. MySpace, Facebook and Friendster) have gained popularity in phishing attacks (Brown, 2008; Unisys, 2008) and are being used as sources to lure individuals to give out their personal information. The latter substantiates the point that threats are constantly finding new weaknesses in technology and using more sophisticated techniques to gain entry through this modern, technological age (Orgill, 2004). Since people can be considered to be the weakest link in a very technologically secure computing environment (according to current standards), they are consequently targeted by social engineering attacks (Orgill, 2004). Much emphasis is placed on making computer systems more secure (technology aspect) and thus, the human element is often forgotten, ignored or neglected. Each new threat adds to the difficulty of securing an information system. The attacker does not have to have any prior knowledge into hacking systems, but rather understanding the use social engineering techniques. Human emotion and manipulation are used to trick victims into giving up personal information. The social engineer attempts to exploit the natural desires of humans to trust others and strangers, to assist in other's labours and to gain favour in their eyes

(Orgill, 2004). PayPal, eBay, American Online (AOL) and the South African Revenue Services (SARS) (<http://www.sars.gov.za/home.asp?pid=42736>) are well known examples of organizations that have all claimed victim to having been financially affected by phishing attacks

People and organizations, especially in a South African context, may not be aware of the dangers that phishing poses or how to detect these threats. This is indeed the case, even though much literary sources educate users on how to effectively identify these threats (Fette, 2007; Garera, 2007; Patel, 2007). People seem too dependant on IT systems to manage security concerns. This lack in responsibility exposes this weakest link, the human factor (Orgill, 2004; Patrick, 2005; Robila, 2006).

### **3 CURRENT PROTECTION MEASURES IN ORGANIZATIONS**

Organizations can effectively manage and protect their information from unauthorized access, by following the internationally accepted and recognized Code of Practice for Information Security Management i.e. ISO 27002 (<http://www.iso27001security.com/html/27002.html>). This international standard is but one ‘best practice’ approach that provides recommendations of what companies should implement to protect their information assets. The standard also addresses many issues and concerns relating to information security. Applying only an international standard may not be adequate enough as even these generally accepted Information Security (IS) standards and best practices do not effectively address the Social Engineering aspect of Information Security and may leave gaps for phishing attacks. The document does not particularly focus/emphasis on the term “phishing” attacks but does indeed mention that it is currently a problem. It rather gives general guidelines that one shouldn’t exchange information with unknown parties or open emails from unknown sources etc. The illusion that emails appear to be from a legitimate source is what allows phishing attacks to be so effective. The email seems relevant in context and seems legitimate, in design, to the individual (Egelman, 2008). The latter is regarded as a spear phishing attack (Microsoft, 2005). Therefore, spear phishing attacks have the potential to pass through strong company regulations and seemingly secure technology controls, relying mostly on the human element for protection (Orgill, 2004).

## Phishing: How an Organisation can Protect Itself

There are many reasons why individuals fall susceptible to phishing attacks. According to Ohaya (2006) some of the reasons include a lack of knowledge of computer systems, lack of security and security indicators, lack of attention to the security indicators, lack of attention to the absence of security indicators, and the sophistication of spoofed sites seem to be the greatest threat. If the site looks authentic, users have confidence in it as they could not tell the difference between a genuine or spoofed web-site. Ohaya (2006) states further that security managers should take the following steps to protect the organization and employees from phishing attacks:

1. “Ensure privacy and security are perceived at a macro level in the organization.
2. Create security policies, standards, and procedures that are part of an ongoing overall security management framework
3. Ensure that all employees in the organization have security education, training and awareness about phishing and other threats in addition to following security policies and procedures.”

Orgill (2004) substantiates this in stating that employee education should cover the company’s strong policy statements, including penalties for non-compliance. In fact, researchers (Ohaya, 2006; Orgill, 2004; Robila, 2006) have shown that user education is the most important aspect of preventing phishing attacks. Kumaraguru (2007) designed and evaluated an embedded training email system that teaches people the dangers of phishing during their normal use of email as he feels that people simply ignore security notices and warnings. Sheng (2007) developed a game that teaches people not to fall for phishing, thus getting them more interested in the fun educational aspect. According to Badra (2007), reducing the phishing threat can be achieved if a given solution could meet the following functions: monitoring potentially malicious activity, authenticating email messages, detecting unauthorized use of trademarks or logos or other proprietary imagery, improving the security patching infrastructure to increase resistance to malware, using personalized information to authenticate an email directly to a user and detecting a fraudulent web site and alerting the user.

According to O'Brien (2000) there are 3 major types of controls that must be developed to ensure the quality and security of information systems

- **Information System controls** (input, processing, output and storage controls)
- **Procedural Controls** (standard procedures, documentation, authorization requirements, auditing)
- **Facility Controls** (physical protection, computer failure controls, network security and biometric controls).

These above-mentioned controls merely focus on the management aspect of the information system in relation to normal everyday conditions of business transactions, specifically the input, processing, output and storage activities in an information system. This approach focuses more on the technological and organizational measures in place rather than an unforeseen human error. It does not encompass provisions for the idiosyncratic nature of the human element, especially within a social context. Phishing has few technical boundaries. Its strength lies in its ability to trick any individual irrespective of experience, knowledge or position in the organization. This method of acquiring sensitive information from the individual could then lead to the entire organization's confidentiality or individual's personal information being put at risk.

While technology is important, organizational and human factors also play a crucial role in achieving information security (Dutta, 2008). These dimensions should play a role in constructing a holistic approach to protect information assets against phishing attacks. The *technological* dimensions would typically involve anti-phishing software, spam filters, firewall etc. The *human* dimension calls for effective awareness and education to assist in strengthening the 'human firewall' and to ideally cultivate a culture of information security behaviour. On the other hand, sound *organizational* measures, e.g. policies and procedures, need to be in place to put everything into perspective. Of these dimensions, the human factor is probably the most important since this is the area that phishing exposes the most. Research suggests that if human behavioural response can be understood, then one may have a solution to the issue of why people fall susceptible to phishing attacks (Downs, 2007). Information

## Phishing: How an Organisation can Protect Itself

Security should not be regarded as a technical issue but rather a multi-dimensional issue. Therefore is a need for all of these dimensions to be considered. In doing so, this should provide for adequate overall risk mitigation against phishing attacks.

Below are the main components which will be addressed in the model and recommendations for each of these components:

**International Standards, Guidelines and Best Practices:** As mentioned, numerous international standards, best practices and guidelines refer to the effective protection of information assets, e.g. ISO 27002 (<http://www.iso27001security.com/html/27002.html>), COBIT (COBIT, 2000), the King II Report (King Report, 2001), etc. Such standards, best practices and guidelines should play an integral role in the eventual plan to protect organizational information assets against phishing attacks.

**Technology controls:** As earlier discussed in this paper, threats are finding new weaknesses in technology. Therefore it is considered a dimension that compromises the integrity of an organization's information security. It is important to address its role in the model. Phishing attacks can breach a weak technological barrier. The "phisher" may rely on the individual or organization to have an outdated or ineffective web browser, outdated anti-virus program due to poor organization policies. The phisher may lure individuals through websites like Facebook, Twitter etc. The use of IRC and Instant messengers are a new breeding ground for phishing attacks. Most organizations should have anti-virus programs installed. However, an effective anti-virus program is only as good as the currency of its virus definition updates that it receives. Besides its primary function of scanning for virus signatures, some anti-virus programs can also detect most phishing websites (<http://anti-virus-tools.software.informer.com/>). The anti-virus program can also remove key-logger Trojans- a virus designed by 'phishers' to monitor keystrokes from the keyboard.

Organizations use firewalls, in a network environment, to filter incoming emails as well as to block unauthorized entry from outsiders. If properly defined through procedures, the firewall also prevents employees from accessing illegal or unwanted websites, in this regard phishing websites.

Proceedings of ISSA 2009

(<http://www.security-forums.com/viewtopic.php?p=5787&id=db1bca5dcddd4bff05dd056501b7e922>).

The internet web browser also forms an important role, in security, in having the built-in capacity to identify spoofed websites. Common web browsers such as Microsoft Internet Explorer 7, Opera 9.5, Firefox 3, and Safari 3.2 etc. can detect most phishing websites. However, each reacts differently to suspicious spoofed-websites in the manner it displays active phishing warnings to the user (Egelman, 2008). This presents a problem in the sense that it may confuse the individual when presented with such a warning. An organizational standard should be set as to identify which browser would best be suited in such a case of an individual falling susceptible to a phishing website.

The operating system (e.g. Windows XP, Windows Vista, etc.) should be regularly updated for software enhancements (updates, patches, hot-fixes etc.) either automatically or by relevant staff. Failure to do so creates an opportunity for viruses to either pose as an application or as a warning notification thus luring the victim to submit confidential information. The latter is another technique of phishing that acquires personal information (<http://computing.vassar.edu/safecomputing/security/ospatch.html>). Phishing attacks can also be in the form of malicious code-based or Trojan-based attacks, in which malicious software causes data compromises (Badra, 2007)

Technological aspects form an imperative part in the eventual protection model against phishing attacks. Clear guidelines need to be provided as to which controls should be implemented in this regard.

**Organizational aspects:** Human Resource related aspects play a major role in the recruitment of skilled and trustworthy staff. This can be done through effective screening etc. Newly appointed staff must be made aware of company policies and procedures. This can be defined in a policy document by the organization requiring employees to sign upon appointment. Failure to comply with these procedures should result in penalties by the staff member. Some of these policies may have a relationship with technology aspects e.g. do not install pirated software, individuals must encrypt sensitive files when emailing clients, software

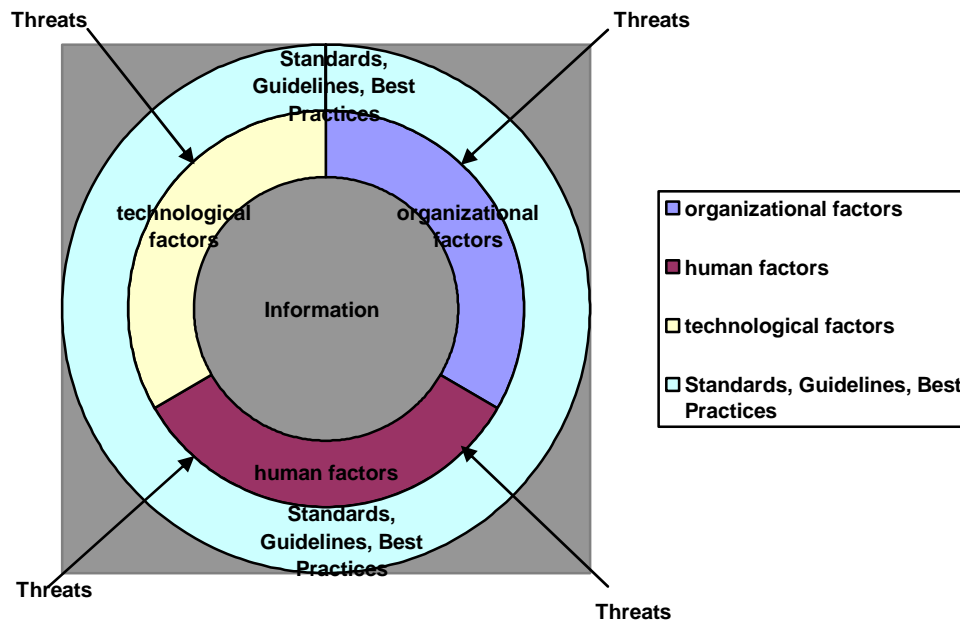
## Phishing: How an Organisation can Protect Itself

updates must be done regularly by IT staff, downloading of files not relative to organization needs is not permitted etc. The organization needs to adopt an information security culture. The organization needs to realize the importance of strengthening and securing their information, and lead the way in ensuring that future security threats are prevented and controlled. This can be done through effective physical and software procedures. It is critically important that the organization should ensure that proper policies, regarding protection against phishing attacks, are defined and that sound procedures are put in place. Once in place, this will then have an effect on the technological aspects and human aspects.

**Human Factors:** As mentioned throughout this paper, the weakest target phishing attacks focus on is through the human aspect. Through education, employees can be made more aware of the activities involved in a phishing attack (van der Merwe, 2005) and how it may affect them and the organization. This can be done through regular training workshops. The training needs to have some incentive or humour in gaining effective participation from its employees. The training should also give relevant examples in context of daily issues that plague employees in the organization, specifically in emails from unknown sources. The latter should address how to identify these threats and what procedures to follow. An added benefit, through training, allows employees to also learn of other current and future threats of information security aspects instead of phishing attacks alone. According to van der Merwe (2005), there are five issues that a company or individual should be aware of in phishing: education, preparation, avoidance, intervention and treatment. All of the latter issues have been considered and addressed in the proposed model.

As previously mentioned, three very important dimensions should form part of the protection model against phishing attacks. These are; technological, organizational and human related dimensions. These dimensions should be governed by applicable standards, best practices and guidelines. Below, figure 1, graphically represents the draft model of the above-mentioned dimensions to be considered in protecting company information from phishing attacks.





*Figure 1: The model highlights major aspects, in an organization, that must be considered to form a complete barrier of defence against phishing attacks*

#### **4 CONTRIBUTION OF THE STUDY AND FURTHER RESEARCH**

The proposed solution will be refined and tested, using design science, through further literature studies as well as a case study in an organization to determine its effectiveness. Sound methodologies will also be utilized to ensure that the model is developed with rigor to result in a trustworthy artifact. Of the three dimensions, through research studied, the human dimension has been established to be the weakest aspect in which phishing threats breach information security.

The detailed, eventual, model will help make an organization more aware of the dangers of phishing and educate them to prevent phishing attacks by addressing all dimensions required



## 5 CONCLUSION

As more organizations provide greater online access for their customers, phishers are successfully using more social engineering techniques to steal personal information and conduct identity theft at a global scale. By understanding the tools and technologies that phishers use, organizations and their customers can take a proactive approach in defending themselves against future attacks. To make this possible, it is imperative that organizations and its employees be properly educated about the dangers of phishing thus addressing the human dimension. It must be understood that all dimensions, as a whole, should be considered in the model and not just one in isolation. This will form a complete barrier against phishing attacks. Although a company may have well defined procedures that employees could read and sign every year, it has proven to be insufficient (Gragg, 2002). The latter can be due to large amounts of policy documentation that employees aren't keen to read and consequently merely signing it. Given a predicted increase in tools available to fight phishing, it is expected that future attacks will continue to be more refined in terms of targeting the user and even specificity (Robila, 2006). The latter such case of an employee within the organization attempting to acquire information illegally through another employee. Therefore, the proposed solution to this problem needs to be designed through an effective, rigorous model.

## 6 REFERENCES

Alkadi, I and Alkadi, G, (2004). '*Information technology in the business world through the years and beyond!*', Journal of Academy of Business and Economics

Badra, M., E-L Sawda, S., Hajjeh, I, (2007). '*Phishing Attacks and Solutions*', ACM International conference proceedings of the 3<sup>rd</sup> International conference on mobile multimedia communications, vol. 329, ICST (Institute for Computer sciences, social-informatics and telecommunications engineering, Nafpaktos, Greece

Proceedings of ISSA 2009

Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008). ‘*Social Networks and context-aware spam*’, Proceedings of the ACM 2008 conference on computer supported cooperative work, ACM, San Diego, CA, USA, pp. 403-412

COBIT (2000), ‘*Control Objectives for information and related technologies*’ (COBIT), 3<sup>rd</sup> Edition, IT Governance Institute, USA, 2000

Downs, J.S., Holbrook, M. and Cranor, L.F (2007). ‘*Behavioral response to phishing risk*,’ ACM International Conference Proceeding series, vol. 269, ACM, Pittsburgh, Pennsylvania, pp. 37-44

Dutta, A., Roy, R. (2008). ‘*Dynamics of organizational information security*’, System Dynamics Review, vol.24, Issue 3.,Wiley Interscience, Accessed 14 April 2009, <http://www3.interscience.wiley.com/journal/121518999/abstract?CRETRY=1&SRETRY=0>

Egelman, S., Cranor, L.F. and Hong, J. (2008). ‘*You’ve Been Warned: An Empirical study of the effectiveness of web browser phishing warnings*’, Conference on Human Factors in computing systems- Proceedings of the 26<sup>th</sup> annual SIGCHI conference on Human factors in computer systems, ACM, Florence, Italy, pp. 1065-1074

Enhancing the development life cycle to produce secure software (2008), Retrieved 28 May 2009 from [http://www.thedacs.com/techs/enhanced\\_life\\_cycles/](http://www.thedacs.com/techs/enhanced_life_cycles/)

Fette, I., Sadeh, N. and Tomasic, A. (2007). ‘*Learning to detect phishing emails*’, Proceedings of the 16<sup>th</sup> International conference on World Wide Web, ACM, Banff, Alberta, Canada, pp 649-656

## Phishing: How an Organisation can Protect Itself

Garera, S., Provos, N., Chew, M. and Rubin, A.D (2007). ‘ *A framework for detection and measurement of phishing attacks*’, Proceedings of the ACM workshop on recurring malcode, ACM, Alexandria, Virginia, USA, pp. 1-8

Gragg, D. (2002). ‘ *A multi-level defense against social engineering*’, SANS Institute InfoSec Reading Room, Accessed on 3 April 2009, <http://www.sans.org/rr/papers/51/920.pdf>

How to keep your computer's operating system and programs up-to-date. Retrieved 17 April 2009 from <http://computing.vassar.edu/safecomputing/security/ospatch.html>

IBM Business Consulting Services (2006). ‘ *Federal Information Security Management Act (FISMA) Compliance Solution- Improving management, operational, and technical controls over information, personnel, and physical security and privacy*’, USA, Accessed on 14<sup>th</sup> April 2009, [http://www-03.ibm.com/industries/global/files/FISMA\\_Cutsheet\\_PS\\_0306.pdf](http://www-03.ibm.com/industries/global/files/FISMA_Cutsheet_PS_0306.pdf)

ICT Standards Board (2007). ‘ *Network and Information Security Standards Report*’, Issue 6.2, Accessed on 17<sup>th</sup> April 2009, <http://www.cen.eu/CENORM/BusinessDomains/businessdomains/iss/activity/nisfinalreport.pdf>

ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management. Retrieved 14 April 2009 from <http://www.iso27001security.com/html/27002.html>

King Report (2001). ‘ *King Report on Corporate Governance for South Africa 2001*’, Accessed on 17 April 2009, <http://general.uj.ac.za/infosci/scipsa/king-report-on-corp-gov.pdf>

Proceedings of ISSA 2009

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). '*Protecting people from phishing: The design and evaluation of an embedded training email system*', Proceedings of the SIGCHI conference on human factors in computing systems, ACM, San Jose, California, USA, pp. 905-914

Microsoft (2008). '*What is spear phishing?-Help prevent identity theft from new targeted phishing scams*', Accessed on 10 April 2009, [http://www.microsoft.com/canada/athome/security/email/spear\\_phishing.aspx](http://www.microsoft.com/canada/athome/security/email/spear_phishing.aspx)

O' Brien, J. (2000). '*Introduction to Information Systems-Essentials for the internetworked Enterprise*, ninth international edition, Irwin/McGraw Hill, United States

Ohaya, C. (2006). '*Managing Phishing threats in an organization*', Information Security Curriculum Development Conference, Proceedings of the 3rd annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, pp 159-161

Orgill, G.L., Romney, G.W., Bailey, M.G and Orgill, P.M (2004). '*The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*', Information Technology Education (Formerly CITC), ACM, New York, USA, Salt Lake City, UT, USA, pp. 177-181

Patel, D. and Luo, X. (2007). '*Take a close look at phishing*', Information Security Curriculum Development Conference'07, Proceedings of the 4th annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, USA

## Phishing: How an Organisation can Protect Itself

Patrick, A., Marsh, S. and Briggs, P. (2005). '*Designing systems that people will trust*', National Research Council Canada, Accessed on 14<sup>th</sup> April 2009, [http://www.iit-iti.nrc-cnrc.gc.ca/publications/nrc-47438\\_e.html](http://www.iit-iti.nrc-cnrc.gc.ca/publications/nrc-47438_e.html)

Robila, S.A and Ragucci, J.W. (2006). '*Don't be a phish: Steps in user education*', Annual Joint Conference Integrating Technology into Computer Science Education, Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, ACM, Bologna, Italy, pp. 237-241

Safecode (2008). '*Software Assurance: An Overview of Current Industry Best Practices*', Accessed on 14<sup>th</sup> April 2009, [http://www.safecode.org/publications/SAFECode\\_BestPractices0208.pdf](http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf)

Security and Privacy / Anti-virus Tools at Software Informer. Retrieved 17 April 2009 from <http://anti-virus-tools.software.informer.com>

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). '*Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish*', Proceedings of the 3<sup>rd</sup> symposium on usable privacy and security, vol.229, ACM, Pittsburgh, Pennsylvania, pp. 88-99

South African Revenue Services – SARS Phishing Attack. Retrieved 14 April 2009 from <http://www.sars.gov.za/home.asp?pid=42736>

Threat Insight Quarterly (2005). '*Phishing and other significant threats of 2004*', Internet Security Systems, Accessed 14 April 2009, [http://documents.iss.net/ThreatIQ/ISS\\_XFIQ0205.pdf](http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf)

Proceedings of ISSA 2009

Unisys (2008). '*Unisys Identifies Five Security Issues Likely to Emerge Across Multiple Industries in 2008*', BusinessWire, Accessed on 14<sup>th</sup> April 2009, [http://www.businesswire.com/portal/site/google/?ndmViewId=news\\_view&newsId=20080115005324&newsLang=en](http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20080115005324&newsLang=en)

van der Merwe, A., Loock, M. and Dabrowski, M. (2005). '*Characteristics and Responsibilities involved in a Phishing attack*', ACM International Conference Proceeding Series; Vol. 92, ACM, Cape Town, South Africa, pp.249-254

Wang, A.J.A. (2005). '*Information Security Models and metrics*', Proceedings of the 43<sup>rd</sup> annual south east regional ACM conference, vol.2, ACM, Kennesaw, Georgia, pp. 178-184

WindowSecurity.com Beyond the Firewall (White Paper). Retrieved 17 April 2009 from <http://www.securityforums.com/viewtopic.php?p=5787&sid=db1bca5dcddd4bff05dd056501b7e922>

Wu, M., Miller, R.C. and Garfinkel, S.L. (2006). '*Do security toolbars actually prevent phishing attacks?*', Proceedings of the SIGCHI conference on human factors in computing systems, ACM, Montreal, Quebec, Canada, pp. 601-610

A Framework for the Rapid Development of Anomaly  
Detection Algorithms in Network Intrusion Detection Systems

**A FRAMEWORK FOR THE RAPID  
DEVELOPMENT OF ANOMALY DETECTION  
ALGORITHMS IN NETWORK INTRUSION  
DETECTION SYSTEMS**

Richard J Barnett<sup>1</sup> and Barry Irwin<sup>2</sup>

Security and Networks Research Group  
Department of Computer Science  
Rhodes University  
Grahamstown, South Africa

<sup>1</sup>barnettrj@acm.org, <sup>2</sup>b.irwin@ru.ac.za

**ABSTRACT**

Most current Network Intrusion Detection Systems (NIDS) perform detection by matching traffic to a set of known signatures. These systems have well defined mechanisms for the rapid creation and deployment of new signatures. However, despite their support for anomaly detection, this is usually limited and often requires a full recompilation of the system to deploy new algorithms.

As a result, anomaly detection algorithms are time consuming, difficult and cumbersome to develop. This paper presents an alternative system which permits the deployment of anomaly detection algorithms without the need to even restart the NIDS. This system is, therefore, suitable for the rapid development of new algorithms, or in environments where high-availability is required.

**KEY WORDS**

NIDS, prototyping, rapid development, anomaly detection, Perl, Snort, frameworks

Proceedings of ISSA 2009

# A FRAMEWORK FOR THE RAPID DEVELOPMENT OF ANOMALY DETECTION ALGORITHMS IN NETWORK INTRUSION DETECTION SYSTEMS

## 1 INTRODUCTION

With the increased frequency of intrusion attempts from the Internet, simple passive technologies such as firewalls are no longer sufficient on their own. Systems which actively monitor traffic within a network are now commonplace and act as a second line of defence for cases when intruders evade first line defences. These systems, known as Network Intrusion Detection Systems (NIDS), act on traffic in one of two specific ways. They either perform signature detection, or they perform anomaly detection. Most current NIDS perform signature detection as a primary feature and perform anomaly detection on a more ad-hoc basis.

While these systems have well defined mechanisms for the addition and alteration of signatures, they have fairly labour intensive methods for the introduction of new algorithms for anomaly detection. This is because these systems usually require new modules to be developed in a compiled language (such as C) and then be loaded. Many of these systems require that these modules be compiled into the NIDS and this process increases the mean time to deployment.

This paper proposes an alternative system which permits the rapid development and deployment of anomaly detection algorithms. This system has its primary use in development environments where the additional time required for other systems makes development cumbersome, and in environments where the deployment of additional (new) algorithms is essential with little or no downtime of the IDS.

### 1.1 Paper Organisation

The remainder of this paper is structured as follows. Section 2 highlights some of the literature which influenced the design of this framework. Section 3 then presents this design, followed by the implementation in Section 4. Thereafter, Section 5 presents a case study of its use, and highlights



A Framework for the Rapid Development of Anomaly  
Detection Algorithms in Network Intrusion Detection Systems

some performance considerations therein. Finally, the paper is concluded in Section 6.

## 2 BACKGROUND

The field of Intrusion Detection, and Network Intrusion Detection in particular, is one with a considerable volume of literature, some of which is related to the construction of this framework, and our extended research. This section highlights some of this work, and describes the context of our extended study.

The authors' ongoing research is focused into the effective detection of network scanning, and was fueled by previous research at Rhodes University [4] which discovered several flaws in the detection methods in popular NIDS such as Snort [10] and Bro [8].

The design of the framework needed to consider numerous factors in scan-detection, network intrusion detection and IDS design. For the purposes of our research, we define scanning as it is defined by Allman *et al.* in [1]. That is, connections being determined as good, bad and unknown (based on the success of the connection) and the classification of hosts as scanning hosts if they produce a majority of bad connections. This definition, coupled with our own taxonomy of network scanning [2] form the basis of a number of algorithms into scan-detection.

Existing research into the construction of a NIDS is scarce, however there is a small selection of research which is of interest. Lee and Stolfo [6] present research into the construction of a novel framework for automated data mining based intrusion detection. Their system, MADAM ID, performed admirably in the 1998 DARPA Intrusion Detection Evaluation [7]. Yang *et al.* [12] present a framework for the use of expert systems and clustering analysis in amalgamating misuse and anomaly detection systems.

In their seminal papers on Snort and Bro (respectively), Roesch [10] and Paxson [8] describe the structure and internal workings of each system. Both Snort and Bro have design features based on the older NIDS, The Network Flight Recorder (NFR) [9] which pioneered the field.

Proceedings of ISSA 2009

### 3 FRAMEWORK DESIGN

The design of a framework for the rapid development of anomaly detection algorithms takes a number of important considerations. This section details a number of those considerations and how they influenced the design of the system.

The design of the framework was based on a number of criteria. These criteria were formulated both from our own need, and from the observed literature. The following were considered:

**Light-Weight** The system needed to be small and efficient with a minimal code base, to keep resource usage by the base system as low as possible.

**Efficient** While the system was designed for prototyping algorithms, it was important to be able to test these algorithms on production traffic. To this end, the system needed to perform well on commodity desktop grade hardware and be able to process traffic from gigabit networking in real time.

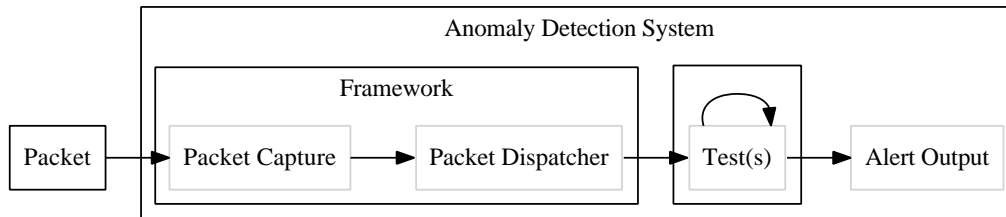
**Interpretable** One of the biggest flaws with the development of preprocessors for systems such as Snort, is the extensive compile time whenever a change is made. For this reason, our framework was required to use an interpreted language.

**End User Simplicity** Finally, the base framework should be independent from each test. This permits authors constructing tests to have limited knowledge of how the base system works. This has the added benefit of permitting changes to the base system without tests having to be rewritten, provided that the interface is well thought out and remains unchanged.

Many of these features are common with Snort and Bro's original design. However, other considerations made for those systems are either implicit in our design, or have been ignored completely.

As a result of these considerations, the framework has been designed to be simple. Figure 1 illustrates this design, and it can be seen that there are only three components to the system. Each of these will be discussed separately.

## A Framework for the Rapid Development of Anomaly Detection Algorithms in Network Intrusion Detection Systems



*Figure 1: Framework Structure*

### 3.1 Packet Capture

The packet capture component of the system is designed to provide an abstract packet data structure to the remainder of the system. This provides a mechanism for different Packet Capture and Dispatcher implementations. As the system is intended to be Light-Weight, the design strips all unnecessary information from each packet before passing it onto the Dispatcher. The packet capture component needs to be as efficient as possible as it is the point at which the most intensive IO occurs within the system, and is discussed further in Section 5.1.

### 3.2 Packet Dispatcher

The packet dispatcher component is possibly the most important in the system. It is this component that loads each of the tests discussed in Section 3.3 and passes the packets captured from the component discussed in Section 3.1. It ensures that incoming packets are processed by the tests, without being dropped and that the tests are executed in order. It also provides an alert mechanism for tests, and the ability to load tests in real-time.

### 3.3 Test(s)

The final component(s) of the framework is(are) the test(s), or the algorithms themselves. As illustrated in Figure 1, the tests are not strictly part of the framework, but a separate element of the overall system. The interface provided by the dispatcher permits several tests to be loaded in a specific order and executed, in real time. The framework allows tests to be loaded and executed without restarting the system. This is to permit the rapid development of algorithms, but at the same time, to permit high availability.

Proceedings of ISSA 2009

## 4 FRAMEWORK DEVELOPMENT

Given the design considerations discussed in Section 3. This section presents the development decisions made in order to achieve the desired design objectives. The authors settled on Perl as an appropriate language for the construction of the framework. This was to permit both the interpreted requirement, but to retain some level of efficiency. Each of the components illustrated in Figure 1 is implemented as a Perl module.

The Comprehensive Perl Archive Network (CPAN) [3] contains numerous modules to perform a wide variety of functions. Amongst these are modules for packet capture, and the authors have made full use of the `Net::Pcap` library, and its interface to *libpcap* to perform efficient packet capture.

The framework was constructed to be threaded, and as a result we could make use of the built in queue system in Perl for the dispatching of packet data. However, we found that Perl's threading system does not share variables between threads by default, and that it is unable to share complex data structures. This limitation was overcome by developing a sharable wrapper for complex data structures, which abstracts the complexities of sharing data from the end user, at a fairly limited performance cost.

The threading system processes each packet in a single thread, and therefore guarantees that tests will run in the correct order for a packet. It does not, however, ensure that packets will be processed in the order that they are lifted from the wire. As IP does not guarantee that packets are received in order, this is of little significance. Perl's ability to compile and recompile code on the fly permitted us to allow the loading and reloading of modules automatically. This fulfils the design goal of permitting rapid development.

## 5 CASE STUDY: NETWORK SCANNING DETECTION

The authors have developed this framework for use in their ongoing research into Scan Detection. This section presents a look at the usability of the framework in the context of rapid development of scan-detection algorithms. The developed algorithms have been tested against both live traffic as it is read off the wire, and traffic previously captured in *pcap* files.

We find that we are able to manipulate algorithms in real time, and observe

## A Framework for the Rapid Development of Anomaly Detection Algorithms in Network Intrusion Detection Systems

the effects of our changes. An unintentional side effect of the implementation of the module loading is, however, that memory is garbage collected during a reload, and it is equivalent to restarting the system.

### 5.1 Performance Considerations

Given that Snort [10] is written in C/C++, it follows that it should offer significantly better performance to our own system, and that the interpreted nature of Perl should offer lower performance. However, since Perl compiles on demand, it offers good performance with a start-up time cost, and a memory cost. Neither of these limitations are of concern, however, and the overall performance remains good.

Despite this we find that the system has a few performance limitations. The threaded testing system permits tests to run effectively, however, we note that the interface to *libpcap* is not as efficient as it could be, and under heavy load the packet capture and dispatch thread pushes the CPU load up. We have not, however, observed any packet loss.

Memory use is significant and is largely due to the design of the tests, rather than due to the framework. The packet data structure is, however, fairly well designed, and a large number of packets can be easily stored in memory.

Our observations are that the packet capture framework can be deployed in a production environment, but that (like with most IDSs [5]) it would perform significantly better when run on its own dedicated system.

### 5.2 Comparison with Snort

Snort is a popular, Open Source NIDS, but is focused on signature detection, rather than anomaly detection. This paper will not comment on the relative effectiveness of the two systems, only on how they operate. Our framework was developed to permit rapid deployment of new algorithms, something which is not performed effectively by Snort. Our system is more CPU intensive than Snort, under load, but not as memory intensive.

Snort offers more sophisticated pre-processing of packets, including stream reassembly and a rule matching system, which make it a fairly large and cumbersome application, and while it is a superb signature detection system, we find that our system processes packets more efficiently if you are only interested in scan-detection. This is largely because we have no interest in

Proceedings of ISSA 2009  
passing packets through the signature engine.

## 6 CONCLUSIONS

This paper has presented the design and implementation of a novel framework for the development of anomaly detection algorithms in the context of network intrusion detection. It has presented the design, and implementation of the framework, and has illustrated how it could be used in the development of anomaly algorithms, in our case scan-detection algorithms.

We have seen that the concept of developing NIDS in an interpreted language is viable, and that Perl is a suitable choice. We have also seen that the overhead for an anomaly detection framework is significantly lower than that for a full blown signature-detection system such as Snort.

### 6.1 Future Work

This research has primarily focused on the development of a framework for the rapid development of anomaly detection algorithms. In particular, we have considered scan-detection. Our research into scan-detection is ongoing and is largely supported by this framework. The framework could, however, be extended in a number of ways. It is a problem which could be offloaded to commodity graphics cards (in a similar way to Gnort [11]) and to integrate it into existing NIDS, such as Snort.

## ACKNOWLEDGEMENT

The authors would like to acknowledge the support of Telkom SA, Comverse, Tellabs, Stortech, Mars Technologies, Amatole Telecommunication Services, Bright Ideas Project 39, THRIP and the NRF through the Telkom Centre of Excellence in the Department of Computer Science at Rhodes University.

## References

- [1] ALLMAN, M., PAXSON, V., AND TERRELL, J. A brief history of scanning. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference*

- A Framework for the Rapid Development of Anomaly Detection Algorithms in Network Intrusion Detection Systems  
*on Internet measurement* (New York, NY, USA, 2007), ACM, pp. 77–82.
- [2] BARNETT, R. J., AND IRWIN, B. Towards a taxonomy of network scanning techniques. In *SAICSIT '08: Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries* (New York, NY, USA, 2008), ACM, pp. 1–7.
  - [3] HIETANIEMI, J. Cpan - comprehensive perl archive network. Online: <http://www.cpan.org/>, April 2001.
  - [4] IRWIN, B., AND VAN RIEL, J.-P. Inetvis: a graphical aid for the detection and visualisation of network scans. In *Conference on Visualization Security (VizSec2007)* (2007).
  - [5] KOHLENBERG, T., ALDER, R., DR. EVERETT F.CARTER, J., FOSTER, J. C., JONKMAN, M., MARTY, R., AND POOR, M. *Snort Intrusion Detection and Prevention Toolkit*. Syngress Publishing Inc., 2007.
  - [6] LEE, W., AND STOLFO, S. J. A framework for constructing features and models for intrusion detection systems. *ACM Trans. Inf. Syst. Secur.* 3, 4 (2000), 227–261.
  - [7] LIPPMANN, R. P., FRIED, D. J., GRAF, I., HAINES, J. W., KENDALL, K. R., MCCLUNG, D., WEBER, D., WEBSTER, S. E., WYSCHOGROD, D., CUNNINGHAM, R. K., AND ZISSMAN, M. A. Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. In *in Proceedings of the 2000 DARPA Information Survivability Conference and Exposition* (2000), pp. 12–26.
  - [8] PAXSON, V. Bro: a system for detecting network intruders in real-time. In *SSYM'98: Proceedings of the 7th conference on USENIX Security Symposium* (Berkeley, CA, USA, 1998), USENIX Association, pp. 3–3.
  - [9] RANUM, M. J., LANDFIELD, K., STOLARCHUK, M., SIENKIEWICZ, M., LAMBETH, A., AND WALL, E. Implementing a generalized tool for network monitoring. In *LISA '97: Proceedings of the 11th USENIX conference on System administration* (Berkeley, CA, USA, 1997), USENIX Association, pp. 1–8.
  - [10] ROESCH, M. Snort - lightweight intrusion detection for networks. In *LISA '99: Proceedings of the 13th USENIX conference on System administration* (Berkeley, CA, USA, 1999), USENIX Association, pp. 229–238.

Proceedings of ISSA 2009

- [11] VASILIADIS, G., ANTONATOS, S., POLYCHRONAKIS, M., MARKATOS, E. P., AND IOANNIDIS, S. Gnort: High performance network intrusion detection using graphics processors. In *RAID '08: Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection* (Berlin, Heidelberg, 2008), Springer-Verlag, pp. 116–134.
- [12] YANG, D.-G., HU, C.-Y., AND CHEN, Y.-H. A framework of cooperating intrusion detection based on clustering analysis and expert system. In *InfoSecu '04: Proceedings of the 3rd international conference on Information security* (New York, NY, USA, 2004), ACM, pp. 150–154.



E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

**E-MAIL SECURITY AWARENESS AT  
NELSON MANDELA METROPOLITAN  
UNIVERSITY  
(REGISTRAR'S DIVISION)**

**Ryno Boshoff<sup>1</sup>, Johan van Niekerk<sup>2</sup>**

<sup>1</sup>Nelson Mandela Metropolitan University  
South Africa

<sup>2</sup>Nelson Mandela Metropolitan University  
South Africa

ryno.boshoff@nmmu.ac.za<sup>1</sup>, johanvn@nmmu.ac.za<sup>2</sup>

**ABSTRACT**

Electronic mail (e-mail) has become a critical business tool within most modern organisations. The proper security features need to be in place to ensure confidentiality, integrity and availability of business related information. After the security features are in place, all staff members need to be educated in the proper use of these features and the proper use of confidential information (ISO SANS 17799, 2005).

This paper presents a survey that was performed in the Registrar's Division at the Nelson Mandela Metropolitan University (NMMU). Structured interview questions were compiled by the researcher. The interviews were conducted on a one-on-one basis with the interviewee. The findings were documented and recommendations were made to improve the usage of the e-mail system and the awareness of security issues amongst the staff at NMMU (Olivier, 2004).

**KEY WORDS**

NMMU, E-mail, Awareness, Policy, Passwords

**E-MAIL SECURITY AWARENESS AT  
NELSON MANDELA METROPOLITAN  
UNIVERSITY  
(REGISTRAR'S DIVISION)**

**1 INTRODUCTION**

E-mail has evolved into a critical business tool in almost all modern organisations. It is not uncommon for an organisation to use an e-mail system as its primary communication method. The information sent and received via e-mail is often of a sensitive and/or confidential nature and should be properly secured (Cisco Networking Academy, 2005).

Although easy to understand and use, e-mail is not a perfectly secure communication medium. In order to protect the contents of an e-mail, organisations should ensure that the necessary security features are in place. Having these security features in place still does not guarantee the security of the information. It is also necessary to educate the end users about these features and about the methods that unauthorized persons may use to get access to the organisation's information. This will help with the detection and prevention of threats and unwanted attempts to access any business information and will ensure confidentiality, integrity and availability of the organisation's information (Cisco Networking Academy, 2005).

The Nelson Mandela Metropolitan University (NMMU) has a link on its staff portal to a website that was designed and is maintained by NMMU, dedicated to communicate Information Security awareness amongst NMMU staff. The purpose of this website is to make the latest Information Security information available to staff at the NMMU and to communicate the latest Information Security (IS) information. This website also has links to the NMMU E-mail Policy, the NMMU Information Security Policy and, guidelines and tutorials with some Information Security fundamentals that have been developed for computer users at the NMMU. Every person using a computer within the NMMU is supposed to go through this basic information. These guidelines and tutorials aim to ensure confident, motivated and educated staff able to

E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

secure business related information. Unfortunately very little or no information exists to verify that these guidelines and tutorials actually work.

This paper aims to help address this lack of knowledge. The paper presents the results of a survey done at the Nelson Mandela Metropolitan University in the Registrar's Division to determine the level of awareness concerning e-mail security amongst end users.

## 2 RESEARCH DESIGN AND METHODOLOGY

A qualitative approach via interview schedules was used to obtain the data. The researcher's aim was to gain an in-depth understanding of the awareness of the staff on e-mail security and their attitude towards the protection of business related information. Closed, fixed-response interviews were used and interviewees were all asked the same questions. They were then asked to choose answers from among the same set of alternatives (Kvale, 1996).

The study was done at NMMU in the Registrar's Division. The sample consisted of 30 staff members, 5 from each department. The Registrar's Division has a total population of 99 staff member. The researcher chose to do the study in this division due to the availability to all staff during office hours. The aim of the study was exploratory and descriptive. The survey questions were created after an extensive literature study during which the researcher attempted to establish the level of e-mail security awareness in the NMMU Registrar's Division (Olivier, 2004).

Due care was taken to ensure respondents participated voluntarily and the entire study was done with full ethical clearance from the relevant authorities (Kvale, 1996).

## 3 SURVEY RESULTS

### 3.1 Direct questions

Question	Yes	No
----------	-----	----

Proceedings of ISSA 2009

<b>1</b>	Do you know whether there is an E-mail Policy at NMMU?	20	10
<b>2</b>	Have you read this E-mail Policy?	10	<b>20</b>
<b>3</b>	Do you open e-mails from unknown people/sources?	<b>22</b>	8
<b>4</b>	Do you have a disclaimer in your new e-mails?	5	<b>25</b>
<b>5</b>	Do you use your work e-mail account for personal e-mails?	<b>28</b>	2
<b>6</b>	When using your work e-mail account for personal e-mail, do you make it clear that these e-mails are an expression of your personal views and not those of the University?	8	<b>20</b>
<b>7</b>	Do you use the university staff and student distribution lists for non-university business?	0	30
<b>8</b>	Do you make use of encryption in the e-mails you send?	4	<b>26</b>
<b>9</b>	Do you make use of digital signatures in the e-mails you send?	4	<b>26</b>
<b>10</b>	Do you access your work e-mail account from your mobile phone or laptop?	0	30
<b>11</b>	If you do access your work e-mail account from your mobile device or laptop, do you know the risks associated when doing this?	0	0

E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

<b>12</b>	If you do access your work e-mail account from your mobile device or laptop, do you know the counter measures to ensure proper security is kept?	0	0
<b>13</b>	Do you access your work e-mail account from home?	8	22
<b>14</b>	If you do access your work e-mail accounts from home, do you know the risks associated when doing this?	0	<b>8</b>
<b>15</b>	If you do access your work e-mail accounts from home, do you know the counter measures to ensure proper security is kept?	0	<b>8</b>
<b>16</b>	Have you given your username/password to Information and Communication Technology (NMMU ICT) staff?	<b>14</b>	16
<b>17</b>	Is there somebody that knows your password?	<b>17</b>	13
<b>18</b>	Is your password written down anywhere so you will not forget it?	3	27
<b>19</b>	Do you have a password protected screensaver?	4	<b>26</b>
<b>20</b>	Do you use the same password in more than one account?	7	23
<b>21</b>	Does your password consist of special characters?	0	<b>30</b>
<b>22</b>	Does your password consist of uppercase and lowercase characters combined?	13	<b>17</b>
<b>23</b>	Does your password consist of more than 6 characters?	28	2

Proceedings of ISSA 2009

<b>24</b>	Does your password consist of numbers and characters combined?	6	<b>24</b>
-----------	--	---	-----------

Question		<b>0 people</b>	<b>1 person</b>	<b>2 people</b>	<b>3 people</b>
<b>25</b>	How many people know your password?	13	<b>11</b>	4	2

Question		<b>0-5</b>	<b>6-10</b>	<b>10-15</b>	<b>16-20</b>	<b>&gt;21</b>
<b>26</b>	How many new e-mails do you send a day?	7	<b>10</b>	6	4	3
<b>27</b>	How many e-mails do you forward a day?	2	<b>16</b>	8	4	0
<b>28</b>	How many e-mails do you receive a day?	0	2	<b>15</b>	9	4

Question		<b>0-20</b>	<b>20-40</b>	<b>40-60</b>	<b>60-80</b>	<b>80-100</b>
<b>29</b>	What percentage of the e-mails sent and received do you consider as confidential?	1	<b>12</b>	8	8	1



E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

Question		Never	When forced	3 Months	6 Months	12 Months
30	How often do you change your password?	12	17	0	1	0

Question		Yes	No	Do not know
31	Do you have a Virus Scanner installed on the work PC?	7	0	23
32	Does your Virus Scanner scan incoming/outgoing e-mails?	0	0	30
33	Is your Virus Scanner updated regularly?	7	0	23

Question		No Screensaver	5 minutes	10 minutes
34	If you have a password protected screensaver, after how many minutes does it become active?	26	3	1

### **3.2 Specifying questions**

**35. Do you have any comments concerning the NMMU E-mail Policy?**

Twenty staff members have not read the policy so they had nothing to say about the policy. Two of the staff members said it is a good E-mail Policy and the other eight said it is easy to understand and to implement.

**36. What do you do with e-mail that you open from unknown sources?**

Eight staff members said that they always delete the e-mails received. Ten staff members said that they have to process e-mails received from unknown people or sources. They receive requests for information on students or staff members that have to be processed and routed to the appropriate person. Twelve staff members confirmed that they open e-mails from unknown people or sources out of curiosity.

**37. Do you know why a disclaimer is needed?**

Twenty three staff members stated that they did not know why a disclaimer is needed. Four staff members said it was to help protect NMMU against any legal actions that could be taken against them because of an e-mail sent. Three staff members said it was the same as a signature within an e-mail.

**38. When using your work e-mail account for personal e-mail, how do you make it clear that these e-mails are an expression of your personal views and not those of the university?**

Five staff members stated that they use a disclaimer in the signature to protect them against legal action. Two staff members said they do not mention NMMU in any way in the personal e-mails they send, so the person receiving the e-mail will know it is not an expression of NMMU. One staff member said that he/she states it in every e-mail that is sent by that staff member.

**39. Do you know why it is good practice not to use you work e-mail account for personal reasons?**

Thirteen staff members said they did not know why it is good practice not to use a work e-mail account for personal reasons. Ten said that they were paid a monthly salary to work, no personal e-mail should be allowed. Six



E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

staff members said that you could receive and forward viruses that could damage, destroy or deny services, and three staff members said his/her e-mail account was the property of the NMMU and should be used according to the rules and regulations stated by NMMU.

**40. What do you consider as confidential?**

Nineteen staff members who were interviewed considered their personal e-mails to be confidential. Thirteen staff members considered student and staff information in e-mails to be confidential. Ten staff members considered work related e-mails to be confidential. Five staff members considered financial information in e-mails to be confidential. Three staff members considered legal information in e-mails to be confidential.

**41. With regards to question number 8 regarding encryption, if you indicated that you do not make use of encryption; can you please elaborate why not?**

Twenty four staff members did not know how to activate and use encryption in the e-mails. Two staff members did not see a reason why encrypting their e-mails was important because they did not consider their e-mails to be confidential.

**42. With regards to question number 9 regarding digital signatures, if you indicated that you do not make use of digital signatures; can you please elaborate why not?**

Twenty four staff members did not know how to activate and use digital signatures in the e-mails. Two staff members did not see a reason why they should add a digital signature to their e-mails because they did not consider the e-mails to be confidential.

**43. What Virus Scanner is installed on your work PC?**

Only seven staff members interviewed, knew the default virus scanner installed on all NMMU's systems is Trend Micro OfficeScan. One staff member acknowledged using McAfee and another acknowledged using Norton Antivirus.

**44. Explain what you know about the following:**

- Virus

Proceedings of ISSA 2009

All staff members interviewed knew that a virus is a program that can damage a system, its hardware and its software.

- Worm

Seventeen staff members said that a virus and a worm have the same characteristics and the same purpose. The rest of the staff members interviewed did not know what a worm is or what it does to an infected system.

- Trojan horse

The majority of the staff members did not know what a Trojan horse is or what it does. One staff member said it has the same characteristics and the same purpose as a virus and another staff member said it is a program that hides and becomes active when ready.

#### 4 DISCUSSION

The following is a brief overview of significant issues highlighted by the survey:

- The NMMU E-mail Policy and the NMMU Information Security Policy are created to provide management direction and support for e-mail and information security in accordance with business requirements and relevant laws and regulations. The policy states what is allowed and what is not allowed within the organisation by any NMMU e-mail account holder. Having and maintaining this policy is not enough. A sound policy needs to be refined over time to adjust for regulatory requirements, business strategy changes and changes in risk. At the NMMU it is clear that most staff members are aware of this policy but **only a few have read this** (ISO SANS 17799, 2005).
- Most interviewees were unaware of **how important** the information is that they are working with.
- The majority of staff members cannot differentiate between “**normal**” information and **confidential** information. Staff members could thus be sending confidential work related information to unauthorized users without their knowledge.
- None of the staff members knows the risks and counter measures associated with using non-NMMU laptops, mobile devices or personal

E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

computers to access business related information. This could pose a risk if staff members access their e-mail accounts from such devices. On the NMMU Information Security website there is a clear description of the consequences when using non-NMMU laptops, mobile devices or personal computers. The website also provides for a step- by-step procedure on how to secure these devices and the connections it uses to access the internet e.g. setting up a VPN (Virtual Private Network), enabling encryption, enabling digital signatures. Clearly the information security content on the website should be “marketed” more internally.

- Only a handful of staff members use disclaimers in the e-mail they send. A disclaimer is a statement denying responsibility intended to prevent civil liability arising for particular acts or omissions. By adding a disclaimer in an e-mail, it could limit the damage after information has been breached and could save NMMU legal fees and save valuable time (Buys, 2004).
- The staff members showed a great uncertainty and lack of knowledge on encryption and digital signatures. The need for encryption and digital signatures is overlooked by the fact that they do not consider the information they work with to be important. A step-by-step procedure is provided on the NMMU Information Security website to show how to activate these features.
- Only a handful of staff members are aware of the virus scanners installed on the system and the current state of it. Most of the staff members have to open e-mails from unknown people or sources. They receive requests for information on students or staff members that have to be processed and routed to the appropriate person. Staff members also use their work e-mail account for sending and receiving personal related e-mails. The use of a virus scanner on these staff members' system is a must. They place the NMMU networks and systems in great danger by continuing to use their e-mail accounts and virus scanners in this manner.
- The sharing of personal passwords is one of the greatest threats to the three components (confidentiality, authentication and integrity) of information security. The staff members clearly indicated that password selection is not seen as an important factor. The key factors when selecting passwords are overlooked. No attention is given to

maximum lengths, permitted characters, etc. and this makes it easier for an unauthorized person to get access to a staff member's password. During the interviews some staff members thought it was acceptable to give the researcher his/her password for examination. Passwords should **never be shared with anyone for any reason.**

## 5 CONCLUSION

Staff members must become more aware of the following:

- NMMU Information Security website and its contents
- NMMU E-mail Policy and NMMU Information Security Policy
- Confidentiality, integrity and availability of information
- Control mechanisms (features) to protect information
- Encryption and digital signatures
- Virus Scanner and threats associated with it
- Password selection and proper use thereof

Being security aware means a person understands that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is e-mailed within an organisation's computer systems and throughout its organisation. From the findings it is clear that there is very limited e-mail security awareness at NMMU in the Registrar's Division. The staff members who were interviewed had hardly any interest in securing the information that they work with and were completely unaware of the consequences of unprotected information. The guidelines and tutorials available on the NMMU Information Security website are not used properly or not used at all. This places NMMU in a very difficult situation with regards to securing valuable information and could lead to the downfall of this organisation.

Encryption and digital signatures are easy ways of ensuring that information sent and received by staff members remains confidential whilst integrity is ensured. The staff interviewed made it clear that they have no interest in making use of these features. The implementation of these two features reduced the risk of unauthorized viewing and altering by a great percentage. Located on the NMMU Information and Security website is a step-by-step procedure on the implementation and use of

E-Mail Security Awareness at Nelson Mandela  
Metropolitan University (Registrar's Division)

encryption and digital signatures within the domain (Cisco Networking Academy, 2005).

A Virus Scanner is considered the first line of defence against all known threats (virus, worm and trojan horse). An in depth knowledge of the Virus Scanner is not needed, but the knowledge of the existence and its current state is. From the findings it is clearly stated by most staff that there is a great lack of knowledge of the current Virus Scanner and the current state of it (Whitman and Mattord, 2007).

The staff interviewed stated that they had not received any form of information security training. Staff members need to attend security workshops, presentations or awareness courses. After the attendance of a security workshop, presentation or awareness course, they need to be reminded of the security aspect on a regular basis. This will ensure continues awareness of information security related matters and the consequence of improper management of information.

## 6 REFERENCES

- Buys, R (2004) *E-mail disclaimers explained*. Available from: <http://www.buys.co.za/> (Accessed 15 June 2008).
- Cisco Networking Academy. (2005) *CCNP2: Remote Access - 3.1*. Available from: <https://cisco.netacad.net/> (Accessed 21 February 2008).
- Kvale, S (1996) *InterViews - An Introduction to Qualitative Research Interviewing*. SAGE Publications, Inc.
- Olivier, M.S. (2004) *Information Technology Research - A Practical guide for Computer Science and Informatics* 2nd edition. Van Schaik Publishers, Pretoria.
- South African National Standard. (2005) *SANS 17799:2005 Edition 2. Information technology – Security techniques – Code of practice for information security management*. Standards South Africa.
- Whitman, M.E and Mattord, H.J. (2007) *Principles of Incident Response and Disaster Recovery*. Thomson Course Technology.

Proceedings of ISSA 2009

Investigating Identity Concealing and Email Tracing Techniques

## INVESTIGATING IDENTITY CONCEALING AND EMAIL TRACING TECHNIQUES

<sup>1</sup>Ickin Vural, <sup>2</sup>HS Venter

Information and Computer Security Architectures Research Group (ICSA)  
Department of Computer Science, University of Pretoria

<sup>1</sup>ickin@tuks.co.za

<sup>2</sup>hventer@cs.up.ac.za

### ABSTRACT

At present it is very difficult to trace the identity of spammers who use identity concealment techniques. It is difficult to determine the identity of the spammer by just analysing the electronic trail.

This paper will look at standard email tracing techniques and how email senders try and hide their electronic trail. The identity concealing techniques that are discussed are: Spoofing, Bot-Networks, Open proxies, Open mail relays and untraceable Internet connections. The techniques used to trace spam that we discuss are: Header analysis and honeypot computers.

The paper will also Investigate advanced digital forensics techniques for email tracing namely Investigating residual data on servers and investigating network devices.

### KEY WORDS

Digital Forensics, Electronic tracing, identity concealment techniques, Spoofing, Bot-Networks, Open proxies, Open mail relays, untraceable Internet connections, Header analysis, honeypot computers.

## INVESTIGATING IDENTITY CONCEALING AND EMAIL TRACING TECHNIQUES

### 1 INTRODUCTION

Unsolicited bulk communication also known as spam is the practise of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients (Spamhaus, 2009).

The sending of unsolicited bulk communications with the intention to advertise products and generate sales is economically viable because senders have no operating costs beyond the management of their mailing lists. Because the cost of setting up a spamming operation is low spammers are numerous. Thus the volume of unsolicited bulk communications has increased dramatically over the past few years (*Messaging Anti-Abuse working group, 2007*).

The costs of spam, involve lost productivity and fraud, these costs are borne by the general public, institutions that store and retrieve mail for their employees and by Internet service providers. Institutions and Internet service providers have been forced to add extra capacity to cope with the high volumes of unsolicited bulk communications (*Europa Press Releases, 2009*).

Anti spamming legislation has been introduced in many jurisdictions. The problem faced by law enforcement is that spammers move their operations to jurisdictions that have no or weak anti spamming laws.

At present it is very difficult to trace the identity of spammers who use identity concealment techniques. It is difficult to determine the identity of the spammer by just analysing the electronic trail using standard email tracing techniques.

This paper focuses on current email tracing techniques and how email senders try and hide their electronic trail. The objective is to present the current state of tracing the origin of unsolicited bulk communications and then suggest techniques utilising digital forensics in an attempt to trace spam.



## Investigating Identity Concealing and Email Tracing Techniques

The remainder of the paper is structured as follows. The background section defines spam in more detail and also defines its cost and causes. . The next two sections are devoted to the state of the art of spamming techniques and how to trace spammers. More specifically, these two sections contrast each other in the sense that the third section looks at techniques that spammers use to conceal their identities, whereas the fourth section looks techniques for tracing the origins of spam so that the spammers can be identified. The paper's main contribution is purported in the next section, which discusses advanced digital forensics techniques for email tracing.

## 2 BACKGROUND

Unsolicited bulk email otherwise known as spam is an email sent to a large number of email addresses, where the owners of those addresses have not asked for or consented to receive the mail (*Internet Service Providers' Association, 2008*). Spam is used to advertise a service or a product. An example of spam is an unsolicited email message from an unknown or forged address advertising Viagra.

Spam is one of the most significant threats to the Internet, accounting for around 60% of all email traffic (*Internet Service Providers' Association, 2008*). Spam costs consumers and ISPs lots of money in bandwidth charges. Despite the growing number of technological means for combating spam, the spammers somehow manage to stay one step ahead and the deluge shows little sign of abating. .

Spammers generally do not pay much for the sending of spam. They accomplish this by exploiting open mail servers to do their task for them. The spammer need only send one email message to an incorrectly configured mail server to reach thousands of email addresses, with the bulk of the transfer being handled by the mis-configured mail server. Recipients in turn need to pay access costs or telephone costs in order to receive content they didn't ask for.

Proceedings of ISSA 2009

ISPs have to bear the bulk of the cost for bandwidth overuse by spammers, this cost is often passed onto the consumer through increased Internet access fees or a degraded service level.

With the introduction of the "Electronic Communications and Transactions Act, 2002" unsolicited emails now have a legal definition and the sending of spam is illegal (*Acts Online, 2002*). Spammers if identified are liable for a fine and prosecution. Thus spammers will attempt to cover their trail to prevent identification.

Spammers are able to send email and cover their trail because Emails use Standard Mail Transfer Protocol (SMTP) which is not a secure protocol and can be tampered with (*Tzerefos, P. Smythe, C. Stergiou, I. Cvetkovic, S. 1997*).

Emails consist of two main parts a message header and a message body. The message header contains information about the destination network address and the source network address as well as routing information. The email headers are not secure and can be easily forged to add false routing data and to hide the source network address. This paper will discuss both email concealment and email tracking techniques respectively in the following two sections.

The following section will describe in detail techniques used by spammers to conceal their identities from persons who would attempt to identify the source of spam mail.

### **3 HOW SPAMMERS CONCEAL THEIR IDENTITIES**

Spammers conceal their identities for a number of reasons. If they are based in a jurisdiction which has strict anti-spamming laws they do not want to be traced for fear of prosecution. If they are based in a jurisdiction which has weak anti-spamming laws then the primary motive is not to be traced and blacklisted. As many ISP's will block any mail from blacklisted sites. The techniques studied are Spoofing, Bot-Networks, Open proxies and untraceable Internet connections.

#### **3.1 Spoofing**

Spoofing is the process whereby a spammer would insert fictitious headers into the email address to hide the network address of their computer. The

## Investigating Identity Concealing and Email Tracing Techniques

spammer will usually insert fake “From” and “Reply-To” headers into the email, these headers would point to a non-existent network address or more commonly an innocent third parties’ network address (*Boneh, Dan, 2004*).

### 3.2 Bot- Networks

A Bot-Network consists of a set of machines that have been taken over by a spammer using Bot software sent over the Internet. This Bot software hides itself on its host machine and periodically checks for instructions from its human Bot-Network administrator. Botnets today are often controlled using Internet Relay Chat (*Evan Cooke, Farnam Jahanian, and Danny McPherson. 2005*). The owner of the computer usually has no idea that his machine has been compromised until its Internet connection is shut down by an ISP. As most ISP’s block bulk mail if they suspect it is spam the spammers who control these Bot-Networks typically send low volumes of mail at any one time so as not to arouse suspicions. Thus the spam mail can be traced to an innocent individuals network address and not the spammers network address.

While the number of Botnets appears to be increasing, the number of bots in each Botnet is actually dropping. In the past Botnets with over 80 000 machines were common (*Evan Cooke, Farnam Jahanian, and Danny McPherson. 2005*). Currently Botnets with a few hundred to a few thousands infected machines are common. One reason for this is that smaller Botnets are more difficult to detect and may be easier to sell or rent.

### 3.3 Open Proxies

An open proxy is a machine that allows computers to connect through it to other computers on the Internet. Open proxies exist because they enable unhindered Internet usage in countries that restrict access to certain sites for political or social reasons. An Internet user in a country that restricts Internet access can access blocked sites by using an open proxy in a country that does not restrict Internet access.

Spammers use open proxies to hide their network addresses. The recipient of a spammers email will not see the spammers’ network address

on the email but the open proxy's network address. It is estimated that sixty percent of all spam is sent using an open proxy (*Boneh, Dan, 2004*).

### **3.4 Open mail relays**

Emails sent over the Internet pass through a number of gateways on their way from the sender to the receiver, these gateways are called mail relays. Each time an email passes through a mail relay it has a Received header inserted, this will have the network address of the computer that connected to the mail relay.

An open mail relay is a mis-configured mail relay that accepts mail from any computer on the Internet and forwards it to any other computer on the Internet as opposed to a normal mail relay that accepts mail from a limited number of computers on the Internet and forwards it to a limited number of computers (*Flavio D. Garcia, Jaap-Henk Hoepman and Jeroen van Nieuwenhuizen. 2004*).

This helps the spammer conceal his identity as it appears that the mail is from the open relay and not from the spammer. However as the spammers network address is still found in the emails headers the spammer would insert fake headers into the email. Open mail relays are usually used together with open proxies to conceal the network address of the spammer.

### **3.5 Untraceable Internet connections**

Spammers can also conceal their identities by accessing the Internet from Internet cafes, university computer labs and by using stolen 3G cards. There is thus no way of tracing spammers who access the Internet using these methods. Even if the network address of the computer used is identified this cannot be connected to the identity of the spammer.

## **4 HOW DIGITAL FORENSIC INVESTIGATORS CAN TRACE THE IDENTITY OF SPAMMERS**

The two primary methods for tracing the origins of spam are header analysis and honeypot computers. The following section studies methods for email tracing and their limitations. The methods studied are header analysis and honeypot computers.

## Investigating Identity Concealing and Email Tracing Techniques

### 4.1 Header analysis

By studying the email headers in a spam email we should be able to identify the senders' network address. Spammers know this and try and divert us from the trail by inserting fake headers. In addition as mentioned previously by using open proxies or Bot-networks the network address of the spammer is not even on the headers. Thus the use of header analysis to trace spammers is highly unlikely.

The only header that cannot be easily forged is the first received header, as all the others may be faked. Spammers will fake their headers to conceal their network addresses. This means that header analysis is not a time and cost effective method to use when tracing spam. The following figure shows an email with the various header tags.

```
Microsoft Mail Internet Headers Version 2.0
Received:      from      s058eml004004.ds1.ad.absa.co.za [1]
                ([10.6.50.91]) by V058EMLFFF004.ds1.ad.absa.co.za [2] with
                Microsoft SMTPSVC(6.0.3790.3959);

                Thu, 5 Mar 2009 11:47:49 +0200
Received:      from      S200INT006001      ([169.202.65.146]) by
                s058eml004004.ds1.ad.absa.co.za      with      Microsoft
                SMTPSVC(6.0.3790.3959);

                Thu, 5 Mar 2009 11:47:49 +0200
Received:      from      relayin-at1.absa.co.za ([169.202.65.20]) by
                S200INT006001 with InterScan Message Security Suite; Thu, 05
                Mar 2009 12:03:31 +0200
Received:      from      kendy.up.ac.za      ([137.215.101.101]) by
                relayin-at1.absa.co.za      with      Microsoft
                SMTPSVC(6.0.3790.3959);

                Thu, 5 Mar 2009 11:45:59 +0200
Received:      from      b040pc181.up.ac.za [3]      ([137.215.40.181]
                helo=notebook)

                by kendy.up.ac.za with esmtp (Exim 4.63)
                (envelope-from <hventer@cs.up.ac.za>)
                id 1LfAB1-0001RS-AW

                for Ickin.Vural@absa.co.za; Thu, 05 Mar 2009
                11:47:39 +0200
```

## Proceedings of ISSA 2009

```
From: "Prof. Hein Venter" <hventer@cs.up.ac.za>
To: <Ickin.Vural@absa.co.za>
Subject: Meeting next week
Date: Thu, 5 Mar 2009 11:45:02 +0200
Message-ID: <FC414216270A45DEAEB887C3BF3C8A18@UP>
MIME-Version: 1.0
Content-Type: text/plain;
    charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Office Outlook 11
Thread-Index: Acmdw5GmQGAIM2STqiIW8+jHkG6AQ==
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579
X-Scan-Signature: 1241d9d45ce102941afa91f8ab9dc533
Return-Path: hventer@cs.up.ac.za
X-OriginalArrivalTime: 05 Mar 2009 09:46:03.0937 (UTC)
FILETIME=[33047910:01C99D77]
```

*Figure 4.1 An Email Header*

The above email is sent by the University of Pretoria's email sever b040pc181.up.ac.za as highlighted at number [3] in the figure. This is sent to the relay server relayin-at1.absa.co.za [2] which, in turn, sends it to Absa's email server s058eml004004.ds1.ad.absa.co.za [1]. This shows us how we can find the identity of the email sender by tracing the route the email took by analysing the header. But as mentioned earlier a spammer can tamper with these headers so as to confuse an investigator.

## 4.2 Honeypot computers

A honeypot is a closely monitored computing resource that is intended to be compromised (*Niels Provos. 2004*). A honeypot computer can be applied to Bot-networks, open proxies and open relays. Thus by setting up a computer to imitate an open proxy or a Bot-network, investigators can attempt to trap the spammers into revealing their network addresses.

#### 4.2.1 Honeypots on Bot-Networks

One way of identifying spammers is to set up a computer to pretend that it is part of a Bot-network (*Boneh, Dan, 2004*). By allowing the honeypot computer to become part of the Bot-network we can obtain the Bot-network software used by the spammer. Once this has been done the honeypot waits for the spammer to send new instructions and then identifies the network address of the sender. The problem with this approach is that spammers could send the instructions to the Bot-networks under their control over open relays and open proxies thus it may be impossible to discover the identity of the spammer's network address.

#### 4.2.2 Honeypots on open proxies

By setting up a honeypot on an open proxy and waiting for spammers to use it in order to send their spam, we can attempt to identify the spammer's network address. This could be done by keeping records of all connections made by the proxy to locate the source of the spam.

The fake open proxies emulate a subset of the HTTP protocol. Requests made with methods other than GET and CONNECT are answered with an error message. GET requests are answered with a randomly generated page. CONNECT requests to port 25 are internally redirected to an emulated open relay. The reason for this redirection is that the spammer may think nothing went wrong and he is connected to the SMTP server he requested, while he actually is connected to a honeypot. CONNECT requests to ports other than 25 are served with a "Request timeout" message (*Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni and Francesca Mazzoni. 2005*).

To identify spammers, it is necessary to encourage them to use honeypot services to their advantages. This is done through the deployment of fake servers, such as open proxies. To ensure traceability of their actions, logging must be enabled for the honey pot open proxy (*Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni and Francesca Mazzoni. 2005*).

Spammers try and get around this by using a proxy chain. A proxy chain is when a spammer sends spam mail through a chain of open proxies

Proceedings of ISSA 2009

and, thus, reducing the chances of their network addresses being compromised (*Boneh, Dan, 2004*).

#### **4.2.3 Honeypots on open relays**

This works by setting up a honeypot on an open relay and waiting for spammers to use it. We would then be able to trace the network address of the spammer using the open relay to send spam.

The fake open relays emulate a SMTP server. All the main commands of the SMTP protocol are implemented, so that spammers cannot notice the difference with a real server. When an e-mail is sent through the open relay, it actually does not reach destination, since all messages are logged but not forwarded, except the very first one. This is done in order to fool a spammer who sends a first probe message to himself to see if the service is properly running (*Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni and Francesca Mazzoni. 2005*).

This technique is similar to that used on open proxies. Thus the spammer would attempt to get around this in the same manner by using a relay chain. The following section describes some advanced techniques used in identifying spammers.

## **5 ADVANCED EMAIL TRACING TECHNIQUES USING DIGITAL FORENSICS**

As discussed previously it is very difficult to obtain the network addresses of spammers. This paper discussed techniques such as header analysis and honeypot computers used to discover the network addresses of spammers. This section discusses digital forensic techniques used to determine the network addresses of spammers. The techniques studied are investigating network devices such as routers, investigating residual data on servers and using bait tactics to identify spammers.

### **5.1 Investigating Network devices**

If logs are unattainable from the servers used by the spammer a routers log can be used instead to obtain information about the spammers network address. (*Patryk Szewczyk, 2007*) If say no access was given to the server logs of the ISP or proxy server that sent the email, the investigator can



## Investigating Identity Concealing and Email Tracing Techniques

analyse the log files of the router or switch that routed the email. This should enable an investigator to determine where the email was sent from.

### 5.2 Investigating Residual data on servers

SMTP servers keep a copy of emails even after they have been delivered. By using this information we can trace the address of the computer that made the connection. By analysing these in a proxy server the identity of the computer making the connection could be obtained. This would require access to the servers which might not always be given as the proxy server might be located in a jurisdiction that does not have anti spamming laws (*Al-Zarouni Marwan, 2004*).

### 5.3 Using Bait tactics to identify spammers

If the email address of the spam message is genuine, forensic investigators can e-mail a message to the sender containing an http “<img src>” tag where the source of the picture is placed on an http server. As soon as the person receiving the e-mail opens it, a log entry with his IP address is recorded on the http server holding the image. This tracks down the sender of the e-mail and establishes his ownership of the e-mail account (*Al-Zarouni Marwan, 2004*). However this technique is not always useful as some browsers automatically block the downloading of images by default (*Microsoft Office online, 2009*).

If the person receiving the e-mail is using a proxy server, his IP address will not show in the HTTP logs but rather, the IP of the Proxy server he/she used. In this case the proxy logs can be checked for persons accessing that picture at that time.

If the person in question is using an open proxy server that does not cooperate with law enforcement, one of the following two tactics can be used to track him/her down:

1. Java Applet: The investigator sends an e-mail with an “embedded” Java applet that runs on the receiver’s machine and extracts his IP address and e-mails it to the investigator.

2. Active X Control: The investigator sends an e-mail address containing an HTML page with Active X that extracts the receiver’s IP address and other information from his machine and sends it to the investigator.

## 6 SPAMMER IDENTIFICATION

One of the issues with identifying spammers is that SMTP is not a secure protocol and can be tampered with. Some researchers have advocated the adoption of a secure email protocol. (*A. Herzberg, 2005*) But until such time that this technology is widely adopted, and its usefulness would be limited if spammers make use of bot-networks and open proxies to send spam, other means of discouraging spammers must be found.

Spammers on the other hand are in the business of spamming because they want to make a profit. Spammers send spam advertising a product that they hope to sell and a bank account number to which payment should be made. By tracing the information in the email message body an investigator should be able to identify the source of some spam. This however is not enough as the enterprise can deny having sent the spam mail and the investigators may not be able to conclusively prove ownership.

Thus a proposal to identify spammers would be to create an implementation that identifies computers which are sending spam. These computers should then be added to a spam list that could be blocked by an ISP. This framework would need to identify bot-networks as well as open proxies sending spam. Once on a spam list, it is up to the individual or organisation concerned to have their network address removed from the spam list.

The detection of spamming computers can be done by analysing the network layer traffic and determining patterns that match bot-networks and open proxies sending spam.

The implementation would detect spam by analysing data provided by an ISP to identify abnormal behaviour on the network to identify spammers. This system will enable ISP's to proactively locate open proxies and bot-networks.

This would require analysing large data sets which would require a large amount of computing power. However the computing power of computers has increased and computers such as blade servers that can be programmed to analyse data using parallel computing techniques are now

## Investigating Identity Concealing and Email Tracing Techniques

available. Thus it is possible for ISP's to analyse large datasets to detect abnormal behaviour in a way that was not possible a number of years ago.

### 7 DISCUSSION

The implementation of a system to detect spammers by analysing network traffic for abnormal behaviour has some shortcomings, mainly that spammers do not usually send out mail in bulk but in smaller packets so as to avoid detection.

The implementation would have to take into account spam email sending patterns to effectively identify spammers. The implementation could either make use of artificial intelligence to learn behaviour by feeding it training patterns or by using graph analysis which is perhaps better suited for large scale data analysis.

The authors of this paper, however, still need to explore their ideas mentioned in this paper in future work so as to produce a proof-of-concept prototype.

### 8 CONCLUSION

This paper outlines the challenges facing digital forensic investigators when attempting to identify spammers. Servers that contain forensic data such as log files showing the network addresses of the computers that have connected to it, that would enable a digital forensic investigation, are not made available by the servers' owners for various reasons. The usual reason for the refusal is that court orders requesting this data to be made available, may not apply to that jurisdiction.

The use of bot-networks means that even if the source of the machine sending the spam is identified the person owning the machine is not the one responsible for sending spam. The use of untraceable Internet connections and open proxies to communicate instructions to bot-networks makes the use of Honeypots unlikely to succeed.

Thus any success in tracing spammers will be matched by spammers using increasingly sophisticated techniques to evade detection. Greater responsibility will have to fall to ISP's in monitoring connections to open

Proceedings of ISSA 2009

proxies as well as attempting to shut down open relays. Nevertheless an arms race between spammers and forensic investigators will continue for the foreseeable future.

## 9 REFERENCES

Al-Zarouni Marwan. 2004. Tracing E-mail Headers. We-B Centre & Edith Cowan University.

Boneh, Dan. 2004. The Difficulties of Tracing Spam Email. Department of Computer Science Stanford University.

A. Herzberg, Controlling Spam by Secure Internet Content Selection, Proceedings of Secure Communication Networks (SCN) 2004, LNCS vol. 3352, Springer-Verlag.

Acts Online, 2002. Electronic Communications and Transactions Act, 2002. Available: [http://www.acts.co.za/ect\\_act/](http://www.acts.co.za/ect_act/). [April 2009]

Europa Press Releases, 2009. Data protection: "Junk" e-mail costs Internet users 10 billion a year worldwide. Available: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en>. [April 2009]

Messaging Anti-Abuse Working Group, 2007. Email Metrics Program: The Network Operators' Perspective. Available: [http://www.maawg.org/about/MAAWG20072Q\\_Metrics\\_Report.pdf](http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf). [April 2009]

## Investigating Identity Concealing and Email Tracing Techniques

Evan Cooke, Farnam Jahanian, Danny McPherson. 2005 . The advanced computing systems association. [Online] The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. Available: [http://www.usenix.org/events/sruti05/tech/full\\_papers/cooke/cooke\\_html/](http://www.usenix.org/events/sruti05/tech/full_papers/cooke/cooke_html/) [April 2009]

Flavio D. Garcia , Jaap-Henk Hoepman and Jeroen van Nieuwenhuizen, 2004. Spam Filter Analysis: IFIP International Federation for Information Processing. Springer Boston

Internet Service Providers' Association, 2008. 'What is Spam?' Available: <http://www.ispa.org.za/spam/whatisspam.shtml>. [April 2009]

Microsoft Research. S-GPS: Spammer Global Positioning System. Available: <http://research.microsoft.com/en-us/projects/S-GPS/>. [April 2009]

Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni and Francesca Mazzoni. 2005. The advanced computing systems association. [Online] HoneySpam: Honeypots fighting spam at the source. Available: [http://www.usenix.org/event/sruti05/tech/full\\_papers/andreolini/andreolini\\_html/](http://www.usenix.org/event/sruti05/tech/full_papers/andreolini/andreolini_html/). [April 2009]

Microsoft Office online, 2009. About protecting your privacy by blocking automatic picture downloads. [Online] Available: <http://office.microsoft.com/en-us/outlook/HP010440221033.aspx>. [April 2009]

Niels Provos. 2004. The advanced computing systems association. [Online]. A Virtual Honeypot Framework. Available: [http://www.usenix.org/event/sec04/tech/full\\_papers/provos/provos\\_html/](http://www.usenix.org/event/sec04/tech/full_papers/provos/provos_html/). [April 2009]

Patryk Szewczyk, 2007. ADSL Router Forensics Part 1: An introduction to a new source of electronic evidence We-B Centre & Edith Cowan University.

Spamhaus, 2009. The Definition of spam. Available: <http://www.spamhaus.org/definition.html> [April 2009]

Tzerefos, P. Smythe, C. Stergiou, I. Cvetkovic, S. 1997. A comparative study of Simple Mail Transfer Protocol (SMTP), PostOffice

Proceedings of ISSA 2009

Protocol (POP) and X.400 Electronic Mail Protocols. Proceedings., 22nd  
Annual Conference on Publication Date: 2-5 Nov1997.

Yao Zhaoy , Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Cheny, and  
Eliot Gillumz BotGraph: Large Scale Spamming Botnet Detection.  
Microsoft Research

## ENHANCED PRESENCE HANDLING

Rudi Victor<sup>1</sup>, Andrew Rutherford<sup>2</sup>, Reinhardt Botha<sup>3</sup>

<sup>1,2,3</sup> Nelson Mandela Metropolitan University  
Institute for ICT Advancement  
South Africa

<sup>1</sup>rudivictor@gmail.com, <sup>2</sup>andrew.rutherford@nmmu.ac.za,  
<sup>3</sup>reinhardt.botha@nmmu.ac.za

### ABSTRACT

The global use of the Internet and modern mobile/cellular communications networks has made ubiquitous communications possible for millions of people worldwide. However, these technologies can interrupt our daily activities through uncontrolled, unwanted disturbances. Such negative effects can be lessened by using context information and presence technology to inform others of our availability for communication. By nature context information can be sensitive and a commodity which its owner values highly. It thus becomes important to assess the impact of releasing such information on personal privacy. This can vary widely, depending on various factors. In this paper the authors review presence technology as a means to control unwanted disturbances. We consider the privacy implications and propose an enhanced presence processing model which leverages Role-Based Access Control (RBAC) principles as well as a new concept, "Availability Profiles". We present the model incrementally over three progressive and logical stages.

### KEY WORDS

Presence, Presentity, Privacy, Watcher, Role-based access control

## ENHANCED PRESENCE HANDLING

### 1 INTRODUCTION

With the evolution of networks, such as mobile/cellular communications and the Internet, the notions of ubiquitous computing and anytime-anywhere communications have become a reality for millions of people worldwide. However, the power of these networks, and related technologies, also have negative implications to consider and manage.

While people are able to work and communicate in a convenient and ubiquitous manner, the same technologies making this possible also cause uncontrolled and frequently annoying interruptions (Markus, 1994), which lead to a loss in productivity. This leads to another layer of technology being needed to manage and control these issues.

Because users would like to be available for communications, but want to minimize the disruptive effects of unwanted disturbances, information such as presence (Day, Rosenberg, & Sugano, 2000) has been used to provide clues as to the current availability of a user. However, providing such context to others can lead to potential concerns regarding privacy, which need to be considered carefully by a user.

In this paper the authors review presence technology as a means to control unwanted interruptions. We consider the privacy implications and propose a Role-Based Access Control (RBAC) (Sandhu, Coyne, Feinstein, & Youman, 1996) model to control the sharing of personal context information. A prototype implementation of the model illustrates the strengths and weaknesses of such an approach. Finally we illuminate future research needed in this area.

### 2 THE COMMUNICATION PARADOX

The sheer number of communication channels available today can, paradoxically, make it increasingly time consuming for human beings to establish communication amongst each other. By the same token these multiple channels of communication can increase the number of unwanted and disruptive communication attempts a person receives.

To illustrate let us view a typical communication attempt scenario from the perspective of both the caller and the callee. Alice wishes to contact Fred.



## Enhanced Presence Handling

She knows Fred has an email address, Instant Messaging (IM) account, an office phone and a cellphone. Alice first sends an email message to Fred in the hopes of getting a prompt reply. Not receiving one, she proceeds to attempt to engage Fred in an IM conversation. After typing several messages with no response she calls Fred on his cellphone, which, after ringing a short period routes her to his voicemail. As a last resort she phones his office number only to hear Fred curtly informing her that he is busy and cannot talk now.

Let us now view Alice's attempts at communication from Fred's perspective. Fred is engaged in an important meeting with his company's managing director. Whilst discussing the latest sales figures his email client alerts him to a new message. He is mildly distracted for a second but continues with his discussion. Several minutes later Fred faces more distractions by the intermittent display of messages from Alice on his IM client. Choosing to ignore them, he continues with his meeting. It is at this time that Alice rings his cellphone. Fred of course had put his phone on silent thus avoiding the embarrassment of it ringing; it does however succeed in vibrating off the desk. Eventually his office line rings and he is forced to answer but abruptly informs Alice that he is busy and hangs up the phone.

From this simple example it is clear that both parties have been impacted negatively by Alice's attempts to contact Fred. She has wasted several minutes of her time in attempting to establish meaningful communication with Fred, which she is unable to do. Fred on the other hand suffered numerous unwanted interruptions which only succeeded in distracting him from a more important task.

The effects of interruption in our daily activities is a prominent research topic (O'Conaill & Frohlich, 1995; Jett & George, 2003; Rennecker & Godwin, 2005). It is clear that a need exists for a solution which controls interruptions while maintaining ubiquitous communications. Thus just switching a communications device off cannot be seen as an acceptable solution because of the loss of all communications.

The availability of user context can assist in making a more accurate communications request (Ljungstrand, 2001). This is a concept well-known from the Instant Messaging (IM) domain where presence information is available to parties. Such information can indicate basic availability as well as detailed information about the current state of a user. Research on the benefits of using such information in communications has established that it can be a useful mechanism to control unnecessary interruptions (Carroll, Neale, Isenhour, Rosson, & McCrickard, 2003; McCrickard, Catrambone, Chewar, &

Stasko, 2003; Sonnenwald, Maglaughlin, & Whitton, 2004). The architecture for the implementation of such a solution is also clear and well defined (Day et al., 2000; Rosenberg et al., 2002; Roach, 2002).

As technology improves and advanced sensors become available, the level and quality of context information that can be obtained becomes very detailed. For instance, a person's location can be determined using his cellphone or his current activity and persons with whom he is engaged can be discovered through his electronic calendar. Such detailed information can be seen as extremely sensitive and private and it becomes important to ensure the privacy of such information. Privacy encompasses the confidentiality and integrity of the information, but also controlling the access to such information by other parties. The problem of preserving the privacy of context information thus becomes an issue of access control.

Prior to presenting our enhanced model it is requisite that we should provide an overview of a current presence processing model.

### 3 CURRENT PRESENCE PROCESSING

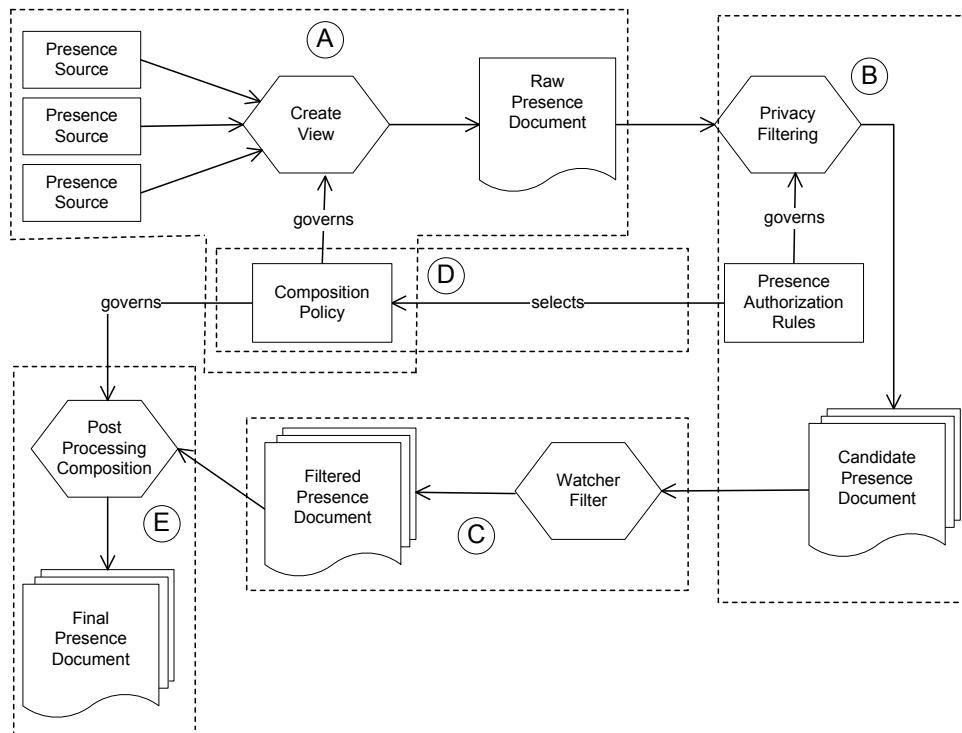
The Internet Draft "A Processing Model for Presence" provides a model that describes and defines the processing operations used by presence agents in processing presence information in a SIP and SIMPLE environment (Rosenberg, 2005). The proposed model, hereafter referred to as the Rosenberg-model, is depicted by figure 1. To facilitate the discussion which follows it will be prudent to clarify two terms. A presentity is an entity that has presence information, and a watcher is an entity that is interested in the presence information of a presentity.

Watchers whose subscriptions have been accepted receive presence information notifications. To fulfill notifications the presence server must generate a presence document for each watcher. This presence document generation process, detailed by Rosenberg (2005), shall be discussed in brief.

The first step in the presence document generation process is collection. Collection involves the obtaining of all the event state information required for giving an accurate picture of a presentity's presence. This event state information can come from a variety of presence sources as illustrated by figure 1.

A composition operation now occurs which compiles all collected information to produce the raw presence document or initial view. "Raw" is appropriate since at this stage the presence document contains the full presence

## Enhanced Presence Handling



*Figure 1: The Rosenberg Presence Processing Model (Rosenberg, 2005)*

picture of a presentity; more information than any watcher might actually see. The composition phase makes use of several techniques to achieve its objectives. These include correlation, conflict resolution, merging and splitting. Correlation uses information in one presence document to effect information in another; conflict resolution must resolve situations where conflicting presence information is reported by multiple sources; merging involves combining different devices or services into a composite device or service; splitting is the antithesis of merging i.e. a single device or service is split into two devices or services.

Having compiled the raw presence document it is requisite to perform privacy filtering. This entails the removal of information from the raw document and thus withholding certain information about the presentity. Presence filtering is influenced by the identity of the watcher and other factors such as time of day, location and so forth. The manner in which privacy filtering is performed is determined by an authorization policy which comprises presence

authorization rules (Rosenberg, 2006).

A watcher may also control the information he receives by specifying filters along with his subscription request. At this point a presence document can be despatched to a watcher.

As a result of privacy and watcher filtering there may be information lacking to differentiate certain device and service elements from one another. In such a case further composition rules will be applied.

The presence processing model depicted by figure 1 has been partitioned into five logical groupings namely A, B, C, D and E. Grouping A represents the collection and composition phases which results in the creation of the raw presence document. A default composition policy is used to generate this raw presence document.

Grouping B represents the privacy filtering which must take place on a watcher-by-watcher basis. Presence authorization rules (Rosenberg, 2006) are applied to ensure that each watcher receives only that subset of presence information to which he is entitled i.e. the candidate presence document. It is possible at this point that the authorization policy can select a composition policy other than the default to generate the presence document sent to the watcher. This optional process is indicated by D.

Grouping C illustrates the ability of the watcher to optionally further filter the presence information he will receive, resulting in a presence document filtered according to his requirements.

Grouping E shows the optional application of further composition rules prior to the generation of the final presence document.

#### 4 ROLE-BASED ACCESS CONTROL (RBAC)

Figure 2 shows the family of role-based access control models expounded by Sandhu et al. (1996). In order to facilitate the discussion of the application of RBAC to presence information it would be a useful exercise to map the primary RBAC terminology to those used in the presence domain.

**User:** In the RBAC model a user is a human being with the potential to gain access to a resource. In the presence domain **watchers** are users who wish to gain access to the presence information of a presentivity.

**Role:** A role in RBAC typically refers to a named job junction and describes the authority and responsibility assigned to a member of the

## Enhanced Presence Handling

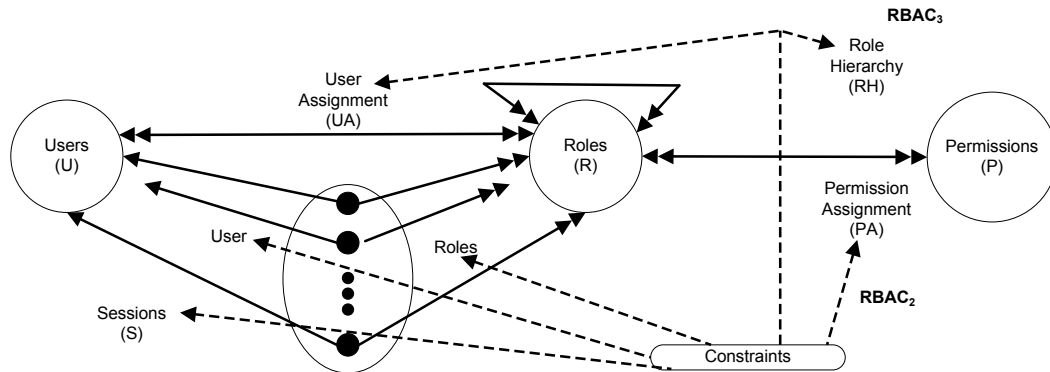


Figure 2: Role-based Access Control Models (Sandhu et al., 1996)

role. There is no presence term currently that maps to a role, but this paper suggests that the concepts of roles should be embraced in the processing and access control of presence information

**Permission:** A permission is said to be an authorization to a mode of access to a resource. Permissions can be equated to the components that comprise a presence authorization rule. Each rule contains conditions, actions and transformations for the purpose of controlling the presence information received by a watcher (Rosenberg, 2006). Conditions control when a particular rule is to be enforced, whilst actions outline the response a presence server should make to a watcher subscription request (Rosenberg, 2006). Transformations provide a filtering mechanism allowing presence data to be manipulated before being presented to the watcher (Rosenberg, 2006).

**Session:** A session provides the mapping between a user and an activated subset of the set of roles to which he is assigned. We believe that in presence processing a session will relate to the period of time during which a watcher presence document is generated. It is at this time that the subset of roles to which a watcher belongs would dictate the privacy filtering operation.

We will now proceed with the introduction of our enhanced presence processing model.

*Table 1: Overview of the PH-model development*

Model Progression	Administration	Processing
$PH_0$	watcher-based presence	presence filtering
$PH_1$	role-based presence	watcher-to-role mapping
$PH_2$	availability profiles	availability filtering

## 5 PROPOSED MODEL

Our enhanced presence processing model will be developed in progressive stages as shown in table 1. Each stage shall be discussed thoroughly and any shortcomings highlighted. These shortcomings will provide impetus for the next stage of our model's development. Initially,  $PH_0$  will be constructed by inheriting the key functionality of the presence handling model of Rosenberg (2005).  $PH_0$  will be formalized and considered as a watcher-based presence handling model.

The next step will be to modify  $PH_0$  with the addition of role-based concepts as presented in the RBAC specification by Sandhu et al. (1996). This second step will elevate  $PH_0$  to a role-based presence processing model ( $PH_1$ ).

The final stage,  $PH_2$ , will add the concept of an *availability profile* to  $PH_1$ . The purpose of  $PH_2$  is to improve the presentity's ability to better handle incoming messages from watchers.

### 5.1 $PH_0$ : Watcher-based Presence

The presence handling model,  $PH_0$ , now proposed, is strongly based on the Rosenberg-model (Rosenberg, 2005). This model provides much more detail than is relevant for the purposes of the  $PH_0$  model and therefore only the essential components and processes have been retained to form  $PH_0$ .

The Rosenberg-model provides for the filtering of sensitive presence information on a per-watcher basis. While not widely implemented, the Rosenberg-model is considered the status quo in a SIP/SIMPLE environment.

Figure 3 shows an architectural view of the  $PH_0$  model, adapted from the more detailed model as represented in figure 1. Figure 3 describes the most crucial part of the Rosenberg-model, namely presence filtering on a per-watcher basis.

There are three basic concepts in the  $PH_0$  model namely, watchers, presence, and subscriptions. These can be formalized as follows:

### Enhanced Presence Handling

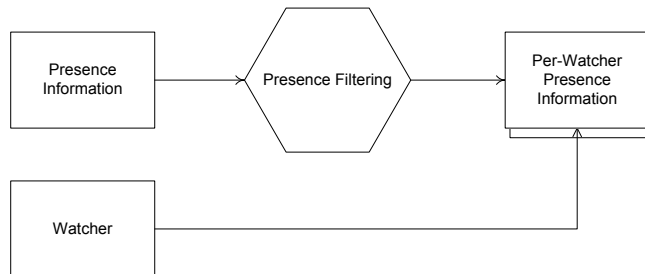


Figure 3: Architectural view of  $PH_0$ , adapted from the Rosenberg-model

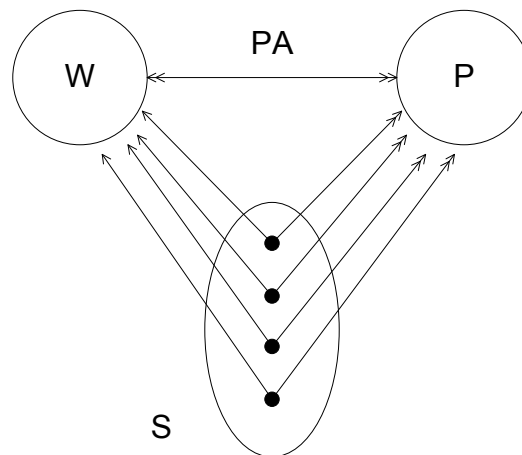


Figure 4: Graphical view of  $PH_0$

- $W$ ,  $P$ , and  $S$  representing watchers, presence attributes, and subscriptions; and
- $PA \subseteq P \times W$  representing presence-watcher assignments.

A graphical view of  $PH_0$  is given in figure 4 and shows that presence is directly associated with watchers in a many-to-many relationship. In figure 4 this relationship is represented by a double-headed arrow between the watchers and presence entities. In other words, a watcher can have access to various presence attributes, and every presence attribute can be provided to many watchers. The formalization of this processing can be represented as follows:

- *watcher* :  $S \rightarrow W$  a function mapping each subscription  $s_i$  to a single watcher  $watcher(s_i)$ ; and
- *presence attribute*:  $S \rightarrow 2^P$  where each subscription  $s_i$  is mapped to a set of presence attributes where  $presence\ attributes(s_i) \subseteq \{p \mid (p, watcher(s_i)) \in PA\}$ .

A watcher obtains a subscription for a presentity's presence information after authorization by the presentity. Thus, every presence subscription is associated with only one watcher. For the duration of the subscription, the watcher is mapped to a set of presence attributes. Every presence attribute to be provided to a watcher needs to be authorized in the presence policy. Access to all other attributes is implicitly denied.

The processing of  $PH_0$  comprises *presence information*, *presence filtering*, *per-watcher presence information*, *watcher filtering* and *watchers*. The Presence Information component maps to grouping A on the Rosenberg-model which details the composition of the current set of presence information in a presence document.

The Presence Filtering activity enforces permission-assignments and maps to grouping B on the Rosenberg-model i.e. the filtering process as being governed by presence authorization rules.

The  $PH_0$  model addresses the one-for-all approach to handling watchers by virtue of its per-watcher filtering. However fundamental flaws still exist namely, (a) undue burden is placed on the presence server in the generation of presence documents and (b) undue burden is placed on the presentity in creating authorization rules for each watcher. This leads us to the next stage of our model's development which incorporates RBAC principles.

## 5.2 $PH_1$ : Role-based Presence

In the Role-Based Access Control (RBAC) model, users are associated with roles, and roles with permissions. The mapping of RBAC concepts to those of  $PH_1$  was shown in section 4. Therefore, the addition of role-based concepts to  $PH_0$  can be formalized by drawing on the formalization of the RBAC model.

The most notable change in  $PH_1$  from  $PH_0$  is the introduction of roles. Roles are defined by Sandhu et al. (1996) as a set of permissions. Similarly, a role in  $PH_1$  is defined as a set of presence attributes. In  $PH_0$  such presence



## Enhanced Presence Handling

attributes are assigned directly to a watcher with a subscription. In contrast, a presence attribute is assigned to a role in  $PH_1$ .

Ferraiolo and Kuhn (1992) state that the concept of roles stems from the realization that in an enterprise control is governed by an employee's role and function. Similarly a presentity behaves differently, based on the identity of the watcher. In  $PH_0$  the control of presence information is aligned with this behavior. However, as the number of watchers increase, it is not feasible for the presentity to maintain distinct per-watcher handling. Therefore,  $PH_1$  introduces roles to group watchers according to their "role and function" (Ferraiolo & Kuhn, 1992) with regards to the presentity. In other words, a watcher is organized according to the relationship that the presentity has with that watcher.

The architectural view of  $PH_1$  is given in figure 5. The diagram shows that instead of a watcher directly accessing presence information, the watcher is first mapped to a role. The  $PH_1$  concepts can be formalized as follows:

- $W$ ,  $P$ , and  $S$  are unmodified from  $PH_0$ ;
- $R$  and  $WA$  are added, representing roles and watcher-to-role assignments respectively;
- $WA \subseteq W \times R$ ;
- $PA$  is modified from  $PH_0$  to contain presence attribute-to-role mappings where  $PA \subseteq P \times R$ .

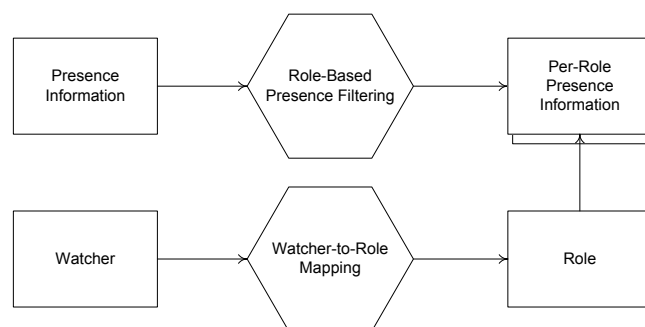


Figure 5: Architectural view of  $PH_1$

Figure 6 graphically depicts the specifics of the  $PH_1$  model. The figure shows that a watcher can be assigned multiple roles, and that a role may be

assigned many watchers. If a watcher activates several roles during the same subscription, scenarios are likely where multiple roles can cause conflicts in the sets of presence information approved for a watcher. The same issue exists on per-watcher filtering of presence such as in  $PH_0$ . This issue has been addressed in the IETF specification on *expressing privacy policy* (RFC 4745) but the resolution is implementation specific. Therefore, the issue need not be addressed by  $PH_1$ .

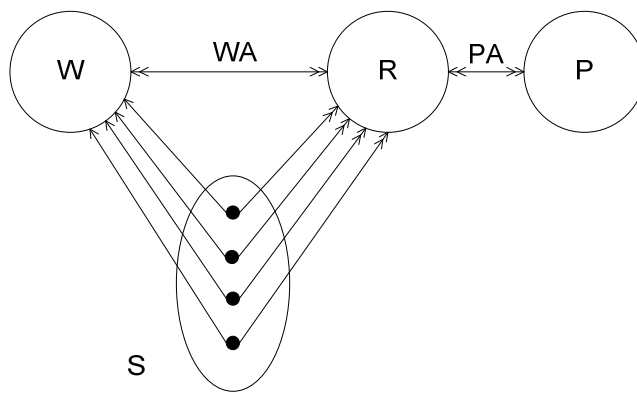


Figure 6: Graphical view of  $PH_1$

The processing specific details of  $PH_1$  can be formalized as follows:

- $roles : S \rightarrow 2^R$  where
- each subscription  $s_i$  is mapped to a set of roles  $roles(s_i) \subseteq \{r \mid (watcher(s_i), r) \in WA\}$  and
- subscription  $s_i$  has the set of presence attributes  $\cup_{r \in roles(s_i)} \{p \in (p, r) \in PA\}$ .

The application of roles to  $PH_0$  results in an improved, role-based presence handling model. It provides a presentity significant advantages in scalability and management of watchers. Furthermore, the presence server need only process presence information for the set of roles as opposed to for each watcher.

However, a presentity's presence information is in a state of flux, continuously changing and updated. In contrast, a subscription does not change as often. A distinction must be made between the presence attributes a watcher

is authorized to view within a subscription, and the actual values of the received presence attributes. The latter may change during the lifetime of a subscription. Thus while  $PH_1$  provides role-based filtering of presence information it still does not fully take into account the needs of the presentity. Such needs are catered for by the third stage of the enhanced model.

### 5.3 $PH_2$ : Availability Profiles

The low cost of sending messages via a wide range of communication channels, combined with the Internet facilitating constant connectedness, increases the chances of being disturbed, especially in the workplace.

If a presentity conveys his/her presence state as “busy”, a watcher may interpret that it is not currently the best time to initiate an interaction and spare the presentity the possible interruption. The problem with providing a presence state such as “busy” to watchers, is the total reliance on the watchers’ interpretation or consideration of such information. Although the presentity implies availability and willingness with a presence state, it is not enforced on the presentity’s side of the interaction. The concept of *availability profiles (AP)* provides such a mechanism.

An architectural view of  $PH_2$  can be seen in figure 7. The diagram shows that  $PH_1$  has been extended with the addition of an availability filter connecting the watcher (W) and presentity (Pr). The input to the availability filter from the watcher-side is the presence information provided to the watcher. In particular, the presented availability information, as embedded in the presence state, is of concern. The availability filter is used to provide the presentity with an availability profile with which incoming communication from a particular watcher is handled.

An availability profile can be defined as the availability and responsiveness with which any incoming communication is handled. The purpose of an availability profile is to help the presentity handle incoming communication with the appropriate amount of responsiveness. Responsiveness in the context of our use can be viewed as *demonstrated availability*.

The  $PH_2$  model can be defined as follows:

- $PH_2$  is unmodified from  $PH_1$  except for the addition of availability profiles (AP).
- An availability profile defines how to handle an incoming watcher-message based on the availability-related presence information provided

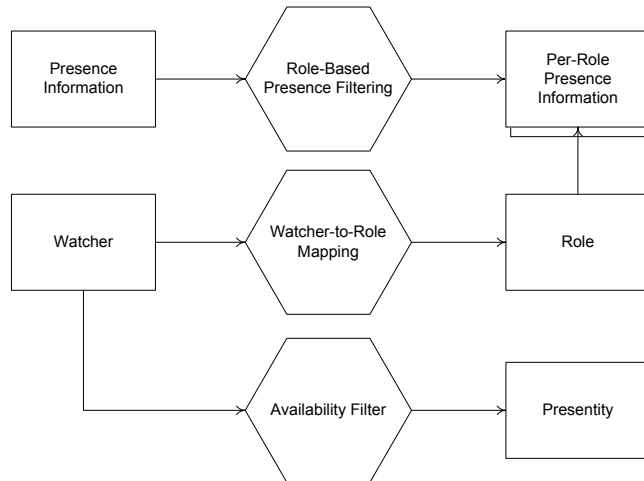


Figure 7: Architectural view of  $PH_2$

to that watcher.

The processing of  $PH_2$  extends  $PH_1$  as shown in figure 8. The model does not specify how an availability profile is to be implemented. However, it can be likened to a real-life working environment where person A is working in his office. If person B enters the office unannounced, it may cause interruption even without communication. However, if person B leaves a note in front of the office, person A will be spared the interruption.

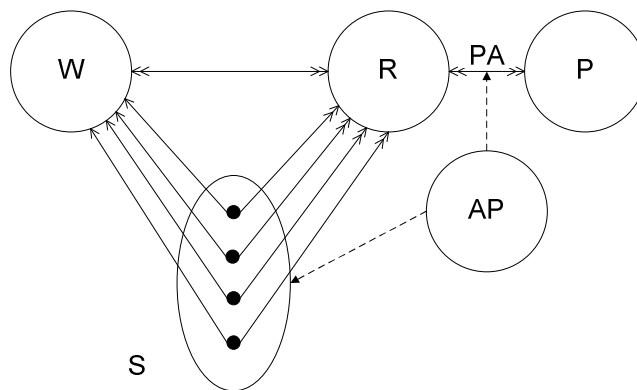
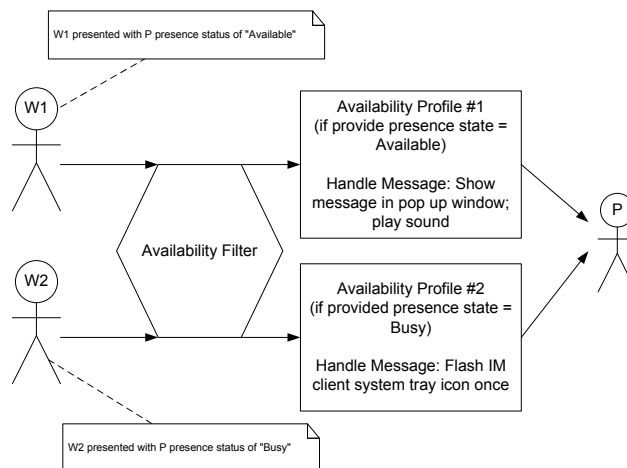


Figure 8: Graphical view of  $PH_2$

## Enhanced Presence Handling

In the example, it can be said that person A presented a presence state of “busy” to all. However, the door was not locked, leaving potential for handling emergencies as well as the potential of unwanted interruptions. An availability profile can be likened to the process of locking the door and providing the key to a specific set of people. The people that have keys, will be able to enter person A’s office, implying high availability. Similarly, to the people without keys, person A can be seen as busy but can be reached by leaving a message at the door. An availability profile can thus help person A to demonstrate the appropriate amount of availability.

The availability filter uses the set of presence information as authorized by the presence-assignments of the watcher within a subscription to produce an availability profile as mentioned in the specification section. Furthermore, the availability profile may modify presence information regarding availability before it is presented to the watcher. This association between the availability profile and presence-assignments is indicated with a broken-line arrow in figure 8. Availability profiles can be likened to constraints in RBAC in that both can limit values. However, availability profiles can modify actual presence attributes and also describe watcher message handling behavior on the presentity’s side, none of which can be achieved with RBAC constraints.



*Figure 9: Example of PH<sub>2</sub> potential implementation*

In the  $PH_2$  model an availability profile is associated with a subscription, and with a watcher through implication. In more general terms, as long as a watcher is provided presence information within a certain combination of

authorizations, communication from the watcher will be treated in a certain way. One such implementation possibility is to associate the availability profile with the presented presence state. Furthermore, the availability profile can then use the presented presence state to handle incoming communication with a certain salience. Figure 9 illustrates such an implementation example in an IM environment. The background to figure 9 is that watcher W1, and watcher W2 are communicating with presentity P. The figure shows that different presence states have been presented to each watcher, i.e. “Available” to W1 and “Busy” to W2. The availability profiles (AP1 and AP2) handle incoming messages based on the presented presence state of P. AP1 allows a watcher’s message to be displayed saliently in the form of a pop up window and a sound alert if the presented presence state is “Available” (indicating high availability). Similarly, AP2 handles incoming messages to watchers that were presented with a presence status of “Busy”. Therefore messages from W2 will be handled inconspicuously by only flashing the IM client icon in the system tray once. The end result is that the presentity is helped in demonstrating the right amount of availability through the level of salience with which the message is displayed.

## 6 CONCLUSION

The Internet and modern mobile/cellular networks have enabled ubiquitous communications for millions of people worldwide. However, a drawback to the power of these technologies is the problem of uncontrolled and unwanted disturbances.

Inadvertent interruptions can often be attributed to a lack of knowledge regarding the current availability for communications of a person. The presence status of a person can provide valuable cues in this regard. However, such information can be highly sensitive and private, and must be distributed in a secure manner. By using an RBAC model we have shown how this can be achieved in an efficient and manageable manner. However, issues still remain. A user might have quite a number of contacts and people he/she interacts with. Automating the process of role and permission assignment is an important factor in making such a model usable and appealing. We envision the use of artificial intelligence to learn from user behaviour, and assist the user in automating and managing access control, as an important area for future work.

## References

- Carroll, J. M., Neale, D. C., Isenhour, P. L., Rosson, M. B., & McCrickard, D. S. (2003). Notification and awareness: synchronizing task-oriented collaborative activity. *International Journal of Human-Computer Studies*, 58(5), 605–632.
- Day, M., Rosenberg, J., & Sugano, H. (2000). *RFC 2778: A Model for Presence and Instant Messaging*. Internet Engineering Task Force. (Available from: <http://www.ietf.org/rfc/rfc2778.txt>)
- Ferraiolo, D. F., & Kuhn, D. R. (1992). Role Based Access Control. In *15th National Computer Security Conference* (pp. 554–563).
- Jett, Q. R., & George, J. (2003). Work interrupted: A closer look at the role of interruptions in organizational life. *Academy of Management Review*, 28(3), 494–507.
- Ljungstrand, P. (2001). Context Awareness and Mobile Phones. *Personal and Ubiquitous Computing*, 5(1), 58–61.
- Markus, M. L. (1994). Finding a happy medium: explaining the negative effects of electronic communication on social life at work. *ACM Transactions on Information Systems*, 12(2), 119–149.
- McCrickard, D. S., Catrambone, R., Chewar, C. M., & Stasko, J. T. (2003). Establishing tradeoffs that leverage attention for utility: empirically evaluating information display in notification systems. *International Journal of Human-Computer Studies*, 58(5), 547–582.
- O’Conaill, B., & Frohlich, D. (1995). Timespace in the workplace: dealing with interruptions. In *Chi ’95: Conference companion on human factors in computing systems* (pp. 262–263). ACM Press.
- Rennecker, J., & Godwin, L. (2005). Delays and interruptions: A self-perpetuating paradox of communication technology use. *Information and Organization*, 15(3), 247–266.
- Roach, A. (2002). *RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification*. Internet Engineering Task Force. (Available from: <http://www.ietf.org/rfc/rfc3265.txt>)

Proceedings of ISSA 2009

- Rosenberg, J. (2005). *A Processing Model for Presence* (Internet Draft). Internet Engineering Task Force.
- Rosenberg, J. (2006). *A document format for expressing privacy preferences* (Internet-Draft No. Version 05). Internet Engineering Task Force.
- Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., & Schooler, E. (2002). *RFC 3261: SIP: Session Initiation Protocol*. Internet Engineering Task Force. (Available from: <http://www.ietf.org/rfc/rfc3261.txt>)
- Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-Based Access Control Models. *IEEE Computer*, 29(2), 38–47.
- Sonnenwald, D. H., Maglaughlin, K. L., & Whitton, M. C. (2004). Designing to support situation awareness across distances: an example from a scientific collaboratory. *Information Processing & Management*, 40(6), 989–1011.



Too Many Laws but Very Little Progress! Is South African  
Highly Acclaimed Information Security Legislation Redundant?

**TOO MANY LAWS BUT VERY LITTLE PROGRESS!**  
**IS SOUTH AFRICAN HIGHLY ACCLAIMED**  
**INFORMATION SECURITY LEGISLATION**  
**REDUNDANT?**

**<sup>1</sup>R Dagada, <sup>2</sup>MM Eloff, <sup>3</sup>LM Venter**

<sup>1</sup>University of the Witwatersrand, <sup>2</sup>University of South Africa, <sup>3</sup>SAP /Meraka  
UTD and University of South Africa

[<sup>1</sup>Rabelani.Dagada@wits.ac.za](mailto:Rabelani.Dagada@wits.ac.za)

[<sup>2</sup>eloffmm@unisa.ac.za](mailto:eloffmm@unisa.ac.za)

[<sup>3</sup>Lucas.venter@sap.com](mailto:Lucas.venter@sap.com)

**ABSTRACT**

South Africa has myriad laws that address information security related issues. One such law is the Electronic Communications and Transactions Act of 2002 (ECTA), which is highly regarded internationally. A study, which forms the basis of this paper, found that not all provisions of this legislation that deal with information security are implemented by both the government and information security practitioners in corporate South Africa. The study found that the South African government has a relaxed approach to implementing some of the legal provisions regarding information security. The ECT Act agitates for the appointment of cyber inspectors who have powers to inspect, search and seize. A magistrate or a judge may issue a warrant requested by the cyber inspector. Although the legislation had good intentions, the government has not yet appointed the cyber inspectors. Although the ECT Act was in part intended to curb the spam emails, the effect of the Act is practically very little. The study also found that some of the information security laws are ambiguous, for example, the Patent Act. Some of the laws pertaining to information security are very old; they were in effect introduced

Proceedings of ISSA 2009

before the Internet was used for commercial purposes. These include the Merchandise Marks Act of 1941 and Copyright Act of 1978.

The findings of this study reflect that information security practitioners were not really familiar with the avalanche of information security related legislation. Be that as it may, the contents of the IT policies from some of the organisations that participated in this study contain the provisions of legislation were catered for in the policies. This should be attributed to the fact that although information security practitioners were not consciously trying to comply with legislation, they relied heavily on the international standards. Most of these standards are in line with the requirements of the South African information security related legislation. In other words, corporate information security policies are within the framework of the Constitution of the Republic and the applicable legislation by default. They are not consistent with constitutional and legislative provisions by conscious effort on the part of the information security practitioners. It is in this premise that this study contains a concept model for legal compliance for information security at the corporate environment. This model embodies the contribution of the study.

#### KEYWORDS

Information Security, Legislative Compliance, Information Security Policies, Model for Legal Compliance

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

### 1 INTRODUCTION

Most organisations around the world as well as in South Africa have developed web sites for information and business related purposes. Some of these Websites merely display information about the organisation, whilst others offer some interactivity with customers. The Internet revolution is developing rapidly due to electronic commerce (e-commerce) (Mattord, 2007; Plotkin & Fagan, 2003). It is on this premise that most organisations are striving to catch up. De Kare-Silver (2001) and (Irwin, Yu, & Winsborough, 2008) noted that it is a daunting task for organisations to master the new environment. He puts it this way: “There is a new game in town and it is now about learning and embracing the new factors for success.” However, ‘the new game in town’ has brought with it a number of challenges. According to Chorafas (2001), the challenges brought by the Internet to the corporate environment include information security risks, threats and crime. The bottom line is that rapid development of technology has an impact on business systems. Negative forces of technology on businesses should be managed.

Negative challenges brought on by technology do not affect corporate actors only. Other constituencies of business, particularly clients, are affected by the growth and diffusion of technology in business. Increasingly, clients have to conduct transactions on the Internet, receive advice from Websites, and interact with business online. The new culture, e-market, raises questions of security and trust. Chorafas (2001) claims that security is e-commerce’s Achilles heel. Dugan, Egan, Kraus & Hancock (2003) report that the business-to-consumer component of e-commerce may be affected by reservations regarding security breaches. On the other hand, the credit card is the most common online payment option and thus both e-commerce customers and merchants are vulnerable to potentially high levels of fraud due to stolen cards and illegally acquired card numbers (Boynton, 2007; Chorafas, 2001:250). Although new technical measures are being established to deal with online fraud, these techniques are not necessarily infallible; a perfect method of encrypting has not yet been developed (Bond, 2002:189). It is on

this premise that information security measures cannot be left to technical methods only (Bond, 2002:188).

The remainder of the paper is structured as follows – literature review, the research problem, the research methodology, findings of the study, concept model of legal compliance for information security at the corporate environment, and conclusion. For the purpose of this paper, the words Information and Communications Technologies (ICT), and Information Technology (IT) will be used synonymously.

## **2. LITERATURE REVIEW: A BRIEF OVERVIEW**

The literature review a brief overview of the issues that are related to e-commerce, information security threats, risks and crime, and legal and policy aspects of information security. It also provides a brief legal framework of cyberlaw in the South African context.

### **2.1 Information security risks, threats and crime**

The introduction mentioned the importance of using information resources. Whilst information resources are essential in participating in e-commerce and the information economy, they are not exempt from risks, threats and crime (Vorster & Labuschagne, 2005; Targowski, 2003). It is therefore advisable for any organisation that uses information resources to have the necessary information security (Gupta, Chandrashekhar, Sabnis & Bastry, 2007; Collin, 1997). Information security provides e-commerce merchants and consumers with the safety and the sense of freedom from risks, threats and crime. Feiler (2000) observes that in e-commerce four different places are involved, that is - the location of the user, the location of the Web server, the location of the Web owner and the virtual location of the site, and thus information security is an essential concern. Privacy is one of the challenges regarding information security (Tondel, Jaatun & Meland, 2008; Lobree, 2001). This, according to Chorafas (2001), is a major problem to any financial transaction in the e-commerce environment.

The processing of e-commerce transactions raises the issue of information security. Windham (1999) reports that during the early era of e-

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

commerce, the Internet was generally regarded to be an unprotected medium. This perception, rightfully so, continues to persist. News of hackers and online fraudsters made headlines and led to fear amongst millions of potential electronic shoppers. They thought the Internet was not a secure environment to provide confidential information. This, according to Windham (1999), held the information economy back from even earlier advancement. Viruses and other forms of hostile code (malware) are universally experienced as an information security problem. The infection rate continues to grow and this affects the e-commerce participants negatively (Champlain, 1998; Tirado, 2008). Heiser (2001) reports that malware has the ability to penetrate firewalls, hijack Virtual Private Networks and also defeat digital signatures. Aggressive code is the most well known source of security lapse. Heiser (2001) lists several examples of malware. These include worms, Trojan horses and macro viruses. In view of these concerns information security is crucial in the business environment. Below is a discussion on policy aspects to be considered for information security.

### **2.2 Policy aspects to consider when providing information security**

It was mentioned in the previous section that some organisations post their information security policies on their Websites. This demonstrates corporate diligence in explaining their commitment to online business security. It was also stated that these policies deal with issues such as the usage of credit cards and other personal data. Windham (1999) provides an example of how America Online posts a privacy policy on its Website regarding the kind of information it collects about people who visit its Website. America Online also explains what it does or does not do with the collected personal data. Tudor (2001) reports that information security policy is formulated to inform all individuals who operate within an organisation regarding how they should conduct themselves when it comes to ICT information security issues. In some instances policies are formulated because of regulatory requirements (Turner, 2000; Irwin, Yu & Winsborough, 2008). Developing information security policies just for the sake of satisfying regulatory obligation is not good enough (Myers & Riela, 2008; Tudor, 2001). Information security policy is used as a communication tool amongst the information system

stakeholders (Champlain, 1998). Turner (2000:191) declared that the advancement of the information economy in terms of the e-commerce rapid growth puts an obligation on government and organisations to develop information security policies and regulatory solutions. During this era of the information economy, information security policies will assist in providing users with security and privacy certainty (Champlain, 1998; Bhilare, Ramani & Tanwani, 2009). Turner (2001) notes that the differences in policy approaches amongst key role players and countries make it difficult to provide a better information security policy and regulatory framework. Although this difficulty takes place at macro level, it manifests itself at micro (organisational) level. Whilst these can be regarded as generic policy aspects, below is a South African legal framework on e-commerce and information security.

### **2.3 Legal framework of e-commerce and information security in South Africa**

There has been rapid use of e-commerce in South Africa; hence the need to develop legislation that would provide security to Internet consumers and merchants (Dunlop, 2005). *South African common law* was not sufficiently addressing issues related to the security of electronic transactions (Goodburn & Ngoye, 2004). According to Dunlop (2005), the South African government did not confine its concern just to information security, but intended to provide a legal framework that would address security, transparency and infrastructural commercial development (Hofman et al. 1999). The e-commerce initiatives that are based on a sound legal framework would enable South Africa to become a leading technology power in the African continent (Dunlop, 2005). It is on this basis that the *South African Department of Communications* established an ICT investment cluster in May 1998 to create a legislative framework on issues relating to e-commerce and information security (Groenewald, 2000). For focus purposes, the following is the research problem.

### **3. THE RESEARCH PROBLEM**

Legal and policy aspects are important in the provision of information security. Although several authors have written about legal and policy

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

aspects regarding information security in the South African context, none of them has explained how these aspects are used in the provision of information security in the South African corporate environment. The question arises as to whether the *Constitution of the Republic* (1996), the *Electronic Communications and Transactions Act* of 2002 (2002), the *King 2 Report* (2002) and other information security related legislation at macro level and the organisations' policies are used by South African organisations in their endeavours to protect their information resources.

Both the 2002 and 2004 website compliance surveys in South Africa “painted a bleak picture of non-compliance and general indifference towards laws and regulations governing websites and the online sale of goods and services in South Africa” (Buys Incorporated Attorneys, 2004). In 2002 26% of South African website operators claimed that they were not aware of the compliance requirements. It is astonishing to note that this number increased in 2004 by 5% to 31% (Buys Incorporated Attorneys, 2004).

The failure to comply with the law, according to Buys Incorporated Attorneys (2004), has led to an increase in website crime: “During March 2002, a defamatory statement posted to the website of *Kick-Off* magazine, ended in the High Court. A month later the *Department of Health* investigated an illegal online pharmacy in Table View and in June of the same year, the *Gauteng Metro Police* attempted to close down a website that warned motorists of speed traps around Johannesburg.” The problem is exacerbated by the fact that most South African companies do not comply with the requirements of Chapter 7 and Part III of Chapter 3 of the ECT Act. They do not seem to realise that failure to comply with the provisions of the law exposes their websites to huge risk and liability. Of the 1 550 websites surveyed by Buys Incorporated Attorneys (2004), the Telkom website ([www.telkom.co.za](http://www.telkom.co.za)) was the only one to score a full 100% compliance rate.

Other than the aforesaid website compliance survey conducted by the Buys Incorporated Attorneys in 2002 and 2004, it appears there had never been any substantial study that focuses on the compliance of information security related legislation by organisations in South Africa. Moreover, it remains to be established whether the existing company policies are in line with the national and international legal regime. The lack of results with

regard to consideration of legal and policy aspects in the South African corporate environment seems to indicate the need for research in this field. There is a gap in the literature as to how information security legal policy and legislation add value to the corporate environment within the South African corporate context. The literature does not show if South African organisations are complying with the national legal and policy framework regarding information security.

Within this context, following questions are posed:

- How are South African companies employing legal and policy prescriptions to enhance information security?
- To what extent do the South African legislation impacts on the endeavours to curb information security related problems? and
- To what extent are organisations in the South African integrating information security legal requirements into their policy formulation and implementation?

### **3.1 Sampling and profile of the organisations**

Twenty-two organisations participated in this study. These organisations are from different industrial sectors. These include IT, telecommunications, mining, services, academia and research, regulatory authorities, public administration, construction, insurance, and banking sectors. It is important to mention that the banking sector dominated all other industrial sectors. This is because the four biggest banks in South Africa – namely Standard bank, First National Bank, Amalgamated Banks of South Africa, participated in this study. In addition to the aforesaid organisations, three organisations (IT governance consultancy and two law firms) were involved. Purpose sampling was employed since the participating organisations were purposefully selected due to the contribution they would add to the study.

### **3.2 Data collection and analysis**

This study used the generic techniques for qualitative data collection and analysis. This study satisfied the principle of triangulation by employing multiple data-gathering methods and sources. Data gathering methods include individual interviews, key informant interviews, observation, and policy documents analysis. Interview protocols for both the individual and



## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

key informant interviews were semi-structured. Interviews were analysed by using open coding. A frequent comparative method was applied to analyse data within and between interviews. Content analysis was applied to analyse the content of interviews. The process involved the instantaneous coding of raw data and the construction of categories. Data collected through document analysis was analysed by comparing it with the South African legal framework pertaining to information security.

### **4. FINDINGS OF THE STUDY**

This section addresses findings that were obtained through interviews, documents analysis, and observation.

#### **4.1 Findings obtained through interview**

##### **4.1.1 The Board of Directors are not involved in the formulation of information security policies**

This study found that the involvement of the Board of Directors in the establishment of the information security policies is very minimal or non-existence. This is in conflict with the spirit of good cooperate governance as espoused by the King II and Draft King Reports. This was confirmed by a Senior Lecturer at a South African university, an expert in information security law: *“King III will have more IT governance provisions. IT governance and security will become the responsibility of the Board of Directors. According to the Draft King III, IT security is an important element of the overall business efficiency and sustainability.”* This study found that policies in all 22 organisations that participated in this study are actually approved at the Chief Information Officer’s (CIO) level. The CIO would convene an ICT Steering Committee which is constituted by representatives from various departments. The problem is that most of these representatives are actually not really senior. This shows that most organisations do not take information security seriously. However in the Draft King III Report, information security policies should be approved by the Board and that the IT Steering Committee should be chaired by the Chief Executive Officer (CEO) and *“all Group Executives are expected to serve in the IT Steering Committee.”* Therefore, flouting this provision demonstrates deviance from compliance requirement.

#### **4.1.2 Very few organisations in South Africa incorporates legislation requirements in the information security policies**

Legislation in South Africa has a lot of impact in policy formulation. A certain information security legal expert had observed that: *“The problem is that very few IT security experts and practitioners are conscious about this. Technology people are more familiar with the standards; unfortunately there is myriad of legislation and governance internationally and in South Africa.”* In South Africa, one of the crucial pieces of legislation is the Electronic Communications and Transactions Act of 2002. This Act deals with the removal of legal barriers to electronic transactions and provides security framework for both the merchants and buyers. The legal expert continued: *“You would expect most information security practitioners to be familiar with sections that deal with security related aspects in this Act, but unfortunately very few security experts and practitioners incorporate the Act’s security requirements in the IT policies. I really think this is highly irregular because it exposes consumers who use websites of the companies that are not integrating the requirements of the Act for e-commerce purposes.”* A Johannesburg-based Managing Director of the IT legal firm concurred: *“One of the observations that I have made is that people buy batches of the policies and they do ISO compliance, for instance ‘2700’ and they will immediately implement those policies rather than drafting the policies based on legislation.”* Most IT departments are aware that they should have information security policies but they do not have the awareness to actually make the policies relevant to them, *“they’d rather purchase just broad generated policies and apply those.”* This means that corporate security executives are not diligent in the execution of security mandate. In addition, they are lax, lack commitment and are characterised by unprofessional demeanour. This account of security professionals and approach to their vocation permeated overwhelmingly during the data collection stage.

During an interview with the Information Security Officer of an agency which provides IT services to the whole provincial government, she indicated that legal department or outside lawyers were not involved in four of their information security related policies and there was no effort to ensure that

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

these policies integrate the legislation requirements. However, she emphasised that the drafting of their Records Management Policy and Data Retention Schedule is guided by the legal requirements. An Information Security Manager in one of the biggest mobile telecommunications network in South Africa and the African continent, confirmed that when the IT department drafts the security policies they “*don’t consciously look at the legislation and try and mend that scientifically against, for example, the Promotion of Access to Information Act.*” However, interestingly they “*relied on the legal department to do that and I think to some extent they did review that and made sure that it was compliant to legislation.*”

### **4.1.3 Legal provisions to fight cyber crime are redundant**

Some of the South African information legal information security provisions were highly acclaimed when they were introduced, but unfortunately they are not yet implemented. These include provisions to prevent viruses, hacking, and industrial espionage. Provisions to fight against the aforesaid IT related crimes are contained in Chapter 8 of the ECT Act of 2002. Hacking, industrial espionage, viruses, spam emails and other cyber related crimes are characterised by an unauthorised access to, interception of or interference with data and thus they are supposed to be tackled by cyber inspectors. A Senior Lecturer who specialises in information security law said the provision for the cyber cops is: “*Articulated in Chapter 12 of the Electronic Communications and Transactions Act.*” It is unfortunate that this provision has not yet been implemented even though the Act was passed more seven years ago.

After realising that cell phones were contributing to the commission of criminal activities, law makers in South Africa established the ‘Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002’. Amongst other things, this Act stipulates that the buyers of the pre-paid SIM cards should be registered by cell phones network operators so that the law enforcement agencies could identify them if and when their cell numbers are used to plan or to commit crime. A legal expert indicated that: “*the Department of Justice will announce a date in which the registration of the people who buy SIM cards commences. The delay in*

*implementing this requirement is not justifiable, especially when you consider the fact that the Act was passed in 2002.”*

Chapter 10 of the ECT Act agitates for the establishment of the Cryptography Providers. This is one of the legal measures to prevent IT related crimes. Cryptography concerns itself with the hiding of information. In an email communication the message would get encrypted and impossible to read by an intruder. The whole message will be gibberish. *“To date the Director General of Communications has not yet established a register of Cryptography Providers.”*

#### **4.1.4 Legal provision that deal with unsolicited communication has serious loophole**

Unsolicited emails, famously known as spam emails, are addressed in Chapter 7 of the Electronic Communications and Transactions Act of 2002. This Chapter of the aforesaid Act deals with consumer protection. The spam emails are dealt with in Clause 45 which prohibits unsolicited commercial communications to the consumers. However, during the interviews, interviewees indicated that this prohibition is not effective. Sellers of the goods, products and services are using a loophole in the Act to send chains of unsolicited messages to the consumers: *“The Act says the sender should give the recipient an option to cancel the subscription. However, consumers are ignorant and thus they are flooded with spam emails. In real essence, the first email that is sent is unsolicited, but it is legal because it gives the recipient an option to opt out. Usually, recipients don’t opt out and thus the subsequent emails cannot be defined as unsolicited because the consumer is deemed to have opted to receive the adverts since he did not opt out. This is entirely within the law.”* The problem is that most banking clients in South have received unsolicited emails which were attached with viruses and spyware.

#### **4.2 Findings obtained through document collection and analysis**

Information security related policies were collected from 16 of the 22 organisations that participated in this study. The collected policies were analysed against information security related legislation. It is important to state that only half of the 16 companies whose policies were analysed have integrated information security legal provisions into their policies. Two of the

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

eight companies that have integrated legislation in their policies had only incorporated legislation requirements in their Records Retention Schedules; the rest of their information security policies do not make any reference to any law. Paragraphs below provide results of the document analysis.

### **4.2.1 Policies regarding hacking**

Hacking has much to do with access control. This is addressed in our Information Security Policy, and Interception & Surveillance Policy. The relevant legislations are the Promotion of Access to Information Act; Electronic Communications and Transactions Act; and the Interception Act.

### **4.2.2 Policies regarding intellectual property, copyright, and trademarks**

Intellectual Property is gradually becoming an important asset amongst the South African companies. According to the information contained in the few collected policies, it includes assets such as, but not limited to – ‘websites content, website source code, software developed within a particular company, software developed by employees, product packaging, trademarks, domain names, marketing information, and the like’. Copyright is addressed by the Intellectual Property Policy. The objective of this policy is to formulate a framework for the establishment, protection, registration, maintenance, management and use of ICT Intellectual Property. This policy is applicable to all employees, third parties, external contractors, and ICT Intellectual Property related contracts entered into by employees acting on behalf of the organization. The relevant legislation is the Intellectual Property Law Amendment Act of 1997, Copyright Act of 1978, Merchandise Marks Act of 1941. The problem is that some of the aforementioned laws are very old and were introduced before the Internet was used for commercial purposes. Other relevant policies for the intellectual property, copyright and trademarks are the Information Security Policy and the Data Privacy Policy. It is a matter of extreme concern to note that the majority of the organizations that participated in this study do not have policies that address the protection of intellectual property, copyright and trademarks.

### 4.2.3 Policies regarding patents rights

None of the companies that participated in this study had a separate policy on patents. Actually, only three organizations addressed the patents protection as part of the intellectual property policy. The researcher concluded that this could be due to the fact that most companies that participated in this study perceive the South African patent law to be ineffective. According to the Patents Act of 1978, computer programmes cannot be patented; however, companies are patenting these programmes anyway. In other words, Companies and Intellectual Property Registration Office (CIPRO), an organ of the state responsible for patents registration – does not respect the Act responsible for patents.

### 4.3 Findings obtained through observation

The researcher investigated the websites of the 22 organizations that participated in this study. The purpose of the observation was to determine if the websites complied with the following information security legal requirements: availability of legal notice, terms and conditions available as hyperlinks, liability disclaimers available as hyperlinks, compliance with the provisions of Chapter 3, Part II and Chapter 7 of the Electronic Communications and Transactions Act, positioning and implementing legal notice correctly, availability of legal notice that is printable or saveable as required by section 11(3) of Electronic Communications and Transactions Act, and availability of policies that address websites legal compliance.

Table 1 below reflects the findings of the observation.

*Table 1: Number of organizations that are compliant with the legislation governing websites and e-commerce.*

ASPECT OBSERVED	NUMBER
Websites with legal notices at all	17
Websites with terms and conditions available as hyperlinks	7
Websites with liability disclaimers available as hyperlinks	11
Websites with legal notices that address the provisions of Chapter 3, Part II and Chapter 7 of the ECT Act	5
Websites that position and implement legal notices correctly	2
Website legal notices that are printable or saveable as required by section 11(3) of the ECT Act	2

Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

Organizations that have policies that address websites legal compliance	5
---	---

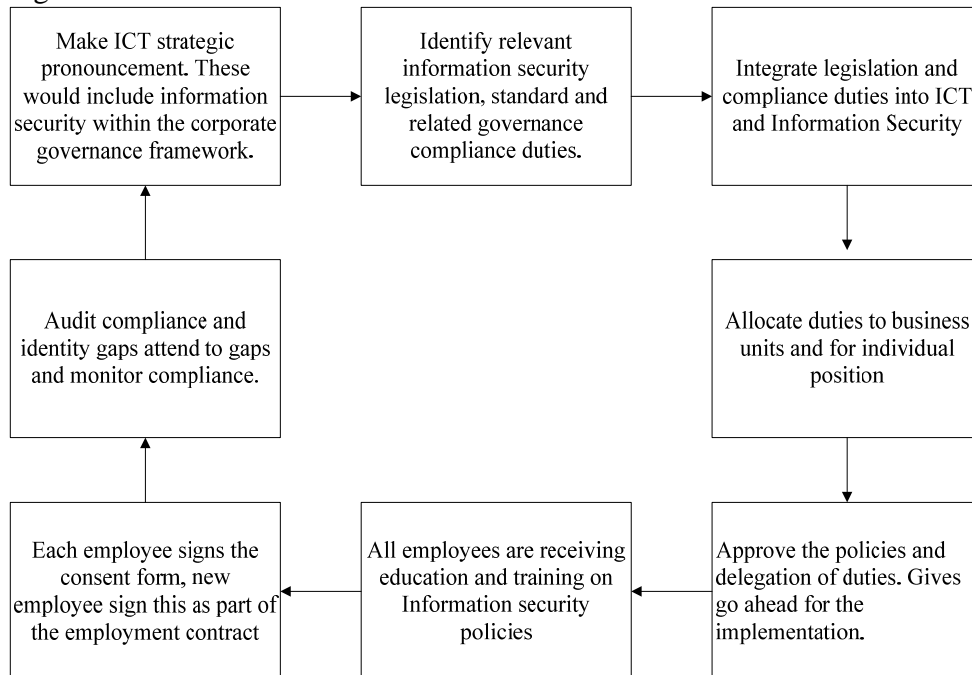
From Table 1 above, one deduces that most companies in South Africa are not complying with the legal requirements of the websites. This may expose the consumers to cyber crime during electronic transactions. It appears most IT and information security practitioners are not familiar with the requirements of the Electronic Communications and Transactions Act of 2002 regarding consumer protection. Although 17 out of 21 websites that were observed have legal notices, their legal notices are very elementary in nature. These legal notices, and/or ‘terms and conditions’ do not make provisions regarding some of the following legal requirements – ‘definitions and interpretation, allowed usage and license, intellectual property rights and domain name use, software and equipment, disclosures required by section 43 of the Electronic Communications and Transactions Act, changes and amendments, privacy, hyperlinks to third parties, security, disclaimer and limitation of liability, removal and correction of content, interception of communications, entire agreement and severability, agreement in terms of Section 21 of the Electronic Communications and Transactions Act, applicable and governing law, and legal costs’. Irrefutably, table 1 conclusively show limited, partial compliance. In some websites there is not attempt to comply with relevant policies at all.

**5. CONCEPT MODEL OF LEGAL COMPLIANCE FOR INFORMATION SECURITY AT THE CORPORATE ENVIRONMENT**

This section suggests a model whereby legal requirements are incorporated into the information security endeavours – policy formulation, implementation, and monitoring. This model is an intellectual property of the writers and can be seen as a synthesis of theory, practice and cognitive perspectives gained over the years of practical experience. The model was necessitated by the main finding of this study which reveals that both the government and corporate South Africa were not implementing some of the information security legal provisions. This model may be very useful to policy formulators, directors of the boards, ICT executives, and information



security practitioners. A graphic representation of the model reflected in Figure 1



*Figure 1: A concept of legal compliance for Information security policies formulation, implementation and multitasking.*

According to the Draft King III Report, IT strategic planning, risk management and information security is the primary responsibilities of the Board of Directors. One does not expect the Board to be involved in a detailed process regarding the formulation of the information security policies, but they should rather make broader pronouncements within the business strategic direction and sustainability, corporate governance, standards, and legislation framework. The Draft King III advises that there should be an ICT Steering Committee at the enterprise's executive level. This ICT Steering Committee will include all executives in the organisations and chaired by the CEO. It is the researchers' contention that relevant



## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

information security and related compliance duties should be identified at this level. Once this has been done, the next step will be the ICT Department.

The ICT Department is headed by the CIO. According the Draft King III Report, the CIO must be business oriented and must be an interface between IT and business. S/he would obviously serve in the ICT Steering Committee and thus s/he take the identified information security legal provisions and related compliance duties and translate them into information security policies. The drafted information security policies will then be taken by the CIO to the ICT Steering Committee for consideration and comment. The Steering Committee will allocate duties business units and/or individual positions. The policies will then be taken to the Board's Sub-Committee for Risk Management for approval. All employees will then be trained regarding the information security policies. They will also be asked to sign the acceptance forms. The Board's Sub-Committee on Risk Management will audit compliance and identify gaps. Thus, the overall intention of the model is to prioritise information security, elevate the profit of business security, and ultimately address corporate security lapses.

### **6. CONCLUSION**

There are more than ten laws that deal with information security in South Africa. The title of this paper poses a very thought proving question – are these laws effective enough in addressing information security challenges in corporate environment? The answer is no. Information security provisions that are contained in certain laws are not yet implemented. There is also a deliberate disregard of the information security legal provisions by some companies and the government entities. It was reported in this paper that most IT and information security practitioners were not familiar with the information security legal requirements. It is perhaps in this premise that most South African companies do not comply with the requirements of the law regarding information security related matters.

In some instances the attitude of the South African government towards its own laws has been lukewarm. The Electronic Communications and Transactions Act, 2002, agitate for the appointment of cyber inspectors who have powers to inspect, search and seize. A magistrate or a judge may issue a

warrant requested by the cyber inspector. Although the legislator had good intentions, the government has not yet appointed the cyber inspectors. This paper reported the confusion related to the legality of the software patents in this country. This matter should be brought to the attention of the legislators. Some of the laws pertaining to information security are very old; they were in effect introduced before the Internet was used for commercial purposes. These include the Merchandise Marks Act of 1941; Copyright Act of 1978; and the Patents Act of 1978. Having said all these, one would conclude that although information security and the legislation thereof do not reflect a perfect marriage; their marriage, with its imperfections, remains necessary.

## 7. REFERENCES

- Bagby, JW 2003: E-commerce law: issues for business. Ohio: Thomson.
- Bhilare, DS, Ramani, AK, & Tanwani, 2009: Information security assurance for academic institutions using role based security metric: an incremental approach. Proceedings of the International Conference on Advances in Computing, Communication and Control, pp 535-540, 23-24 January 2009. New York: ACM.
- Bond, R 2002: New economy equity: navigating security and legal issues in digital business. Worcester: John Wiley & Sons.
- Boynton, BC 2007: Identification of process improvement methodologies with application in information security. Proceedings of the 4<sup>th</sup> annual conference on information security curriculum development. New York: ACM.
- Buys, R 2004: 2004 South African website compliance survey results nothing to be proud of. Buys Inc. Attorneys/Legalsentry.
- Champlain, J 1998: Auditing information systems: a comprehensive reference guide. New York: John Wiley & Sons.
- Chorafas, DN 2001: The Internet supply chain: impact on accounting and logistics. New York: Palgrave.
- Collin, S 1997: doing business on the Internet. London: Kogan page
- Conkling, WR & Hamilton, JA 2008: The importance of information security spending: an economic approach. Proceedings of the 2008 spring simulation multiconference, pp 293-300. San Diego: The Society for Computer Simulation, International.
- De Kare-Silver, M 2001: E-shock: the new rules – Internet strategies for retailers and manufacturers. New York: Amacom.

## Too Many Laws but Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?

- Draft Report on Governance for South Africa, 2009. The Institute of Directors in Southern Africa and the King Committee in Corporate Governance. Johannesburg.
- Dugan, JC, Egan, EM, Kraus, AD & Hancock, EM 2003: Privacy & e-commerce in the United States. (In: Plotkin, ME, Wells, B & Wimmer, K eds. 2003: E-commerce law & business (Volume 1). New York: Aspen Publishers).
- Feiler, J 2000: Managing the web-based enterprise. London: Morgan Kaufman.
- Godburn, D & Ngoye, M 2004: privacy and the Internet (In: Buys R & Cronje, F eds. 2004: Cyberlaw: the law of the Internet in South Africa. Van Schaik Publishers, pp 97-112).
- Heiser, J 2001: An introduction to hostile code and its control (In: Tipton, HF & Krause, M eds. 2001: Information security management handbook. London Auerbach Publications, pp 475-495).
- Hofman, J, Johnston, D, Handa, S & Morgan, C 1999: Cyberlaw: a guide for South Africans doing business online. Cape Town: Ampersand.
- Irwin, K, Yu, T, & Winsborough, WH, 2008: Avoiding information leakage in security-policy-aware planning. Proceedings of the 7<sup>th</sup> ACM workshop on privacy in the electronic society, pp 85-94. New York: ACM.
- King Report on Corporate Governance for South Africa 2002. The Institute of Directors in Southern Africa and the King Committee in Corporate Governance. Johannesburg.
- Lobree, BA, 2001: E-mail security (In: Tipton, HF & Krause, M eds. 2001: Information security management handbook. London Auerbach Publications, pp 55-82).
- Martin, J 1996: Cybercorp: the new business revolution. New York: Amacom.
- Mattord, HJ, 2007: Rethinking risk-based information security. Proceedings of the 4<sup>th</sup> annual conference on information security curriculum development, 28-29 September 2007. New York: ACM.
- Merriam, SB 1998: Qualitative & case study applications in education. San Francisco: Jossey-Bass Publishers.
- Myers, JP, & Riela, S, 2008: Taming the diversity of information assurance & security. Journal of Computing Sciences in Colleges, 23(4), pp 173-179. Consortium for Computing Sciences in Colleges, USA.
- South Africa, 1941: Merchandise Marks Act. Pretoria: Department of Trade and Industry
- South Africa, 1978: Copyright Act 98. Pretoria: Department of Trade and Industry.
- South Africa, 1978: Patents Act No. 57. Pretoria: Department of Trade and Industry.

Proceedings of ISSA 2009

- South Africa, 1993: Trade Marks Act 194. Pretoria: Department of Trade and Industry.
- South Africa, 1997: Intellectual property laws amendment Act. Pretoria: Department of Trade and Industry.
- South Africa, 2000: Promotion of Access to Information Act. Pretoria: Department of Justice and Constitutional development.
- South Africa, 2002: Electronic Communications and Transactions Act. Pretoria: Department of Communications.
- Targowski, AS 2003: Electronic enterprise: strategy and architecture. Hershey: IRM
- Tirado, I 2008: Business oriented information security requirements development. Proceedings of the 5<sup>th</sup> annual conference on information security curriculum development, pp 56-58. New York: ACM.
- Tondel, IA, Jaatun, MG, & Meland, PH 2008: Security requirements for the rest of us: a survey. IEEE Software, pp 20-27. Los Alasmitos: IEEE Computer Society Press.
- Tudor, JK 2001: Information security architecture: an integrated approach to security in the organization. Boca Raton: Auerbach.
- Turner, C 2000: The information e-economy: business strategies for competing in the global age. London: Kogan Page.
- Vorster, A, & Labuschagne, L 2005: A framework for comparing different information security risk analysis methodologies. Proceedings of the 2005 annual conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries, pp 95-103. SAICSIT.
- Windham, L 1999: Dead ahead: the web dilemma and the new rules of business. New York: Allworth Press.

Inductively Deriving an Organisational Information Security  
Risk Management Agenda by Exploring Process Improvisation

# INDUCTIVELY DERIVING AN ORGANISATIONAL INFORMATION SECURITY RISK MANAGEMENT AGENDA BY EXPLORING PROCESS IMPROVISATION

<sup>\*1</sup> Kennedy N Njenga

<sup>\*2</sup> Irwin Brown

<sup>\*1</sup> Department of Business IT, University of Johannesburg; Tel: 011 559 1253

<sup>\*2</sup> Department of Information Systems, University of Cape Town; Tel: 021 650  
2677

## ABSTRACT

In times of heightened uncertainty and unpredictability it is believed that incrementalist approaches that are not resolute to order and control in information security risk management (ISRM) are necessary. This is because information security incidents that occur in context are noted to differ one from another. Incrementalist approaches to ISRM apply when contextual security risk instances are rare, unique and complex. This paper qualitatively explores and draws viewpoints from information security management on the incrementalist viewpoint of managing information security risk. Attention is given to *process improvisation*, an explication of combined functionalism and incrementalism which places an emphasis on ways in which practitioners creatively mitigate information security risk. An in-depth case study approach has been used to explore this phenomenon and grounded theory techniques employed to analyse the data. The process of inductive theory building that serves as impetus for an ISRM agenda shows the fit between data and the emerging theory on process improvisation. Findings highlighted in this paper yield rich insights about how an ISRM agenda may incorporate incrementalist and functionalist approaches. Implications for such an agenda to practising information security professionals are also presented.

Proceedings of ISSA 2009

**KEY WORDS**

Information Security, Risk, Process Improvisation, Incrementalism,  
Agenda-setting

# INDUCTIVELY DERIVING AN ORGANISATIONAL INFORMATION SECURITY RISK MANAGEMENT AGENDA BY EXPLORING PROCESS IMPROVISATION

## 1 INTRODUCTION

Information Security Risk Management (ISRM) professionals take an approach to security that is often guided by; importance of security, user perception, costs, availability and compliance with laws rules and regulations (Jochem *et al.* 2006). These approaches according to Dhillon & Backhouse (2001) are functionalist and are the *oppositus* of incrementalism. Functionalist approaches are those approaches that are resolute to order and are evidenced by numerous publications that offer normative guidelines for design, implementing and managing secure information systems (Baskerville 1988; Straub & Welke 1998). Functionalist frameworks for information security that for instance use CobiT or Code of Practice for Security Management have evolved from an inventory of resources and threats from which risk profiles are created (Jochem *et al.* 2006). Hu *et. al.* (2007) has outlined functionalism in information security by considering how modern organisations have established routines and order to cope with internal and external influences of information security risk.

In times of heightened uncertainty and unpredictability it is believed that incrementalist approaches that are not resolute to order and control in information security risk management (ISRM) are necessary. This is because emergent technology, increased usage of computers and the internet has created risks and along with this much uncertainty (Siponen and Kukkonen 2007). Incrementalist approaches to ISRM apply when contextual security risk instances are rare, unique and complex. It is expected that approaches that are incremental can mitigate risk and lead to normalisation of situations.

This paper holds the view that agenda-setting for ISRM takes cognisance of functionalist approaches to ISRM to the detriment of incrementalism. Setting the agenda for ISRM has therefore been largely influenced by the choices in functionalism postulating salience transfer in

ISRM. Saliency transfer is the ability to transfer issues perceived important into corporate ISRM agendas. Corporate agenda in ISRM are issues that big business and corporations consider important.

The purpose of this research was to conceptualise how saliency transfer in ISRM agenda-setting could be made richer by understanding the combination of incrementalist and functionalist approaches as impetus to ISRM agenda-setting. This research explored *improvisation* and specifically how *process improvisation*, as an explication of both incrementalism and functionalism was manifested in ISRM activities and its possible influence to corporate ISRM agenda. The research makes a theoretical contribution by arguing that agenda-setting in ISRM may also take cognisance of combined incrementalist and functionalist approaches.

The paper is structured into five main sections. This first section has introduced and set the context for research. In the next section the various approaches to ISRM are discussed. In this section, functionalism and incrementalism in ISRM are examined in detail. *Process improvisation* in organizations as an explication of both incrementalism and functionalism is also discussed in this section. What follows is a description of agenda setting in ISRM. The third section is the description of the research and justifies the use of a single case study. The research methodology applied is also discussed. In this section also, the use of grounded theory techniques is explained and justified. The fourth section presents and discusses the research findings which are subsequently used to construct a model for agenda-setting in ISRM. By use of the constructed model, this section discusses the possible influence of *process improvisation* to ISRM agenda. In the fifth section concludes the paper by explaining possible benefits of *process improvisation* for information security practitioners.

### **1.1 Research Value**

Little research has been undertaken, to explain saliency transfer of combined incrementalist and functionalist approaches to ISRM agenda-setting. This research aims at providing deeper insights into this discussion.

## **2 APPROACHES TO ISRM**

Organisations currently manage ISRM by focussing on planning and implementing procedures and guidelines as contained in a standard code



## Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation

of practise such as ISO 17799 (Eloff & Eloff 2003; ISO 17799). Dhillon (1997), Dhillon & Backhouse (2001) and Hirschheim *et. al.* (1989) have analyzed existing ISRM methods in the light of formalized rule structures in designing and managing security. An information security planning methodology has also been suggested by Straub & Welke (1998).

### 2.1 Functionalist and Incrementalist Approaches to Information Security Risk Management

Researchers in information security who have suggested, rational choice (Wheeler and Venter 2006) and clear structured policies as being one of the ways to deal with risks and uncertainties are, for the purpose of this research, classified as **functionalist approaches** (Von Solms and Von Solms 2005; Vorster and Labuschagne 2006). Von Solms (2006), talks of structured frameworks for internal controls and policies that are directed and managed by organizations. There are also researchers have become aware of an increasing number of ‘new’ approaches that explore alternative perspectives related to the interpretive, radical humanist and radical structuralist paradigms. These latter paradigms are based on sociological and philosophical theories (Hu *et al.* 2007). Researchers using these latter approaches which call for alternative ways of understanding ISRM have been classified as **incrementalists**. Salmela *et al.* (2000) highlighted principles of the incremental approach, when observing a particular organization’s activities. They described the incremental approach as **highly reflexive**, with decisions being made at any time. The way in which the incremental approach in organizations was observed can also be compared with theories related to reflexivity such as **contingency theory**. Adler *et al.* (1999) exemplified contingency theory when making reference to efficient organisations which were designed to fit the nature of their primary tasks. It should be noted that some organisations practise the incremental approach whereby functionalism takes a small part while activities and decision making are made on a one-by-one basis.

## 2.2 Process Improvisation: Combined Functionalism and Incrementalism

Formulation of information security policies that take cognisance of both functionalism and incrementalism i.e. information security risk management, and strategic information systems plan (SISP) has been proposed by Doherty (2006) as a way adding richness to both disciplines. Similarly, researchers such as Björck (2004) realized the need to look at organizations afresh by postulating a neo-institutional theory in studying IT security issues in organizations. Björck (2004) argues that the revolutionized modern organization requires new ways of explaining why formal security structures (functionalism) and actual security behavior (incrementalism) differ and why organizations often create formal security structures without implementing them fully. It has been from such observations that has lead researchers to have a closer look at have organizational *improvisation* by showing its relevance in current competitive environments (Crossan & Sorrenti 1997; Moorman & Miner 1998). Ciborra *et al.* (2000) considered *improvised* activities as **simultaneously structured** (functionalist) and **unpredictable**; planned but emergent; discernible after the fact but spontaneous (incrementalism) in its manifestation. *Process improvisation* as a type of improvisation in organisations has been a phenomenon researched by social scientists due to its perceived importance in contextually relating content and sequence of previous processes and routines in novel ways that affect outcomes (Cunha 2003). *Process improvisations* affect the manner in which products are developed Miner *et al.* (2001).

## 2.3 Agenda-setting in ISRM

It can be noted that first-level agenda setting as traditionally studied by researchers use objects or issues to influence the people. The formation of an ISRM agenda depends on information security practitioner conception of what is important in ISRM. It has been noted that information security practitioners often set an ISRM agenda that is devoid of incrementalism. This is because incrementalism has not been counted as important because of its “soft” appeal i.e. a derivative from the social sciences. Understanding *process improvisation* (as a fusion approach) in ISRM could help reconcile tension between structure (functionalism) and

## Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation

reflexivity (incrementalism) and set the pace for a richer agenda-setting since it comprises a rich mixture of centralised structure and novel spontaneity (Cunha 2004; Ciborra *et al.* 2000; Segars and Grover 1999). In this way information security practitioners may be forced to think about such issues and therefore involves salience transfer among practitioners.

### 3 METHODOLOGY

A single case research was used which was exploratory, interpretivist and contextual. The researcher identified and selected a single case on the assertion that this case was *uniquely positioned* to generate a full variety of evidence including documents, artefacts, interviews and observations.

#### 3.1 Data collection

The primary data consisted of a series of 11 in-depth interviews. All interviews were tape recorded. After each interview, the information was transcribed verbatim in writing. In addition, notes were taken as the interviews progressed. It is from the transcribed responses from the interviewees that the research formed the contextual case for the phenomenon of *improvisation* being investigated. The interviews were conducted for 60 to 90 minutes per session. This generated close to 700 transcript minutes for data analysis.

#### 3.2 Units of Analysis in the Single Case

The single case followed set procedures as directed by the CobiT, ITIL, ISO IEC 17799 frameworks and methodologies. It was therefore easy to map out the units of analysis as activities defined by these frameworks, since these activities *were already implemented* in the organisation. There was a clear structure of how these activities were to be implemented and performed (based on CobiT, ITIL, ISO IEC 17799). The ISRM activities and hence the units of analysis are summarised in **Table 1** below.

*Table 1. Open Coding of Improvisational Data Incidents*

<b>Units of Analysis</b>	<b>ISO IEC 17799</b>	<b>ITIL</b>	<b>CobiT</b>
Information Assets Access and Data Control	<i>Section 3 of ISO 17799</i>	<b>Application Management, Control Methods and Techniques</b> 7.2 Understanding the applications relationship to IT services	<b>DS 11</b> Manage Data
Information Security Architecture	<i>Section 4 of ISO 17799</i>	<b>ICT Infrastructure Management, Technical support</b> 5.4	<b>PO 2</b> Define the Information Architecture
Information Security Policies	<i>Section 5 of ISO 17799</i>	<b>Security Management;</b> <i>Fundamental of Information Security;</i> 4.1 Control	<b>DS 5</b> Ensure Systems Security
Information Security Event Monitoring	<i>Section 9 of ISO 17799</i>	<b>Service Level Management;</b> 4.4.7 Establish monitoring capabilities	<b>DS 10</b> Manage Problems and Incidents
IT Governance and Regulatory Compliance	<i>Section 12 of ISO 17799</i>	<b>The Technical Support</b> 5.4 The technical support process	<b>PO 8</b> Ensure Compliance with External Requirements
Disaster Recovery and Business Continuity	<i>Section 12 of ISO 17799</i>	<b>Availability Management</b> 8.3 The availability management process	<b>DS 4</b> Ensure Continuous Service

### 3.3 Inductive Theory Building and the Use of Grounded Theory Techniques

Inductive theory building emphasizes the fit between data and the emerging theory, rather than moving deductively down from a prior hypothesis. The researcher used the grounded theory techniques of open coding to achieve this. Grounded Theory Techniques (GTT), (Glaser & Strauss 1967; Strauss & Corbin 1990; Glaser 1992) formed a basis for

Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation

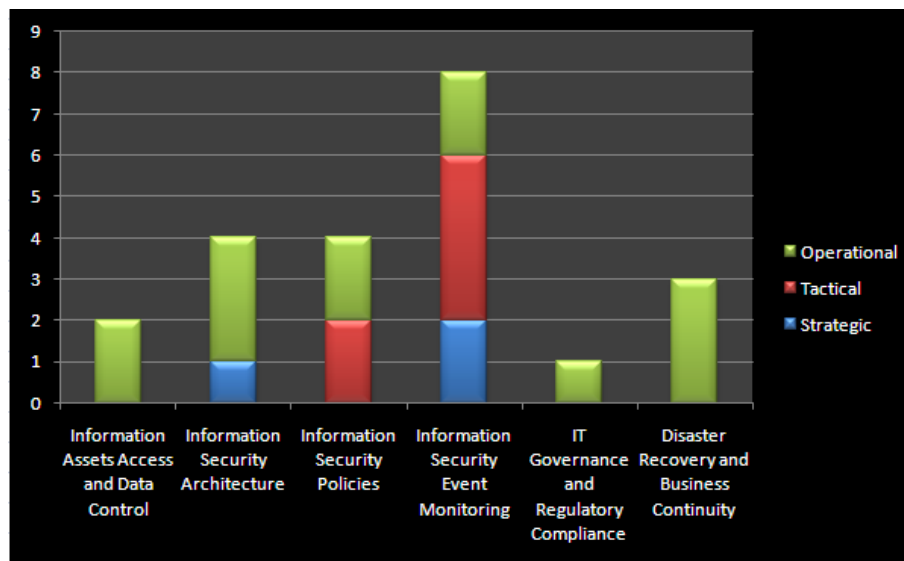
content analysis (see *step 1* below). GTT also for purposes of this research proved an attractive way for inductive reasoning. Orlikowski (1993) and Trauth & Jessup (2000) have demonstrated successfully GTT application in organizational and information systems research in the past. What follows is a detailed explanation for each step as shown by **Table 2**.

Table 2. Open Coding of Improvisational Data Incidents

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
<b>Data Incidents (Transcribed Interviews)</b>	<b>Context of Data Incident</b>	<b>Researcher's memos</b>	<b>Level (Strategic, Tactical, or Operational)</b>	<b>Concepts generated</b>
<p><b>Extracting Data Incident;</b></p> <p>The researcher started by looking for elements of <i>process improvisation</i>. The process of breaking down and analysing the data and assigning labels is described as content analysis by researchers (Glaser and Strauss 1967).</p>	<p><b>Determining Context of Data Incident;</b></p> <p>Through conversation analysis (Denzin et al. 2003) the researcher provided the context for selected data in the data-sets for incidents that reasonably suggested <i>process improvisations</i>.</p>	<p><b>Deriving Open Codes from Researcher's Memos;</b></p> <p>The process of writing memos that would guide open coding (grounded theory technique) in STEP 3 involved several sub-steps. The first step was to examine in-vivo codes.</p>	<p><b>Determining Level;</b></p> <p>The inductive aspect of analysing data was made possible by extracting and understanding data that reflected aptitude for a fusion of structure and creative thinking simultaneously at three organisational levels.</p>	<p><b>Creation of Codes and High Level Concepts Inductively;</b></p> <p>Deriving codes was by way of examining data-sets in-depth and careful analyzing these.</p>

## 4 RESEARCH FINDINGS

This section provides a summary of units of analysis from the single case and the data-sets examined in each unit of the case. In total, a series of **23 concepts** (high level concepts) were generated from open coding that were interpreted to be *process improvisational* actions in ISRM. There were more conceptual instances of concepts relating to *process improvisation* at Event Monitoring activities than other activities for this case. The case also suggests that improvisations were less likely to be present in activities relating to IT Governance and Regulatory Compliance. This is shown by *Figure 1* (next page). The case also suggests that process improvisation was much more presented at operational rather than at strategic levels within the organisation.



*Figure 1. Process Improvisation in ISRM activities*

### 4.1 Deriving an ISRM Agenda: Theoretical Synthesis

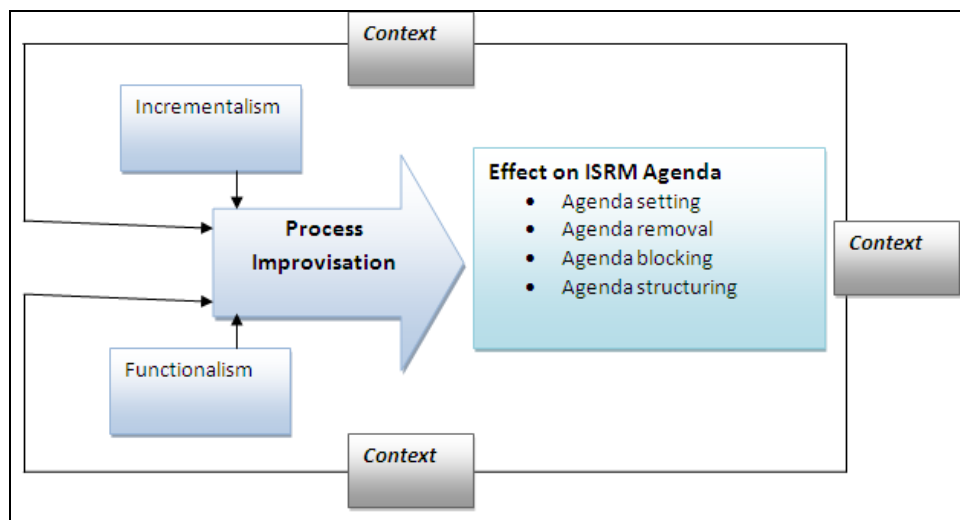
Research findings show that the occurrence of *process improvisation* was in many cases *contextual* due to security incidents being rare and unique. These incidents therefore required a novel way of handling these

Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation

particularly at activities relating to Event Monitoring. Only by hindsight would practitioners’ perceive that they were *process improvising*.

Insights as to these revelations led the researcher to conceptualise on how an ISRM agenda would be formulated, which brought awareness of these to ISRM practitioners. There would be different ways by which practitioners would perceive this information. They would as explained by Eriksson and Noreen (2002);

- a) Realise the importance of *process improvisation* in ISRM and hence set the agenda; (*agenda-setting*).
- b) Realise that *process improvisation* has not effect in ISRM, hence be removed; (*agenda removal*).
- c) Realise that encouraging *process improvisation* would be interpreted as discouraging structure and functionalism and would therefore be deliberately be prevented from being discussed (*agenda blocking*)
- d) Discuss the importance of process improvisation but this would not necessarily translate into concrete action of formalising it (*agenda structuring*). *Figure 2.* below summarises this discussion.



*Figure 2. Inductively deriving an ISRM agenda: Adapted from Eriksson and Noreen (2002)*

## 4.2 Implications for Practices

The researcher is of the opinion that it takes a discrete, bold, conscious step towards bridging this theory and practice. The need to encourage *process improvisation* would be justified since *process improvisation* offers information security practitioners and practices various ways to remain flexible and adaptive in turbulent situations while allowing for co-presence efficiency and effectiveness in detecting change and immediately taking advantage of this change.

## 5 CONCLUSION

For *process improvisation* to be included as an agenda item in ISRM information security practitioners should perceive its importance. It is hoped that this discussion has highlighted this. Information security practitioners should see themselves as *socio-constructive agents* who are creative and who create reality around themselves. They should see *process improvisation as leading to a rich and good ISRM practice*.

## 6 REFERENCES

- Adler, P. S., Goldofta B. and Levine D. I., (1999) "Flexibility verses Efficiency? A case Study Model of Changeovers in the Toyota Production System" *Organization Science* Vol. 10:1 pp. 43-68
- Baskerville, R., (1988) "*Designing Information Systems Security*" John Wiley & Sons, New York, NY.
- Björck, F. (2004). "Institutional Theory: A New Perspective for Research into IS/IT Security". In *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37 2004)*, 5-8 January 2004, Big Island, HI, USA: IEEE Computer Society.
- Ciborra, C.; Braa K.; Cordella A.; Dahlbom b.; Hanseth O.; Hepso V.; Ljungberg J.; Monterio E.; and Simon K. A. (2000) '*From Control to Drift*', Oxford University Press, Oxford:



Inductively Deriving an Organisational Information Security  
Risk Management Agenda by Exploring Process Improvisation

- Crossan, M. M., and Sorrenti, M., (1997) “Making sense of Improvisation” *Advances in Strategic Management*, Vol 14:0 pp. 155-180.
- Cunha, M. P., (2003). “Organizational improvisation and change: two syntheses and a filled gap”, *Journal of Organizational Change Management* Vol. 16:2 pp. 169-185.
- Cunha, M., P. (2004) “Management Improvisation” *FEUNL Working Paper No. 460*. Available at SSRN: <http://ssrn.com/abstract=882455>
- Deetz, S. (1996) “Describing Differences in Approaches to Organization Science: Rethinking Burrell and Morgan and their Legacy,” *Organization Science* Vol. 7:2, pp. 191–207
- Dhillon, G. (1997) “*Managing Information Systems Security*”, MacMillan Press LTD. United Kingdom.
- Dhillon, G. and Backhouse, J. (2001) “Current Directions in IS Security Research: Toward Socioorganizational Perspectives,” *Information Systems Journal*, Vol. 11: 2.
- Doherty, N. F. (2006) “Aligning the information security policy with the strategic information systems plan. *Computers & Security* Vol. 25:1 pp. 55-63
- Eloff, J., and Eloff, M., 2003 “*Information Security Management – A New Paradigm*” Proceedings of SAICSIT 2003, pp. 130 –136.
- Eriksson J., and Noreen, E. (2002) 'Setting the Agenda of Threats: An Explanatory Model', *Uppsala Peace Research Papers No. 6*. Uppsala: Department of Peace and Conflict Research, Uppsala University.
- Glaser, B., G. and Strauss A (1967) “*The Discovery of Grounded Theory: Strategies for Qualitative Research*”, Aldine Publishing Co, Chicago IL.
- Glaser, B.G. (1992). “*Basics of Grounded Theory Analysis: Emergence Vs. Forcing*”. Sociology Press: California.
- Hirschheim, R. and Klein HK, (1989) “Four Paradigms of Information Systems Development” *Communications of the ACM*, Vol 32:10, pp. 1199–1215.
- Hu, Q., Hart, P., and Donna Cooke, D., (2007) “The role of external and internal influences on information systems security – a neo-institutional

Proceedings of ISSA 2009

perspective”, *Journal of Strategic Information Systems* Vol 16:0 pp. 153–172.

ISO/IEC 17799 Code of practice for Information Security Management, International Organization for Standardization/ International Electrotechnical Commission. Available at <http://www.iso.ch/iso/en/ISOOnline.opennerpage>

Jochem, A., Bewier, A., Bongers, L., Borger, L., Coene, H., Elsinga, B., Jonkman, E., Kuiper, R., Oostdijk, M., Rijsenbrij, D., Smulders, A. (2006) "Security Principles: Information security on the management agenda" *Genootschap van Informatie Beveiligers (GvIB) Expert Letter*, Volume 1:3 pp. 1-11

Miner A. S., Bassoff P. and Moorman C., (2001) “Organizational Improvisation and Learning: A Field Study” *Administrative Science Quarterly* Vol. 46:2 pp. 304-337

Moorman, C., and Miner, A. (1998) “Organisational Improvisation and Organisational Memory,” *Academy of Management Review* Vol 23:4 pp. 698-723.

Orlikowski, W. J., (1993) “CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development” *MIS Quarterly* Vol 17:3.

Salmela, H., Lederer, A.,L. and Reponen, T. (2000) “Information systems planning in a turbulent environment” *European Journal of Information Systems* Vol. 9:1 pp. 3–15

Segars, A. & Grover, V. (1999) Profiles of strategic information systems planning. *Information Systems Research* Vol. 10:3 pp.199-232

Siponen, M. T., and Kukkonen, H. O., (2007) “Of Information Security Issues and Respective Research Contributions,” *The DATA BASE for Advances in Information Systems* Vol 38:1.

Straub, D. and Welke, R. (1998) “Coping with systems risk: Security planning models for management decision making,” *MIS Quarterly* Vol 22:4 pp. 441–470.

Inductively Deriving an Organisational Information Security  
Risk Management Agenda by Exploring Process Improvisation

Strauss, A. and Corbin, J. (1990), “*Basics of Qualitative Research: Grounded Theory Procedures and Techniques*” Sage, Thousand Oaks, CA.

Trauth, E.M. and Jessup, L.M. (2000) “Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use,” *MIS Quarterly* Vol. 24:1 pp. 43-79.

Von Solms, B. (2006). “What every Vice-Chancellor and Council Members should know about the use of ICT” Proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa.

Von Solms B and Von Solms R (2005) ‘From Information security to...business security’? *Computer and Security* Vol 24:4 pp 271-273.

Vorster A., and Labuschagne L. (2006). “A new comparison framework for information security risk analysis methodologies”, *South African Computer Journal*, Vol 37 pp. 98 – 106.

Wheeler M., and Venter H. (2006). ” Change Management: A case study at the University of Pretoria”, Proceedings of the Conference on Information Technology in Tertiary Education (CITTE) Pretoria, South Africa.

Proceedings of ISSA 2009

## INTEGRATING INFORMATION ASSURANCE INTO SYSTEM ADMINISTRATION

Erik Hjelmås<sup>1</sup>, Nils Kalstad Svendsen<sup>1</sup>, Stephen D. Wolthusen<sup>1,2</sup>

<sup>1</sup>Norwegian Information Security Laboratory  
Department of Computer Science  
Gjøvik University College  
N-2818 Gjøvik  
Norway

<sup>2</sup>Information Security Group  
Department of Mathematics  
Royal Holloway, University of London  
Egham, Surrey TW20 0EX  
United Kingdom

<sup>1</sup>{erikh,nilss}@hig.no, <sup>2</sup>stephen.wolthusen@rhul.ac.uk

### ABSTRACT

While the cost and flexibility benefits resulting from distributed and cloud computing environments are clearly evident, this approach also has far-reaching implications for the threat surface presented as well as general information security risks, particularly to availability. The design of cloud-based storage services also implies that data once stored with such services may very hard to recall. The ease with which these services can be used implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture unless the implications are understood clearly. As the impact is both technical and legal in nature and can easily have a temporal extent well exceeding the life-time of a given configuration, we argue that the professional education of system and network administrators must take these security aspects into consideration even at the undergraduate level. We therefore outline a curriculum integrating information security and security management topics into a 3-year (180 credit points in the European Credit Transfer System) Bachelor of Science degree in Computer Science

Proceedings of ISSA 2009

with specializations in either *Network and System Administration Operations* or *Information Security* intended to enable students to create, operate, and maintain information systems not only fulfilling functional, efficiency, and robustness requirements, but also minimizing information security and liability risks.

### **KEY WORDS**

Security Architecture, Curriculum Design, Information System Architecture

## INTEGRATING INFORMATION ASSURANCE INTO SYSTEM ADMINISTRATION

### 1 INTRODUCTION

The ability to construct virtual information systems either locally or using a wide range of options from externalizing individual services to a fully distributed or cloud computing [2] environment rapidly implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture as it may be faster and more cost-effective to call upon an external service provider than to bring internal services on-stream [4]. Moreover, the use of services rather than capital equipment and the prospect of off-loading most of the administrative responsibility associated with such services all provide strong incentives at levels from system administrators to system architects.

The use of such facilities does, however, involve a number of risks both technical and legal in nature which must be fully understood as some of the consequences of service use are difficult if not impossible to reverse and hence can have a temporal extent that far exceeds the life-time of a given configuration. At the same time it is unlikely that, as requirements emerge at the operational level, decisions on how to meet requirements will be escalated to a strategic system architect's level at all time. Given that many such services are, however, interdependent on each other either directly or indirectly, even a small number of externally provisioned services can represent a long-term commitment.

Because of this, we argue that system and network administrators even at the operational level, where first-line responsibility is likely to reside with staff holding undergraduate or professional degrees, must increasingly have a solid understanding of network and service architecture and the information security and security management implications, making distinctions in degrees and pathways increasingly questionable. Based on these observations and the fact that the European Higher Education Area (also known informally as the *Bologna system*) offers a flexible mechanism for structuring degree programs in a modular fashion, we propose to adapt curricula in the computer science area in such a way that students wishing to specialize in

system architecture and management or professionals intending to update their qualifications can do so in a cohesive and integrated manner.

The remainder of this paper is therefore structured as follows: Section 2 briefly reviews the types of services and facilities available to information system architects and administrators, while section 3 discusses the information security implications resulting from these developments. Based on this, sections 4 and 5 then derive a set of requirements for integrating information security into undergraduate programs for information system administration and architecture and a proposed approach for meeting such requirements within the scope of ACM/IEEE curriculum recommendations, followed by a discussion on ways of enhancing the mobility of graduates both geographically and particularly along career pathways in section 6 and brief conclusions in section 7.

## 2 DISTRIBUTED AND CLOUD ENVIRONMENTS

Distributed computing services are, despite recent and periodic re-naming and different efforts at promoting such services, has been a long-standing vision arguably originating with the *Computing Utility* proposed by the MIT MAC project [5] as articulated by Fano and subsequently implemented substantially in the Multics system [3]. It is particularly noteworthy in this context that one of the core concepts of modern cloud computing, i.e. the sharing and remote commercial use of virtual machines dates to the mid-1960s. In the following, section 2.1 briefly reviews some of the key features of current distributed computing architectures, while section 2.2 highlights systems management aspects of such architectures.

### 2.1 Distributed Computing Platform Components

While terminology varies considerably, a simple taxonomy of distributed computing elements can be derived based on the granularity of the services offered. At the finest level of granularity, individual services, typically web or database services (currently being referred to as *applications in the cloud* or AITC) are providing business processes or components with state distributed across servers and client systems. Several implementation variants, frequently hybrid, ranging from legacy CORBA environments via SOAP and WS infrastructures [14] to AJAX [8] based on the design principle of representational state transfer (REST) originally articulated by Fielding [6].



## Integrating Information Assurance Into System Administration

Each service may in turn depend on others and can require several service layers (frequently employing database back-ends). Moreover, a number of ancillary services can be required, including service discovery mechanisms, name services and, when security mechanisms are utilized, key management infrastructures. Moreover, each of these services can be provided in a geographically distributed manner, adding the interconnecting networks to the infrastructure required for provisioning such services. While general deployment of such services is limited, some areas such as externally provisioned email services are increasingly common.

Similar design principles employing middleware components are also found in more complex service-oriented architectures in which complex business processes are composed of multiple implementation services and events typically coordinated on enterprise service bus responsible for process choreography and service orchestration [13]; this is also referred to as *platforms in the cloud* (PITC). Software as a service (SaaS) as originally described by Bennett *et al.* [1] can be considered a derivative of this approach in that the service delivery uses the same technical underpinnings while state is typically retained on the application service provider's systems; infrastructure dependencies are therefore potentially of similar complexity as in the case of uncoupled web services. However, the most popular approach commonly associated with the term cloud computing (also referred to as *infrastructure in the cloud*, IITC) is of a more coarse granularity in that it is centered on the provisioning of virtual machines and storage space available commercially from a number of sources [10]. Although this eliminates some of the interdependency layers noted above, access to services will still require queuing, network and cryptographic key management as well as potentially front-end infrastructures, while both virtual machines and storage will frequently be re-located dynamically to provide improved response times and failure tolerance as well as load balancing.

### 2.2 Cloud Management

Although particularly in case of IITC residual system management responsibility lies with the service user and network as well as enabling infrastructure must still be maintained, significant portions are migrating to the infrastructure provider. This requires not only the elaboration of service level agreements (SLA) for all relevant aspects of the service, but also monitoring compliance with SLAs and the deployment of mitigation and service level

enforcement mechanisms [12].

### 3 SECURITY CHALLENGES

A number of security issues arising from the distributed environments outlined in section 2 are easily identified. While securing confidentiality and integrity of data in transit is trivially addressed using standard cryptographic protocols, even storage presents a number of difficulties as encrypting data at rest may both interfere with desired functionality and adversely affects application performance. Moreover, as data is processed, by definition, on systems under the control of one or more third parties, it will be available as plaintext in such an environment. This raises questions both about the trustworthiness of service providers and the strength of compartmentalization between virtual machine instances, which must not only be maintained during operation but also in case of virtual machine migration [16].

Further security issues arise from uncertainties about the integrity of the computing and communication platform themselves, which can affect the integrity of both the applications and that of active monitoring, e.g. by Byzantine behavior in suppressing or altering messages. This type of threat is also present for the case of key and identity management; as key material is implicitly exposed, it may be accessible to adversaries at endpoints or within the management infrastructure of the service provider.

Given the exposure of network traffic as well as potential cross-service contamination and hence the increased risk of denial of service attacks compared to systems within an organization's perimeter, availability is a major security consideration. While reliability models can provide predictable high levels of availability in the face of random (Gaussian) failures, this may not be the case for deliberate attacks, which may indeed target the very mechanisms providing robustness and redundancy such as load balancing mechanisms.

However, while the above touches upon several critical and in part insufficiently resolved security challenges in cloud computing, there are further implications for legal and management perspectives which must also be taken into account. In most backup configurations, multiple copies and generations of backup data are interspersed on storage media at different access hierarchies. While this redundancy is typically desirable in the event of failure, deletion of data sets such as in case of the termination of a service agreement is problematic, particularly if a service provider does not isolate backups for

## Integrating Information Assurance Into System Administration

different customers as is commonly the case and implied in terms and conditions of service providers. Similarly, both servers and storage media may be in different physical locations with services and data migrating among locations to provide optimum resource usage and service levels. However, while such migration and distribution is deliberately transparent at the implementation level, physical location can imply that a given datum or service may fall under different jurisdiction. In some cases this may even affect the legality of a service or transactions, but a major concern arises from the possibility of seizing evidence in criminal or civil proceedings as well as for compliance purposes. Moreover, certain processes may rule out the use of cloud computing environments entirely [11].

### 4 CURRICULUM REQUIREMENTS

Enabling students to make informed decisions on service provisioning and deployment and taking security considerations into account in network and system administration must be balanced with requirements for the core of the respective curriculum. In doing so, the structure of undergraduate degrees in the European Higher Education Area limits the ability to add modules as it defines a B.Sc. degree to encompass 180 credit points in the European Credit Transfer System (ECTS) over three years of studies. However, as will be shown in section 5, key aspects of the required knowledge can be incorporated in core modules of the computer science undergraduate degree, and can also provide a running theme which can be carried forward to the capstone project in the B.Sc. dissertation. This permits the concentration of specific aspects conjoining information assurance and system administration in selected elective modules, thereby providing students with the flexibility to choose their specialization area relatively late in the course of their studies or to combine the specialization areas of Network and System Administration (NSA) and Information Security (IS).

At the same time, the specialization areas are designed to be aligned with recognized standards and best practices in the respective areas; in the case of NSA, this is the Computing Curricula Information Technology (CCIT) [9], albeit with a stronger emphasis on technical capabilities. For IS, the alignment is with the Certified Information Systems Security Professional (CISSP) domains; once again, the focus here is more on technical aspects.

As several of the issues noted in section 3 also have legal aspects connected to them, this is incorporated in the form of elective modules. Either special-

ization area, however, provides a balance between the core computer science curriculum including a solid mathematical foundation [15] whilst establishing a solid foundation for subsequent postgraduate degrees, particularly specializing in information security either in direct succession to the undergraduate program or after a hiatus [7].

## 5 CURRICULUM DESIGN

While, as noted in section 4, all specialization areas are built around a strong computer science core and incorporate information assurance elements, the pathways and elective modules themselves differ, with the IS pathway providing further options to specialize in topics relevant to information assurance and security.

### 5.1 B.Sc. Information Security (IS)

The B.Sc. in computer science with its specialization in information security combines the core of a traditional computer science program with information technology and information assurance along with up to date knowledge and skills related to current information technology.

The core pathway is illustrated in figure 1; this is augmented by elective modules covering the CISSP core bodies of knowledge — Access Control (AC); Application Security (AS); Business Continuity and Disaster Recovery Planning (BCDR); Cryptography (C); Information Security and Risk Management (ISRM); Legal, Regulations, Compliance and Investigations (LRCI); Operations Security (OS); Security Architecture and Design (SAD); and Telecommunication and Network Security (TNS) — with the exception of Physical Security (PS), which are structured in the modules as shown below (several additional electives are not shown); here, the first digit denotes the year of the program in which these electives are typically chosen.

**IMT3491** Ethical Hacking and Penetration Testing

**IMT3551** Digital Forensics

**IMT3771** Introduction to Cryptology

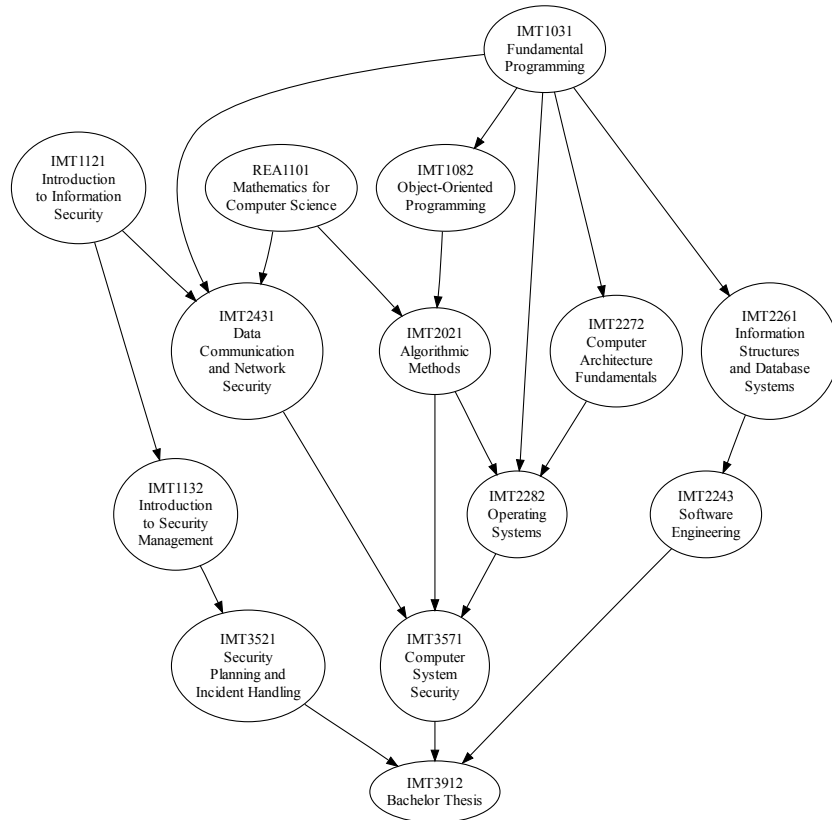
**IMT3292** System Administration

**IMT3281** Software Development

**IMT3511** Discrete Mathematics

**IMT2291** Web Technology

## Integrating Information Assurance Into System Administration



*Figure 1: Module Interrelations in the IS Core Curriculum*

- IMT3441** Application and Database Management
- SMF1042** Basic Economics
- SMF2051** Organizational Management including Labour Laws
- IMT1271** IT Service Management
- IMT1321** IT Management

Figure 2 visualizes the coverage of these core aspects, where grey fields indicate partial, and black fields full coverage of the relevant subject areas.

### 5.2 B.Sc. Network and System Administration (NSA)

The B.Sc. with specialization in network and system administration (NSA) provides a more operationally-focused program compared to the IS specialization and is intended to provide the private and public sector with IT

	IMT1031	REA1101	IMT1121	IMT1082	IMT2431	IMT1132	IMT2021	IMT2272	IMT2261	IMT3521	IMT2282	IMT2243	IMT3571	IMT3912	IMT3491 (E)	IMT3551 (E)	IMT3771 (E)	IMT3292 (E)	IMT3281 (E)	IMT3511 (E)	IMT2291 (E)	IMT3441 (E)	SMF1042 (E)	SMF2051 (E)	IMT1271 (E)	IMT1321 (E)	SMF2081 (E)	
AC																												
AS																												
BCDR																												
C																												
ISRM																												
LRCI																												
OS																												
PS																												
SAD																												
TNS																												

Figure 2: Matching CISSP Domains to IS Specialization Courses

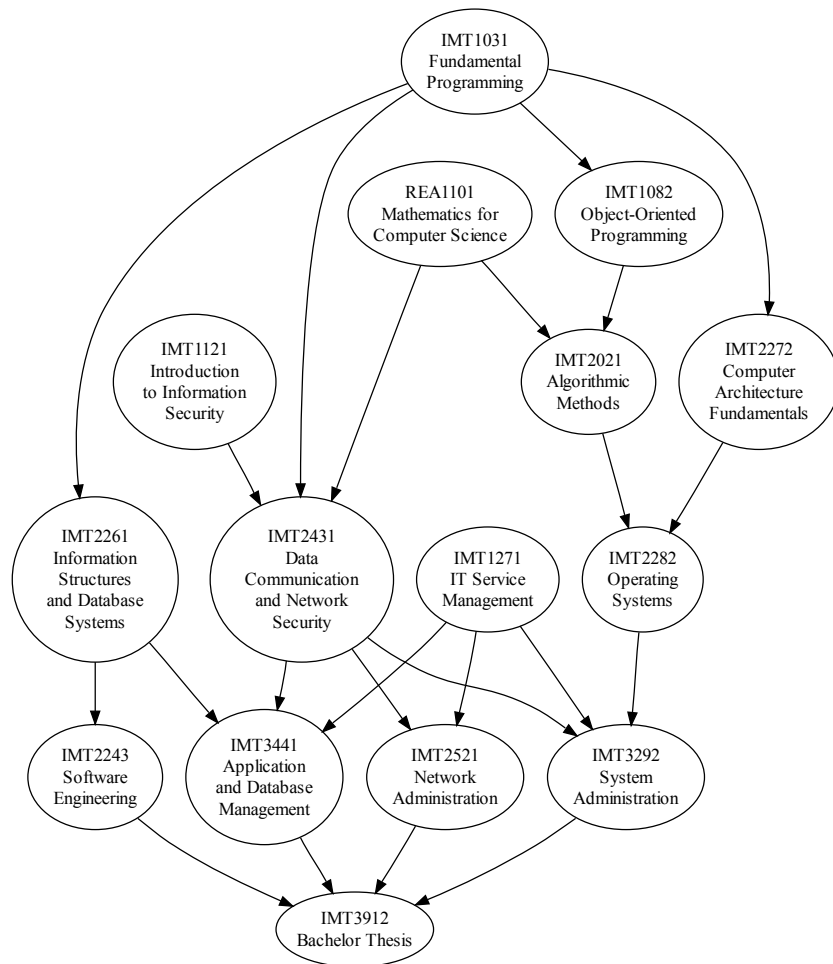
professionals having a broad range of competence in evaluating and maintaining computerized infrastructures, and the ability to integrate a range of different technologies and their integration into an organization's structure.

Analogous to figure 1, the NSA core pathway is illustrated in figure 3, while the following list provides modules which are not already included in the elective roster shown in section 5.1:

- IMT2072** Ergonomics in Digital Media
- IMT1042** Basic Economics
- IMT3102** Object-Oriented Software Development
- IMT3571** Computer System Security
- IMT1132** Introduction to Security Management
- IMT3521** Security Planning and Incident Management
- IMT3781** Introduction to Computer Law

While there is no immediate equivalent to the CISSP body for network system administration, the curriculum is aiming to cover the pervasive themes noted above and particularly makes reference to background knowledge required for a solid understanding of the ITIL (Information Technology Infrastructure Library) including the methods and skills required to successfully implement the best practices codified therein. In doing so, the NSA specialization aims to follow the *pillars-first* approach rather than the *integration-first* strategy advocated by CCIT, but aims to provide the strong

### Integrating Information Assurance Into System Administration



*Figure 3: Module Interrelations in the NSA Core Curriculum*

motivation that such an integration approach by using the topics described in sections 2 and 3 as the common theme without sacrificing technical depth in the process. At the same time, the program discussed here is, regardless of the specialization chosen, a more technically oriented program and eschews human-computer interaction and organizational issues, although these can be chosen as elective modules.

## 6 ENHANCING MOBILITY

Two areas of mobility are considered here, *career* and *international* mobility. An undergraduate degree as described in the present paper must fulfill dual purposes in that it simultaneously should prepare graduates for employment yet at the same time provide sufficient foundations and particularly introduce the methods of academic inquiry to enable suitably qualified candidates to proceed with postgraduate studies. We have outlined previously how students interested in information security and assurance are provided with opportunities at both the M.Sc. and Ph.D. levels in dedicated programs [7] and are deliberately structuring these postgraduate programs in such a way that they can also be taken in a part-time or low-residency format, making use of electronic media to provide interaction between students and faculty and among students where possible and scheduling lectures and seminars in a predictable manner, resulting in a desirable combination of continuing and mature students which can also contribute a professional perspective to fellow students. While the undergraduate program described here was, unlike the postgraduate programs, originally aimed primarily at domestic students, we are moving to provision all programs in English to allow better integration of international students. However, given the stronger emphasis on lectures, low-residency options are not considered feasible, although once again electronic communication forms are used extensively to support students. Given the diverse backgrounds of students, moreover, emphasis is placed on highlighting both common principles and possible divergences in areas such as legal courses.

## 7 CONCLUSION

In this paper we have described our approach to provisioning an undergraduate degree program in computer science which allows students to specialize in the critical areas of information security and network and system administration while at the same time neither sacrificing the technical foundations later enabling them to successfully pursue postgraduate programs nor the ability to become productive professionals. The common theme of distributed and cloud system assurance provides a strong motivational anchor which can encourage students to pursue topics without sacrificing depth as is commonly the case in integration-first courses. We have also carefully designed curricula to enable international and career mobility, showing clear pathways for



## Integrating Information Assurance Into System Administration

both academic and professional development in the information security and assurance area.

### References

- [1] K. Bennett, P. Layzell, D. Budgen, P. Brereton, L. Macaulay, and M. Munro. Service-based software: the future for flexible software. In *Proceedings of the Seventh Asia-Pacific Software Engineering Conference (APSEC 2000)*, pages 214–221, Singapore, December 2000. IEEE Press.
- [2] R. Buyyaa, C. Shin Yeoa, S. Venugopala, J. Broberga, and I. Brandic. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, June 2009.
- [3] F. J. Corbató and V. A. Vyssotsky. Introduction and Overview of the Multics System. In *Proceedings of the AFIPS Fall Joint Computer Conference (1965 FJCC)*, volume 27 part 1, pages 185–196, Las Vegas, NV, USA, November 1965. AFIPS, Spartan Books.
- [4] M. Fan, S. Kumar, and A. B. Whinston. Short-term and long-term competition between providers of shrink-wrap software and software as a service. *European Journal of Operational Research*, 196(2):661–671, July 2009.
- [5] R. M. Fano. The MAC System: The Computer Utility Approach. *IEEE Spectrum*, 2(1):55–64, January 1965.
- [6] R. T. Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. PhD thesis, Department of Information and Computer Science, University of California, Irvine, Irvine, CA, USA, 2000.
- [7] E. Hjelmås and S. D. Wolthusen. Full-Spectrum Information Security Education: Integrating B.Sc., M.Sc., and Ph.D. Programs. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, pages 9–16, Kennesaw, GA, USA, September 2006. ACM Press.

Proceedings of ISSA 2009

- [8] A. T. Holdener III. *Ajax: The Definitive Guide*. O'Reilly, Sebastopol, CA, USA, 2008.
- [9] B. M. Lunt, J. J. Ekstrom, S. Gorka, G. Hislop, R. Kamali, E. Lawson, R. LeBlanc, J. Miller, and H. Reichgelt. Information Technology 2008 — Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (ACM/IEEE Computer Society. Technical report, Association for Computing Machinery, November 2008.
- [10] J. Murty. *Programming Amazon Web Services*. O'Reilly, Sebastopol, CA, USA, 2008.
- [11] Payment Card Industry. Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures. Technical report, PCI Security Standards Council LLC, October 2008.
- [12] V. Stantchev and C. Schröpfer. Techniques for service level enforcement in web-services based systems. In *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services (IIWAS 2008)*, pages 7–14, Linz, Austria, November 2008. ACM Press.
- [13] S. Tarkoma. *Mobile Middleware Architecture, Patterns, and Practice*. John Wiley & Sons, Inc., Chichester, UK, 2009.
- [14] S. Weerawarana, F. Curbera, F. Leymann, T. Storey, and D. F. Ferguson. *Web Services Platform Architecture*. Prentice-Hall, Englewood Cliffs, NJ, USA, 2005.
- [15] S. D. Wolthusen. The Role of Mathematics in Information Security Education. In *Proceedings of the 5th IFIP TC11.8 World Conference on Information Security Education (WISE 5)*, pages 129–136, West Point, NY, USA, June 2007. Springer-Verlag.
- [16] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang. PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In *Proceedings, Third Asia-Pacific Trusted Infrastructure Technologies Conference (APTIC '08)*, pages 9–18, Hubei, China, October 2008. IEEE Press.



# **PART 2**

## **RESEARCH IN PROGRESS PAPERS**

Proceedings of ISSA 2009

A Proof of Concept Implementation of a  
Secure E-Commerce Authentication Scheme

## A PROOF OF CONCEPT IMPLEMENTATION OF A SECURE E-COMMERCE AUTHENTICATION SCHEME

Carolin Latze<sup>1</sup>, Andreas Ruppen<sup>2</sup>, and Ulrich Ultes-Nitsche<sup>3</sup>

<sup>1,2,3</sup>University of Fribourg  
Department of Informatics  
Boulevard de Perolles 90  
1700 Fribourg  
Switzerland

<sup>1</sup>carolin.latze@unifr.ch, <sup>2</sup>andreas.ruppen@unifr.ch, <sup>3</sup>uun@unifr.ch

### ABSTRACT

E-Commerce applications such as online shopping or e-banking are steadily gaining popularity in every-day life. Yet, many users are not aware of how to avoid the associated security problems: they don't choose secure passwords, check server certificates, or reliably react to browser warnings when a certificate can't be verified. Thus, protecting users from physical and social attacks such man-in-the-middle, pharming or phishing attacks is of main importance in online business. This work describes a proof of concept implementation of a secure e-commerce authentication scheme using everyday devices like Trusted Platform Modules (TPMs) and mobile phones. As the prototype has shown very promising results, the authors believe that such an authentication protocol might be a possibility in order to avoid the attacks mentioned above.

### KEY WORDS

E-Commerce, Authentication, TPM

# A PROOF OF CONCEPT IMPLEMENTATION OF A SECURE E-COMMERCE AUTHENTICATION SCHEME

## 1 INTRODUCTION

Nowadays, people use more and more e-commerce applications, like online-shopping and online-banking. Those online offers allow for attacks like phishing, pharming and man-in-the-middle attacks which try to steal the user's credentials in order to misuse his account. Advanced users would probably be able to detect those attacks, but the majority of the users are naïve users who do not think about security issues. Therefore, the technology has to help those users to avoid such attacks. In 2007, the authors of this work proposed to use trusted devices like PCs with a trusted platform module (TPM) or (trusted) mobile devices for authentication in e-commerce applications [1]. This paper presents a proof of concept implementation of that authentication protocol as well as its evaluation in a real world testbed.

The paper starts with a short introduction into the attacks to be avoided, goes on with an introduction into the proposed solution, its verification and implementation. It ends with an evaluation and a short conclusion.

## 2 PHISHING, PHARMING, AND MITM ATTACKS

Phishing, pharming and man-in-the-middle (MITM) attacks are the most dangerous user authentication attacks in online business today. Of course there are also other serious problems like key loggers and other kind of spyware on the user side, but those can be circumvented with an up-to-date anti-virus and anti-spy software or - for the advanced users - with intrusion detection and artificial immune systems. This work concentrates on an easy but efficient way to protect the user from phishing, pharming, and MITM attacks, which are described in detail in this section.

### 2.1 Phishing Attacks

Phishing attacks belong to the group of social engineering attacks. That means that they do not profit of a technical problem or bug but on careless or naïve users. Phishing relies on the idea that it is possible to talk the user into revealing her credentials by pretending to be a trusted organization

## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

with a trustable concern. Examples are e-mails claiming that there has been a problem with the users account at bank XY and in order to clarify that, the user should submit her credentials to a side referenced by a link in the e-mail. On first sight, that link might really look like it belongs to bank XY but it does not. It belongs to an evil site whose only goal it is to collect all those user credentials. After the user entered her credentials there will usually come a message thanking the user and confirming that the problem could be solved.

### **2.2 Pharming Attacks**

Pharming attacks have the goal to redirect the user to an evil website without forcing the user to click on the wrong link. This type of attack relies on manipulating the DNS entries or the host file on the user's machine. The user may then type the correct URL of the online shop or bank but will be directed to an evil page looking like the desired page but whose only value is to collect user credentials. After having given his credentials, the user will see an error message and get redirected to the original page.

### **2.3 Man-in-the-Middle Attacks**

Man-in-the-Middle (MITM) attacks are more sophisticated than pharming and phishing. As the name suggests, MITM attacks require an attacker to reside between user and the online service, she wants to reach. If the user wants to connect to the online service, she will instead connect to the MITM, who himself is connected to the online service. Instead of only stealing the user's credentials, the MITM can also modify transactions sent by the user. Imagine a user wants to connect to her bank. He will be connected to the MITM instead who forwards the user credentials to the bank (probably after having stored them). If the user then sends a transaction together with the transaction number (TAN), the attacker can easily alter the transaction as he also owns a TAN now. He will then send the altered transaction to the bank and reply with a wrong transaction confirmation to the user. Unlike phishing and pharming, this attack is also successful when using TANs and e-tokens.

### 3 STRONGER AUTHENTICATION IN E-COMMERCE

In 2007, the authors published their solution to protect the users against the attacks mentioned above [1]. They propose to implement an authentication protocol, that makes use of trusted devices like Trusted Platform Modules (TPMs) or mobile phones. A TPM is a small trusted chip, built into most of the computers shipped today, which has been specified by the Trusted Computing Group (TCG) [3]. This chip provides secure storage for keys and hashes and some basic cryptographic functions. Furthermore, it is the root of trust and measurements of a PC and may be identified uniquely worldwide. Such features make it extremely useful for authentication purposes. If there is no TPM available the authors of [1] propose to use a mobile phone as trusted device. To make a mobile phone really trustable, one might think about enhanced SIM cards like those from SanDisk [4] or the multimedia cards from Gemalto [5]. If neither TPM nor a trustable mobile phone is available, the authors propose to use One-Time Passwords (OTP) sent by SMS.

#### 3.1 Authentication Using a TPM

This authentication method is the most secure of all the three mentioned above. Before ever beginning such an authentication, there has to occur an offline key exchange between the online shop and the user. This can be done using signed snail mail. The user will get a CD-ROM from the online-shop containing the shops public key and a piece of software, that seals that key to the user's TPM, generates a new user key and prints the public part. The user then has to send the printed public key back to the online shop, who will store it electronically. Additionally that CD-ROM contains the client authentication software needed to run the authentication protocol with the server in case it cannot be expected to be implemented on every mainstream operating system.

The authentication protocol itself is more or less a standard challenge/response protocol, where the TPM calculates the challenge to the server and verifies its response. As mutual authentication is required for really secure authentication schemes, the server also has to trigger a challenge/response protocol, where the user's TPM has to calculate the response. After both runs, both sides can be sure, they are connected to whom they wanted to be connected. The security of this protocol relies on the TPM, that does all the



## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

security-critical tasks.

### 3.2 Authentication Using a Trustable Mobile Phone

As it might be possible that a user does not possess a modern computer with a TPM or that the user wants to connect to the online shop from another PC, the authors of [1] proposed another authentication using trustable mobile phones. A mobile phone becomes trustable when it either contains a Mobile Trusted Module (MTM) [6] or an extended SIM card that can run applications in its secure environment like those from SanDisk [4] or Gemalto [5].

Before starting an authentication with that device, there has to be an offline key exchange as mentioned above. This can be done using read-only memory cards, as most of the modern mobile phones have card slots. Printing the key from a mobile phone is obviously not easily possible. Therefore, the authors propose to deliver memory cards with a read-only part for the server's public key and the software mentioned above and a read-write part to store the clients key. If the user sends the memory card back using signed snail mail, it should not be possible to tamper with that key.

The authentication itself is very similar to the authentication using the TPM. The difference is that the server runs the challenge/ response protocols with the mobile phones and not with the computer, the user uses! As this does not secure the connection between the user's computer and the server, the server has to ask the user for a transaction confirmation on the mobile phones every time it receives a transaction request.

### 3.3 Authentication Without a Trusted Environment

There may be users that neither possess a PC with TPM nor a trustable mobile phones. But nowadays almost everybody possesses some kind of mobile phone no matter how old it is. Therefore, the authors of [1] propose to use One-Time Passwords (OTPs) as backup solution for those users. There is no offline key exchange in advance since there is no trusted medium on the user's side to store the keys. The only thing that has to be registered at the online shop in advance is the user's mobile phone number. For security reasons, this should be done using signed snail mail. Afterwards, if the user wants to connect to the online shop, he will get an OTP in a SMS on his mobile phone, that has to be sent back to the server to be really authenticated.

Later, every transaction request received by the shop has to be confirmed by the user using SMS.

## 4 AVISPA VERIFICATION

The AVISPA framework [7] stands for Automated Validation of Internet Security Protocols and Applications and provides a good and fast way to check protocols for security flaws.

### 4.1 Modeling of the E-Commerce Protocol

AVISPA provides a High Level Protocol Specification Language (HLPSL) [7] to model network protocol in order to prove their security. HLPSL models participants of the protocol as so called basic roles. In order to specify the basic roles, the protocol should be written in A-B (Alice - Bob) notation:

```
A->S: A
S->A: {Ns.S}_Ka
A->S: {Ns.Na}_Ks
S->A: {Na}_Ka
```

From that A-B notation, the basic roles can be specified easily. The following code snippet shows The HLPSL expression of the role A (the client in our case):

```
role alice(A,S: agent,
           Ka,Ks: public_key,
           SND,RCV: channel(dy))

played_by A def=
  local
  State: nat,
  Na,Ns: text
  init
  State := 0
  transition
  0. State=0 /\ RCV(start) =|>
     State':=2 /\ SND(A)
  2. State=2 /\ RCV({Ns'.S}_Ka) =|>
     State':=4 /\ Na':=new() /\ SND({Ns'.Na'}_Ks)
     /\ request(A,S,alice_server_ns,Ns')
```

## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

```
    /\ witness(A,S,alice_server_na,Na')
4. State=4 /\ RCV({Na'}_Ka) =|>
   State':=6 /\ secret(Na',na,{A,S})
```

end role

For a detailed description of the syntax see [7].

The security goals to check are the authentication between the server and client (A) and the secrecy of the nonces exchanges during the authentication. In HLPSL the goals are specified as follows:

```
goal
secrecy_of na,ns
authentication_on alice_server_na
authentication_on alice_server_ns
end goal
```

When verifying this protocol with AVISPA against the goals, no vulnerabilities have been found:

SUMMARY

SAFE

[...]

ATTACK TRACE

%% no attacks have been found..

Therefore, the protocol described in Section 3 can be assumed to be secure, which means that nobody can impersonate the client to be authenticated against the server and the nonces are not released to an attacker. Obviously, there has to precede a key exchange to secure the connections, but as this work concentrated on the authentication itself, the key exchange is not part of this paper.

## 5 PROOF OF CONCEPT IMPLEMENTATION

In 2008, there has been done a proof of concept implementation as part of a master thesis [2]. This implementation will be described in the following sections.

### 5.1 The TPM Emulator

As described in Section 3 TPM is an emerging technology on the market. But even if more and more laptops ships with TPM support there are still

many machines without a hardware TPM. Besides that, developing directly on the hardware TPM can be very annoying since the only way to reset a TPM is to reboot the machine. For these reasons M. Strasser developed a TPM emulator which comes as a Linux module [11]. But even if this TPM emulator enables older devices to use this technology, it should be clear that a software TPM will never be as secure as a hardware TPM.

## 5.2 TrouSerS - An Open Source TCG Software Stack

In order to keep the TPM a low cost device, the Trusted Computing Group (TCG) proposed to implement only the security critical functions inside the TPM and move the uncritical functions into the so called TCG Software Stack (TSS). One of the popular TSS implementations is called TrouSerS [9]. TrouSerS implements the TSS in C and is released under the Common Public License (CPL). It was developed by IBM. Today TrouSerS supports the TSS 1.1 specification and work on the TSS 1.2 specification has begun. Although TrouSerS deviates from the TSS specification in some points for more convenience, it is possible to compile it with strict TSS compliance.

## 5.3 Gammu

Gammu (GNU All Mobile Management Utilities) [10] is an open source project trying to close the gap between Linux and mobile phones. Gammu can connect to several mobile phones either over bluetooth or the USB sync cable. The mobile phone support goes from SMS sending and reading to placing phone calls and basic synchronization of the address-book and calendars. Gammu works perfectly with a Sony Ericsson K800i that we used. Gammu can be used as a normal application or in daemon mode. Furthermore, when running in daemon mode, Gammu supports two back-ends: a simple file back-end similar to mailboxes and a MySQL back-end. The latter one is interesting since no parsing is needed for reading out the content of a received SMS. Therefore, Gammu could be easily integrated into the mobile phone assisted authentication part of the protocol proposed in [1].

## 5.4 Implementation

All three methods described in Section 3 have been implemented. As the system should be comfortable and as transparent as possible to the user, it

## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

was one of the goals of the implementation that the built system is integrated seamlessly into an existing system. Only few changes are necessary to an existing login procedure in order to integrate the three protocols. In fact they can be inserted right after the standard login procedure and the redirection of the client to the landing page for logged in users. The TPM and the transaction confirmation protocols are delivered as PHP code to provide the functionality of the authentication server to PHP and a little C program which does actually the binding between PHP and the authentication server written in C and the necessary PHP code to provide the functionality of the authentication server to PHP. The implementation is based on a client-server

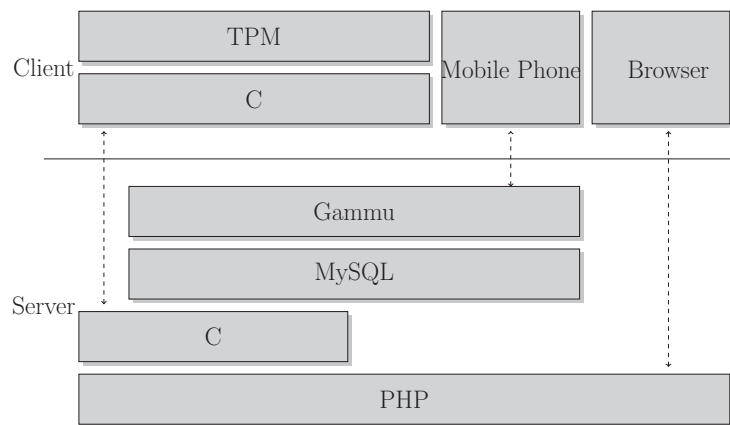


Figure 1: Layered model of the involved components

architecture, where the user of the e-commerce application plays always the role of the client. The figure 1 shows a layered model of the involved parties. Each layer can only communicate with the layer above/below. The communication between the client and the server uses HTTP for the browser, a TCP socket for the communication with the TPM and the GSM network g for the mobile cell phone.

For the mutual authentication with the TPM and the transaction confirmation over SMS, two server parts are needed: the HTTP server and the authentication server. The HTTP server is responsible to serve the HTML pages and do the standard login procedure. The authentication server is responsible for the mutual and the strong part of the authentication. The authentication server is written in C. It provides the following functionality: Allowing the TPM to authenticate and supporting the communication with

the HTTP server. The TPM authentication is based on a message exchange over sockets. Furthermore the user session will be created in PHP. It is therefore mandatory to inform PHP about a successful authentication.

The messages exchanged for the transaction confirmation use the GSM network. Therefore the authentication server only needs to check for incoming SMS and verify if they correspond to a transaction confirmation. If this is the case, the HTTP server is informed about a successful transaction.

The communication between the authentication server and the HTTP server relies on a broadcast server. The authentication server broadcasts successful TPM authentication and successful transaction confirmations over a broadcast channel. The HTTP server can listen to this message in order to decide whether the validation has been successful or not.

The SMS one-time-password implementation is slightly different. In order to authenticate, a user has to give its credentials plus the one-time-password received on his mobile cell phone. Just as for the TPM mutual authentication and for the transaction confirmation, the user session has to be created in PHP. However Gammu only needs to send an SMS. Sending an SMS through Gammu means to execute an INSERT query on the database which corresponds to Gammu. Since the answer will be sent back through the web page, there is no need for an additional authentication server listening to incoming SMS.

## 5.5 Evaluation

Having a more secure way to authenticate is nice. Being transparent to the user is also nice. But all this is worth nothing if the performance is bad. By performance we understand the additional server load due to the encryption and decryption of the messages, the additional server load due to the Gammu SMS server as well as the time needed to authenticate successfully to the system. These three measures are important. The first two for the service provider: if the increase of the server load is too high, no one will provide this type of authentication. The third measure is important for the user: the advantage of e-commerce applications is the rapidity of the service. If the login decreases the performance of the system too much, it loses this advantage.

Measuring the time a login takes is quite easy: just take a stop watch and do a login. However measuring the additional CPU consumption on the server is difficult. Having an accurate measure would require doing multiple

## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

connections from multiple clients at the same time, first without the TPM authentication and then with. Unfortunately it was not possible due to limited hardware resources, and therefore all measures have to be done using one server and one client with a TPM enabled machine, which still gives a good estimate of the resource consumption. The setup is as follows:

- The server is an Intel® Pentium® 4 3.00 GHz with 1Go RAM running an Ubuntu 32bit system.
- The client machine is an Intel® Core™2 Duo 2.26GHz with 2Go RAM, and Intel® TPM and running an Ubuntu 64bit system.

In order not to bias the experiment, only one client is authenticating to the server at a time. Besides that, the server and the client only run the necessary software to authenticate (this means a browser window and the authentication protocol on the client side and Apache, Gammu and the authentication server on the server side).

In the first test, 80 successive TPM authentications were done, but between each 5 authentications a pause of 10 minutes was accorded in order to give the TPM the time to clean up some stuff. The experience showed that the mean authentication time is 4.7 seconds and 75% of the measured times are less than 3.73 seconds. Besides that the additional server load due to the encryption and decryption of the exchanged messages stayed below 1%. These results are encouraging and prove that the implementation is usable.

The second and third security enhancements needs some additional hardware to enable the server to send and receive SMS. Gammu allows the sending and receiving of SMS through a cell-phone or other GSM capable device (like UMTS cards). For the following experiences a *Sony Ericsson K800i* was used as hardware back-end for Gammu. In order to evaluate the performance of the one-time-password login the following experiment was repeated 10 times and the time for each login measured:

- Enter the username and password.
- Wait for the SMS containing the one-time-password.
- Copy the received one-time-password into the browser.
- Submit the form to the server.
- Wait for the successful authentication.

The experiment showed that the mean authentication time is 19.5 seconds. Furthermore 75% of the login attempts took less than 21 seconds. Even if this is 4 times longer than the TPM authentication, this result is still quite satisfying compared to actually used systems.

The third test validated the usability of the transaction confirmation over the GSM network. Since two messages are exchanged over the GSM network the transaction confirmation takes more time than the one-time-password authentication. Experiments showed that the mean confirmation time is of 27.1 seconds. The experiment was made under the assumptions that the measurer knew how to reply to an SMS. Furthermore, the phone-number of the e-commerce application was the first number in the address-book of the cell-phone. This means that it took only four steps to insert the phone-number of the e-commerce application into the SMS. As before we can assume the time needed by the web-server to catch the submitted form and display the success page as negligible. The experiment showed that 75% of all mutual confirmations took less than 28.7 seconds. This make this system quite usable.

For the three presented systems it was proven that the measures follow a normal distribution which confirms that there are no side effect appearing with an increasing number of authentications/ confirmations. However the measures for the one-time-password and the mutual transaction confirmation only gives a rough idea of the performance of the system. In fact the receiving and sending of SMS depends on parameters relying on the GSM provider. Sending an SMS at New Year's eve will take much more time than sending the same SMS an ordinary Sunday morning.

## 6 CONCLUSION

This work presents a promising proof of concept implementation of a secure e-commerce authentication protocol formerly proposed by the authors. As the evaluation has shown, the presented protocol is usable in practice even in that early non-optimized state. The implementation proves to be done easily and is transparent to the user. Obviously the protocol also introduces a new degree of complexity as it requires either a TPM or a mobile phone. Furthermore the offline handshake option requires some work before connecting to a service. Therefore the e-commerce providers have to calculate the risk of those attacks for their application. It is clear that online-banking applications need more security, like using the TPM, than simple online-shops



## A Proof of Concept Implementation of a Secure E-Commerce Authentication Scheme

that might be secured sufficiently using the one time password. Concluding one can say, that the proposed protocol is a promising approach in order to implement a user-friendly and secure e-commerce authentication method.

### References

- [1] C. Latze and U. Ultes-Nitsche. Stronger Authentication in E-Commerce. How to Protect Even Naive Users Against Phishing, Pharming and MITM Attacks Communication Systems, Networks, and Applications (CSNA 2007), Beijing, China, October 2007
- [2] A. Ruppen Enabling stronger authentication mechanisms in todays e-commerce applications Master Thesis, April 2009
- [3] The Trusted Computing Group. Trusted Computing Platform Alliance. Main Specification Version 1.1b Trusted Computing Group 2003 Available at <https://www.trustedcomputinggroup.org/specs/TPM>
- [4] SanDisk SanDisk Mega SIM (tm) Available at [http://www.sandisk.com/oem/productcatalog\(1271\)-.aspx](http://www.sandisk.com/oem/productcatalog(1271)-.aspx)
- [5] Gemalto Gemalto Multimedia SIM Available at <http://www.gemalto.com/telecom>
- [6] The Trusted Computing Group. TCG Mobile Trusted Module Specification Trusted Computing Group 2008 Available at <https://www.trustedcomputinggroup.org/specs/mobilephone/>
- [7] The AVISPA Project <http://www.avispa-project.org/>
- [8] AVISPA Web Tool <http://www.avispa-project.org/web-interface/index.php>
- [9] TrouSerS <http://trousers.sf.net>
- [10] GNU All Mobile Management Utilities <http://www.gammu.org>
- [11] TPM Emulator <http://tpm-emulator.berlios.de/>

Proceedings of ISSA 2009

## USAGE CONTROL POLICY ENFORCEMENT IN OPENOFFICE.ORG AND INFORMATION FLOW

C. Schaefer<sup>1</sup>, T. Walter<sup>1</sup>, A. Pretschner<sup>2</sup>, M. Harvan<sup>3</sup>

<sup>1</sup>DOCOMO Euro-Labs  
Germany

<sup>2</sup>Fraunhofer IESE  
Germany

<sup>3</sup>ETH Zurich  
Information Security  
Switzerland

<sup>1</sup>[schaefer,walter]@docomolab-euro.com,

<sup>2</sup>Alexander.Pretschner@iese.fraunhofer.de, <sup>3</sup>mharvan@inf.ethz.ch

### ABSTRACT

Usage control is a generalisation of access control addressing how data is to be handled after it has been released. To control the data handling enforcement mechanisms have to be in place where the data is being used. These enforcement mechanisms can be implemented on different layers of the system. One way to do the enforcement is on the application layer. This paper describes how usage control policies can be enforced in OpenOffice.org using the component technology UNO (Universal Network Objects) provided by OpenOffice.org. The drawbacks and sketches how to overcome these are also identified.

### KEY WORDS

Information flow, usage control, policy enforcement

## USAGE CONTROL POLICY ENFORCEMENT IN OPENOFFICE.ORG AND INFORMATION FLOW

### 1 INTRODUCTION

In companies it is common to have a policy describing how sensitive information is to be used (sometimes referred to as *managed information*). Sensitive information can be construction plans for machines, documentation of a product or anything else containing secret information of a company. Policies to protect company assets can be seen as *usage control policies* as they go beyond standard access control policies. For example, it can be specified that no user besides the author can edit a patent application (access control policy), and that it must be stored in the company intranet only. Further, copying and pasting information is allowed within the document but not into another document (all the previous are usage control policies).

Theoretical work exists (see for example [4]) on how to specify these kind of policies. With respect to the above mentioned usage control policies we address three problems in this paper. First, it is not clear how to map *high level policies* to *low level policies* that can be enforced. Second, it is not obvious how to map *actions on data*, i.e. do not copy confidential data into another document, to *actions of processes on data*, i.e. using an office application and perform copy/paste. Third, we need to determine how to *control actions*.

The solution we employ is to define an information flow model for OpenOffice.org (OO). This allows us to define where control is applicable in OO (third of the above mentioned problems) and how high level policies are mapped to low level policies understood by OO (first problem). Obviously, the OO instance is the process that manipulates the data and it is this process to be controlled (second problem).

To verify our approach we have developed an architecture and prototypical implementation using the Universal Network Objects (UNO) component technology from OpenOffice.org. The implemented framework uses a description of what has to be enforced and intercepts all actions according to this description. Actions (like Print a document) performed by OO can either be allowed or forbidden; others (like Save as) can also be modified, e.g. allowing only a specific file format and a specific directory where the document can be saved. We show which requirements can be enforced by our architecture,

## Usage Control Policy Enforcement in OpenOffice.org and Information Flow

and provide examples of what we have implemented. Additionally we show the limitations of our approach.

Our contributions are the design and implementation of usage control enforcement in OpenOffice.org as well as the definition of an information flow model for office like applications. The information flow model is the basis for the development of the enforcement model. The enforcement model is capable to control all the information going into and out of OO. These are the first steps to an enforcement architecture for usage control policies.

The remainder of the paper is structured as follows. Section 2 introduces the related work and describes how UNO is working. A description of the information flow model is shown in Section 3. This is followed in Section 4 by a description of the architecture of the OpenOffice.org controller enforcing the usage control policies. Section 5 lists some limitations of this approach and is followed by the summary in section 6.

## 2 RELATED WORK

Usage control [10, 8] is a topic that has received some attention in the research community recently. It is a generalisation of access control and deals with how data is to be handled once it has been released to a third party. The existing work has laid theoretical foundations for usage control by for example specifying usage control languages. Digital rights mechanisms (DRM) are part of usage control and can be used as enforcement mechanisms.

### 2.1 Usage Control Enforcement

A classification of enforcement mechanisms which are needed for usage control is introduced in [11, 5]. *Inhibit* specifies actions that are forbidden like it is forbidden to print a document. *Finite delay* specifies the class where an action is delayed until some conditions are met, e.g. approval by management before a patent application is filed. It might occur in a usage control policy that a disclaimer “Printed by” has to be added to a document. This forms the third class *modify* as some additional information before the actual printing is added. The sending of a notification to someone else that the data has been modified falls in the *execute action* category.

Another paper [11] looked into existing DRM mechanisms and analysed which enforcement classes are supported by those mechanisms. The result was that all DRM mechanisms supported the inhibit class but only a few

mechanisms supported more classes. But no analysed mechanism supported all classes.

DRM systems, like the one used in Apple's iTunes, are currently focused on protection of multimedia content like audio and video. The mechanisms mainly provide access control and control the distribution of the content by not allowing to copy the content to other devices or only to a restricted number of other devices. Approaches like Sealed Media [6] or Microsoft's RMS [1] also exist which focus on the protection of documents. These approaches provide mechanisms for access control and the distribution of documents but again not all classes mentioned above like for example *modify* are supported. Our approach goes beyond the existing ones providing support for all enforcement classes.

## 2.2 OpenOffice.org and UNO

OpenOffice.org [3] is an open-source office software suite for word processing, spreadsheets, presentations, graphics and databases. It stores all data in an international open standard format (ODF - Open Document Format) [7].

OO provides an interface called UNO [2] with which OO can be controlled by external programs. The external program can either be integrated into OpenOffice as an extension (a plugin mechanism) or it can be a program running independently.

### 2.2.1 Dispatch Framework

OO has a so called *Dispatch Framework* [2] which defines interfaces for a generic communication between an office component (i.e. some functionality provided by OO) and a user interface. This communication process handles requests for command executions and gives information about the various attributes of an office component. The user interface sends messages to the office component and receives information from the office component.

The framework maintains a list of DispatchProviders. These DispatchProviders contain information about what to do when some execution command is coming from the user interface. When a command is issued the first DispatchProvider in the list suitable for this command performs all necessary actions. A DispatchProvider can also perform part of the work for the command and then pass on the control to another DispatchProvider which is then finishing the task.

### 2.2.2 Commands

Commands are the basic entities in the dispatch framework and are executed by the dispatch framework providing all the functionality necessary for an office suite. Save for example is a command that stores a modified document using the same name it was opened with. Commands are accessible through the menu or the button bar. The execution of a command might trigger an event (see Section 2.2.3) like OnPrint. Using UNO external programs can execute commands and for example print a document without the involvement of the user but adding the above mentioned disclaimer “Printed by”.

### 2.2.3 Events

UNO-Events [2] consist either of a pair of events describing the start of a command (e.g. OnLoad) and the end of a command (e.g. OnLoadDone) or they consist of one event describing either the beginning (e.g. OnPrint) or the end (e.g. OnNew) of a command. It is possible to receive these events through a subscription mechanism.

## 3 INFORMATION FLOW

As an intermediate step towards the enforcement of usage control policies in OO we define an information flow model for OO. The information flow model allows us to identify the actions that generate an information flow in and out of OO. As a next step towards the enforcement of usage control policies, the behaviour of these actions is to be controlled. Furthermore, these actions are the low-level actions which are the target of a mapping from high-level policy actions to low-level actions. For instance, a “do not edit” action is mapped onto inhibiting “copy”, “paste” and “cut” commands and their shortcuts.

### 3.1 OO Information Flow Model

We define the fundamental entities that make up the information flow model [9]. The level of abstraction chosen has been motivated by our consideration of keeping the model simple on one hand but powerful enough on the other to allow for an appropriate design and implementation of enforcement mechanisms. Thus, the chosen abstraction of a data item  $D$  to be controlled is a document as policies are defined for documents as a whole, and thus

modelling the content of the document down to the level of characters, paragraphs, graphics etc. would have been too detailed. Further, taking the current implementation of OO into account, the entity dealing with a document is the OO process itself, however a document opened by OO is worked on by an editor instance. Several editor instances form the set of principals  $P$ . Data containers  $C$  are files which are referenced by a file name (= identifier). A data container holds zero or more data items; i.e. documents that are stored in ordinary files, backup files or in memory. Given an editor instance, certain actions like Save trigger an information flow between data containers (from memory into the original file). The relevant actions, i.e. where information is flowing between containers, we consider are: Open, Save, Save as, New, Close, Copy, Cut, Paste, Export, Insert and Delete.

The information flow model is defined over the above entities. We define states to consist of two elements: a storage function that maps containers to sets of data items and that is of type  $C \rightarrow 2^D$ ; and a naming function that maps principals and identifiers to containers and that is hence of type  $P \times F \rightarrow C$  where  $F$  is the set of identifiers (i.e. file names). Intuitively, *storage functions* capture which data is stored in which containers. The intuition behind the naming function is that a principal has certain container accessed using a specific name. States are accordingly defined as  $\Sigma = (C \rightarrow 2^D) \times (P \times F \rightarrow C)$ . Transitions between two states are effected by principals that perform actions:  $\Sigma \times P \times A \rightarrow \Sigma$ .

The initial state of the system is given by the allocation of documents in containers and the OO instance running but no editor instance.

The idea of the information flow model is to provide one particular kind of semantics for a system, namely the information flow in-between different containers. Monitoring this information flow is a prerequisite for the implementation of enforcement mechanisms. In the following section we concentrate on the first aspect, i.e. information flow monitoring.

### 3.2 OO Information Flow Monitor

The above OO information flow model is represented in Figure 1. It shows an OO instance and the containers the OO instance is using. Note the special containers for Insert and Delete content as well as Export and the Clipboard. The memory container is implicit with the editor instances.

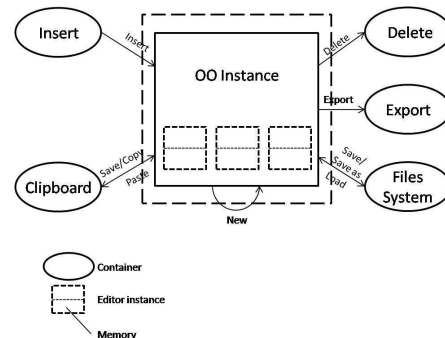
According to the model, an information flow monitor can be implemented and monitor all the information flow that crosses the stroked line. This



## Usage Control Policy Enforcement in OpenOffice.org and Information Flow

monitor would do a bookkeeping of when and where information has flown.

The stroked line also indicates where enforcement mechanisms have to be in place to enforce usage control policies. Thus the flow monitor is an integral part of the enforcement architecture.



## 4 ENFORCEMENT ARCHITECTURE

Figure 1: OO Information Flow Model

Using the above described UNO an OO controller was designed that enforces usage control policies using different enforcement mechanisms. Here an enforcement mechanism is a piece of software that checks if the execution of a specific command is allowed or not according to some policy and then can allow or forbid, sometimes modify the execution of this command. The controller is an external Java program that connects to an OO instance and can control OO completely.

The controller consists of four parts which all have different functionality. The mode manager (MM) (Section 4.3) manages the different modes the controller software can be in: normal or in enforcement mode depending on the current document. Additionally it has the responsibility to store the configuration of the enforcement mechanisms per document (Figure 2). The policy decision point (PDP) (Section 4.1) is the component which decides if a mode change is necessary and triggers the transition into the respective new mode. The policy enforcement point (PEP) (Section 4.2) receives the information about which enforcement mechanisms have to be used from the PDP (via the mode manager) and configures the enforcement mechanisms accordingly. The policy manager (Section 4.4) is responsible for reading in an XML configuration file. The file specifies the enforcement mechanisms and their parameters thus representing the usage control policy for the document(s) currently loaded. Using the information from the XML file the policy manager supplies the MM (via the PDP) with the correct configuration information. A more detailed explanation follows.

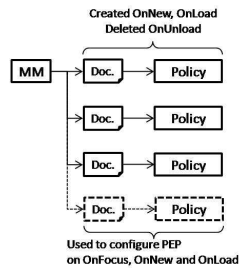


Figure 2: MM configuration

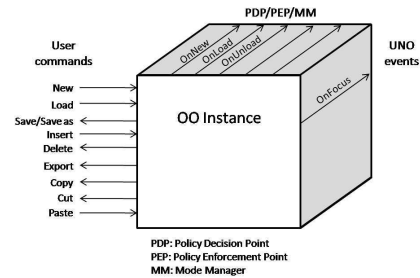


Figure 3: OO and PDP interaction

#### 4.1 PDP

The PDP interacts with the OO instance as shown in Figure 3. The OO instance receives user commands and generates UNO events as discussed in Section 2.2. The PDP listens for UNO events (for more details on UNO events see [2]) and intercepts their execution as further detailed below. The most important events we are interested in are OnNew, OnLoad, OnUnload and OnFocus. If the OnNew event is received the default enforcement mechanisms have to be applied. If the event OnUnload is received the mode manager needs to be triggered that the configuration for the closed document can be deleted from the list of possible modes (Section 4.3). OnFocus indicates that the user is looking at another document thus a different set of enforcement mechanisms might be applicable. At the OnLoad event an existing document is newly loaded into OO thus the current mode has to be changed and a new one has to be created using the configuration information for this newly loaded document.

As the PDP is only considering the events mentioned before there is a *static* configuration of the enforcement mechanisms for a specific document at its first access. So there is no *dynamic* policy update implemented at the moment which means that once the document is loaded no change in the number of enforcement mechanisms for this document is taking place. Furthermore the inhibitors are always active when a document has the focus. Thus, a user can not issue a *forbidden* command because all forbidden commands are disabled from the menu.

The decision if an action is allowed or not is partly delegated to the enforcement mechanisms. For example the Save as modifier is deciding if the storage path for a document is correct or not and if not correct modifies it. An extension to the PDP, but not implemented yet, is a state machine which

## Usage Control Policy Enforcement in OpenOffice.org and Information Flow

decides if an action is allowed or not depending on the current state and past behaviour. For example, a policy might exist that allows a document to be printed only three times. The PDP would then decide that after the document has been printed three times it must not be printed anymore.

### 4.2 PEP

The PEP gets the configuration information of the mechanisms from the PDP respective mode manager and configures the individual mechanisms which are described in more detail in the following (Figure 4).

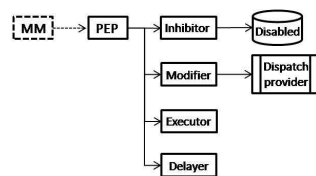


Figure 4: PEP configuration

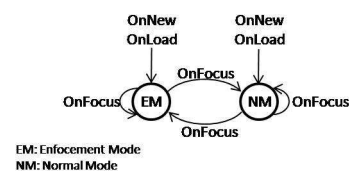


Figure 5: MM enforcement modes

Additionally the PEP sets the current enforcement mode whenever a document is newly loaded or focus changes; then the PEP acts as follows: First the inhibitor is used to disable the forbidden commands and if no command is forbidden all commands are enabled again.

Next existing modifiers are removed not to interfere with the new enforcement mode. After the removal it is checked if there are modifiers for this mode and which type of modifier (at the moment PrintModifier or SaveAsModifier can be selected) needs to be enabled. The name of the modifier is stored in a list. New modifiers are instantiated according to configuration information.

#### 4.2.1 Inhibitor

The inhibitor can block any command that OO can execute. It is for example possible to forbid a user printing a specific document by disabling the shortcut Ctrl-P to start the print job and the Print menu entry.

On a technical level it is implemented like follows. The inhibitor gets from the PEP a list of forbidden commands. These commands are inserted into a configuration list provided by OO<sup>1</sup> (Figure 4). This list defines the

<sup>1</sup>This configuration list is to be found in `/org.openoffice.Office.Commands/Execute/Disabled`.

commands currently disabled. After the insertion of the commands into the list the configuration of OO is refreshed and the inserted commands are not available anymore neither via the menu or the button bar nor via shortcuts. Modifying this list and refreshing the configuration of OO is done every time there is a switch to another document. So inhibiting commands is done depending on the document.

#### 4.2.2 Modifiers

The modifier is a `DispatchProvider` (Figure 4) which intercepts a command before it gets executed and modifies some parameters for this command. In OO every command has a so called `DispatchProvider` which implements the effect of the command. A newly written `DispatchProvider` can be executed before or instead of the original version. It can manipulate the parameters of a requested command or the content passed on to this command and then pass on the modified command and/or content to the original `DispatchProvider` where the command is finally executed. The new `DispatchProvider` can also perform some actions which are not executed in the original `DispatchProvider` and thus modify the result of the command execution.

Every document has its own list of `DispatchProviders` as for example a spreadsheet document needs other providers than a text document. Thus it is necessary to get the correct reference (frame) for the document so that the modifier can be inserted in the right list of `DispatchProviders`.

Modifiers have to be implemented using an abstract modifier class which requests that every modifier needs to implement the `configureModifier(...)` and `removeModifier()` methods. With the first method the modifier gets all necessary parameters for the configuration and the second method restores the original `DispatchProvider`. Furthermore `queryDispatch(...)` has to be re-implemented so that the correct (new) `DispatchProvider` is chosen, with all (new) functionality being implemented in the `dispatch(...)` method.

#### 4.2.3 Execution of Action & Finite Delay

The execution of actions and the finite delay is not implemented yet but similar to the modifier there may exist several different executors and delayers and thus a generic version of both can not be implemented. For this reason an abstract executor class and an abstract delayer class are defined which need to be implemented. Each of the classes has two methods. One method for the configuration and the other one for the removal of the classes.

### 4.3 Mode Manager

The mode manager is responsible for managing the enforcement modes the controller software can be in (Figure 5). Basically two modes exist. The normal mode (NM) where no enforcement mechanism is active and an enforcement mode (EM). The enforcement mode is described by the enforcement mechanisms and their configuration active for one particular document. It exists in several variants where each variant is associated with one open document and might have different enforcement mechanism configurations associated with it. Thus the current active mode depends on the current document and describes the enforcement mechanisms to be applied

The mode manager passes the necessary configuration information of the enforcement mechanisms for the current document to the PEP whenever a mode change happens (Figure 5).

Technically two classes for the mode manager exist. One class holds all mode information including docURL (a string representation of the document name containing the URL where the document is stored) for the document and if modifiers, inhibitors, delayers or executors are existing (inclusive configuration information for those) for this mode. The other class manages the list of modes that are currently needed as there is one mode per opened document and depending on the document the mode is changed. Thus if a document is loaded a mode for this document is created and if a document is unloaded the corresponding mode is deleted.

### 4.4 Policy Manager

The policy manager consists of two parts. The translator class configures a new mode by inserting the configuration information from the XML configuration file into the mode to be newly created.

The second part is reading the configuration information from the XML configuration file and finally passing it on to the translator class. The configuration file specifies which modifiers, inhibitors, delayers and executors are applicable for this document

## 5 REMARKS

As mentioned above there are some limitations to the enforcement of usage control policies in OO using UNO. There is no support of some kind of access control on UNO APIs. Thus every extension or external program can revert

the modifications done by the controller using the same API. Furthermore only the functions provided by OO can be controlled so it is for example possible to prevent sending a document by e-mail using the menu entry but if the menu entry is enabled it can not be controlled to whom the document is send as the e-mail program is external. Here a coordination with the e-mail program would be necessary to enforce the policy for the document.

The clipboard is a special case which can not be controlled completely by the OO controller software as the clipboard itself is an external component but nevertheless an integral part of OO. The controller software can not prevent a user from copying something into the clipboard so it needs the help of the clipboard itself to control the flow of information to the clipboard. So the clipboard should have a controller software, too, that can communicate with the OO controller. Whenever something is copied from OO to the clipboard the clipboard controller can ask for the policy of the document the content is coming from. The OO controller knows which document has currently the focus and from which content can be copied into the clipboard. Thus the OO controller can forward the appropriate policy to the clipboard controller. The clipboard controller can then allow or not allow the pasting of the clipboard content.

Summarizing it is necessary to have also controllers in the other parts of the system like for example in the clipboard, the e-mail program or the operating system. Only with all the other controllers that work together it is possible to completely enforce a usage control policy.

## 6 SUMMARY

The paper showed how enforcement mechanisms for usage control can be implemented, based on an information flow model, using the UNO of OpenOffice.org. It was explained how the controller software for OpenOffice.org is working which enforces usage control policies. For this means a XML configuration file is read in that describes the configuration of the enforcement mechanisms for a document subject to a usage control policy. The information in the configuration file is used to build an internal representation of the mode OO has to be in for this document. Depending on which document has the focus the appropriate enforcement mechanisms, as specified in the configuration file, are applied.

Additionally it was shown that not all possible usage control policies can be enforced as the controller is for an application with a limited set of

## Usage Control Policy Enforcement in OpenOffice.org and Information Flow

functionalities. Some other restrictions to this approach were shown as there is for example no access control on the APIs UNO is providing.

### References

- [1] Microsoft rights management services. <http://www.microsoft.com/rms>.
- [2] *OpenOffice.org Developer's Guide*. [http://doc.services.openoffice.org/wiki/Documentation/DevGuide/OpenOffice.org\\_Developers\\_Guide](http://doc.services.openoffice.org/wiki/Documentation/DevGuide/OpenOffice.org_Developers_Guide).
- [3] OpenOffice.org, April 2009. <http://www.openoffice.org>.
- [4] M. Hilty, A. Pretschner, C. Schaefer, and T. Walter. Enforcement for Usage Control: A System Model and a Policy Language for Distributed Usage Control. Technical Report I-ST-20, DOCOMO Euro-Labs, December 2006.
- [5] J. Ligatti, L. Bauer, and D. Walker. Edit Automata: Enforcement Mechanisms for Run-time Security Policies. *International Journal of Information Security*, 4(1-2):2–16, February 2005.
- [6] S. Media. *Sealed Media Enterprise DRM - How it works*. Sealed Media, July 2006. [http://www.sealedmedia.com/products/how\\_sm\\_works.htm](http://www.sealedmedia.com/products/how_sm_works.htm).
- [7] OASIS. OASIS Open Document Format for Office Applications (OpenDocument), July 2008. [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=office](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office).
- [8] J. Park and R. Sandhu. The UCON ABC Usage Control Model. *ACM Transactions on Informations and Systems Security*, 7:128–174, 2004.
- [9] A. Pretschner, M. Büchler, M. Harvan, C. Schaefer, and T. Walter. Usage Control Policy Enforcement without and with Information Flow. Technical Report T5010131, DOCOMO Euro-Labs, February 2009.
- [10] A. Pretschner, M. Hilty, and D. Basin. Distributed Usage Control. *CACM*, 49(9):39–44, September 2006.
- [11] A. Pretschner, M. Hilty, F. Schütz, C. Schaefer, and T. Walter. Usage Control Enforcement - Present and Future. *IEEE Security & Privacy*, 6:44–53, July/August 2008.

Proceedings of ISSA 2009



The Design of a Logical Traffic Isolation Forensic Model

## THE DESIGN OF A LOGICAL TRAFFIC ISOLATION FORENSIC MODEL

<sup>1</sup>Innocentia Dlamini, <sup>2</sup>Martin Olivier

Information and Computer Security Architectures Research Group (ICSA)

Department of Computer Science, University of Pretoria

<sup>1</sup>idlamini@csir.co.za, <sup>2</sup>molivier@cs.up.ac.za

### ABSTRACT

The network evidence currently presented in a court of law is often insufficient for prosecution purposes due to a loss of packets during the network transmission. Such packet loss may be caused by the congestion of data transmitted over the network, which only serves to further compound the delay in data transmission. The paper in hand extends the earlier work done on a forensic model for traffic isolation based on Differentiated Services (DiffServ). The logical traffic isolation (LTI) forensic model intends to solve the packet loss problem that may cause evidence to be insufficient. It isolates suspicious traffic from the normal flow by placing it on a dedicated route using DiffServ prioritising characteristics that avoid congestion of the suspicious traffic. The LTI model further includes a preservation station that serves to record all suspicious traffic before it is forwarded to its destination. This paper focuses on the analysis and design of the LTI model. An attempt is made to design a more flexible and reliable system – with a minimal loss of evidence – by incorporating some of the design algorithms.

### KEY WORDS

Differentiated services, preservation station, network forensics, suspicious traffic, unified modelling language, Network Intrusion Detection System.

## THE DESIGN OF A LOGICAL TRAFFIC ISOLATION FORENSIC MODEL

### 1 INTRODUCTION

This paper presents the design of the concept of a forensic model for Logical Traffic Isolation (LTI) based on Differentiated Services (DiffServ), as proposed by Strauss et al. [1]. Whenever network forensic investigations need to be performed, it is to the advantage of investigators if the crime is still in progress [2]. Seeing that they do not have to shut down the communication, they can often succeed in gathering enough evidence. The LTI model intends to solve the packet loss problem that can be the cause of insufficient evidence. It isolates suspicious traffic from the normal flow and places it on a dedicated route using DiffServ prioritising characteristics, thus avoiding a congestion of the suspicious traffic. The LTI model also includes a preservation station that serves to record all suspicious traffic before it is forwarded to its destination.

The LTI model utilises the DiffServ approach to isolate malicious traffic from normal traffic [1]. This could well reduce cost, since DiffServ is a standard technique. If a DiffServ infrastructure is already in place where an investigation needs to be performed, evidence collection could be facilitated with minimal changes to the network. The DiffServ approach allows Network Forensic investigators to attach both their marking station (ingress router) and preservation station to a cyber victim's network. The purpose of the marking station is to isolate the suspicious traffic and that of the preservation station is to investigate the situation at hand. The advantage of this approach is that it requires minimal network downtime and, most importantly, minimal network reconfiguration. This DiffServ-based scheme makes provision for a preservation station to store records of the isolated traffic with a view to its later analysis [1].

However, in order to minimise network transmission problems such as transmission delays and high network traffic, the preservation station proposes to store only records related to malicious network traffic. While

## The Design of a Logical Traffic Isolation Forensic Model

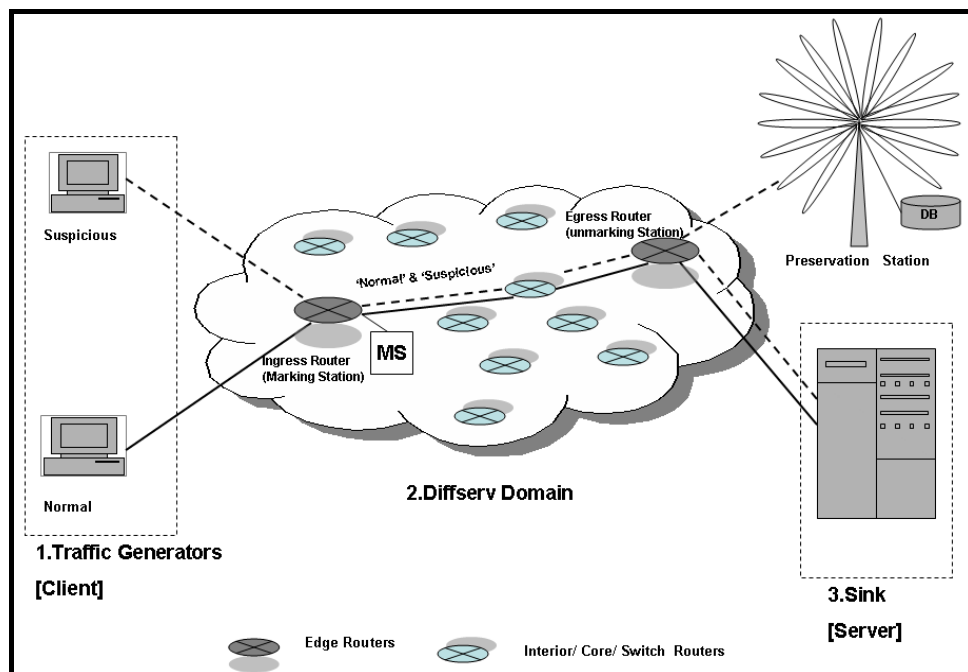
the proposal seems plausible, it has not been tested yet to prove the LTI system's viability. In order to ensure a successful and reliable implementation, this paper uses various design techniques in modelling the LTI model. A Unified Modelling Language (UML) technique is favoured in most of the cases. It provides abundant diagrams that can explicitly depict most of the processes and the interaction between the components of the LTI model. The rest of the paper is structured as follows: Section 2 discusses the architecture of the LTI model. Section 3 presents a design of the LTI model using the system design technique, while Section 4 serves to conclude the paper.

## 2 THE LTI ARCHITECTURAL MODEL

The design stage started with a careful revision of the requirements of the LTI system that were defined by Strauss et al. [1] after adding further elements. Some of the requirements included the type of network setup already in place. The system is intended to solve the problem of inefficient and inadequate evidence by introducing a preservation station for capturing identified packets. This station can be easily plugged into the network whenever an intrusion has been detected, thus allowing the system to immediately conduct an investigation while the suspected cyber-crime is being committed, i.e. live-network forensics. [2]

For experimentation reasons, the LTI system should have seven nodes: two nodes on a traffic generator that act as users and generate normal and suspicious traffic randomly; three nodes or routers on the DiffServ network, in other words the ingress, immediate and egress routers; and a sixth node that is the preservation station for recording the traffic that has been detected as suspicious. The last node is the sink server that receives and processes the requests generated. (Both the traffic generator and the sink server are additional nodes.) The LTI system should be able to isolate the two types of generated traffics within the DiffServ network and record the suspicious packets at the preservation station. The system is designed on the basis of three assumptions: (1) The network has its intrusion detection system in place; (2) There are various users transmitting data (represented by a traffic generator for experimentation purposes); and (3) The receiver or the destination node is represented by the sink server.

The requirements of the system served as the foundation for this study and resulted in the following implementation infrastructure of the LTI model (see Figure 1). It provides a conceptual view of the LTI model based on DiffServ for isolating suspicious traffic. The model consists of two traffic generators on the client side to initiate suspicious and normal traffic and of the DiffServ network with three routers (ingress, interior and egress) for experimental purposes. The preservation station ensures forensic soundness and system reliability [3] [4], while the sink server receives and responds to all the requests generated by the traffic generator. This nodal setup is, however, for experimentation purposes only.



*Figure 1: The Implementation Infrastructure of the LTI model using DiffServ*

The two clients generate normal and suspicious traffic and forward these packets to the DiffServ domain. The ingress edge router at the entrance boundary of the DiffServ domain is the first domain recipient and serves as a marking station. This router is responsible for *packet classification* and has *marking*, *shaping* and *dropping* capabilities. The ingress router marks any suspicious traffic by using the packet classifier

## The Design of a Logical Traffic Isolation Forensic Model

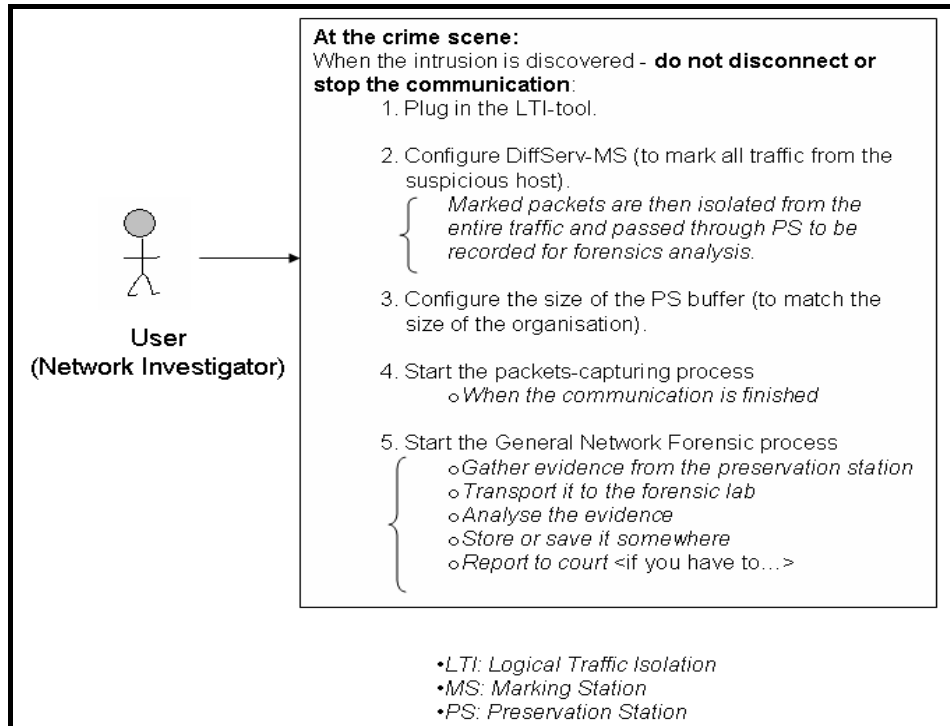
and forwards them to the nearest core router. The core routers are found within the centre of the DiffServ domain, and they simply forward traffic towards the egress router. The egress router is found at the exit boundary of the DiffServ domain. It unmarks the traffic and decides the destination of each network packet according to its behaviour: compromised traffic is forwarded to the preservation station and then to the sink server, while normal traffic is sent directly to the sink server. In a network-related cyber incident, the investigator searches the preservation station when conducting his/her investigation and captures all recorded suspicious network packets as evidence. The LTI model is further formalised in various UML diagrams. This includes the sequence diagram and activity diagram. The following section discusses the design of the LTI model in detail.

### **3 THE LTI SYSTEM DESIGN**

The second step in the design of the LTI model is its representation using the UML design technique. Although the UML is not a cure-all, it does simplify our work. These diagrams do not include too much detailed information; they simply depict the applicability and functionality of the LTI model and the involvement of the requirements of the system.

#### **3.1 The LTI System Scenarios**

In Figure 2, the Network Investigator (the actor) interacts with the system by performing different processes.



*Figure 2: The Scenarios Involved in the Logical Traffic Isolation system*

These processes are:

- Plug in the LTI tool
- Configure DiffServ-Marking Station (MS)
- Configure the buffer size of the Preservation Station (PS)
- Start the packets-capturing process
- Start the Network Forensics [2] investigation into the system

The LTI model involves all of the above processes during the course of an intrusion; in other words, it starts immediately when the intrusion has been detected.

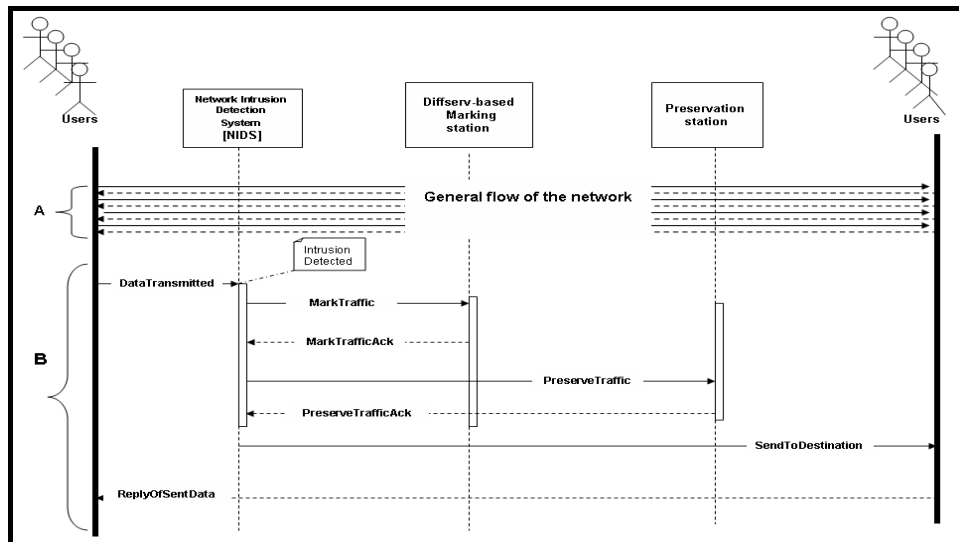
When an investigator arrives at the crime scene, the suspicious communication has to be left up and running in order to capture and record the detected packets. The LTI tool should easily plug into the

## The Design of a Logical Traffic Isolation Forensic Model

affected network and require only minor configuration to suit the size of the network at hand. Such configuration includes enabling the marking station to mark the packets from the suspicious host, considering the buffer size of the preservation station and ensuring correspondence with the size of the organisation. When the necessary configuration has been completed, the investigator can start the tool to capture suspicious packets. As soon as the suspicious communication is over, the normal network forensics processes can be initiated (see Figure 2, note 5). The processes involved in the LTI model can be arranged into different sequences, as is discussed in the following subsection.

### 3.2 The Sequence Diagram of the LTI Model

A sequence diagram is also part of the UML. It is used to show how processes operate with one another and in what order. Figure 3 depicts five components.



*Figure 3: Sequence Diagram for the Logical Traffic Isolation System*

These components include the users, a Network Intrusion Detection System (NIDS) (this can be any detection system; it differs from one organisation to the next), DiffServ network, a preservation station and the sink server. As mentioned above, the NIDS and sink server are part of the model. Two categories of traffic can be distinguished – suspicious and normal traffic. These are randomly generated. In Figure 3 above, Scenario A represents the normal network traffic flowing from the users to their destinations (which is represented by the sink server for supporting the experimentation of the LTI model).

This network passes through all the nodes, except the preservation station. Scenario B represents the sequence when suspicious traffic has been detected. The NIDS system reports to the DiffServ module to mark this traffic and give it higher priority. It also provides proper routing methods to find it, as suspicious traffic is the type of traffic that is special and significant to the cyber investigator. Suspicious traffic is first routed to the preservation station to be recorded, after which it is allowed to be routed to its destination. The ReplyOfSentData shown by dotted lines depicts the destination user's reply to the initiation user's request. The same procedure as in B can also be applied to show the response of the targeted system. As part of the UML diagrams, the activity diagram is used in the following subsection to show the activities performed by the actors involved in the LTI system.

### 3.3 The Activity Diagram of the LTI Model

Activity diagrams provide another means for clarifying which actor carries out which activity. Consider the activity diagram in Figure 4, which provides a breakdown of main activities into different subactivities. This diagram starts with normal flow of the network, assuming that a detection system is already in place. The latter serves as a deciding device as it informs the network administrator of any detected incident.

The network administrator easily plugs in the LTI tool and then configures the marking station to mark the packets of detected traffic. The LTI system checks whether the packets have been marked, and if not, sends them back. Once they have been marked, they are forwarded to the preservation station to be recorded. The system again checks to ensure that



The Design of a Logical Traffic Isolation Forensic Model

packets have indeed been recorded and sends them back if not. Once they have been recorded, they are sent on to their destination (sink server is used in our model as a supporting node). The system continuously checks whether more packets should be detected and, if this is the case, returns them to the marking station to start the process again.

The Network Forensics [2] [5] investigation process commences at this stage and its activities are included in a type of activity diagram. The investigation process is initiated and the approved Network Forensic tool is used to collect the evidence recorded by the preservation station. This step continues until all evidence has been gathered. The next activity that is performed is the transportation of forensic evidence to the forensic lab; followed by the analysis of all evidence gathered.

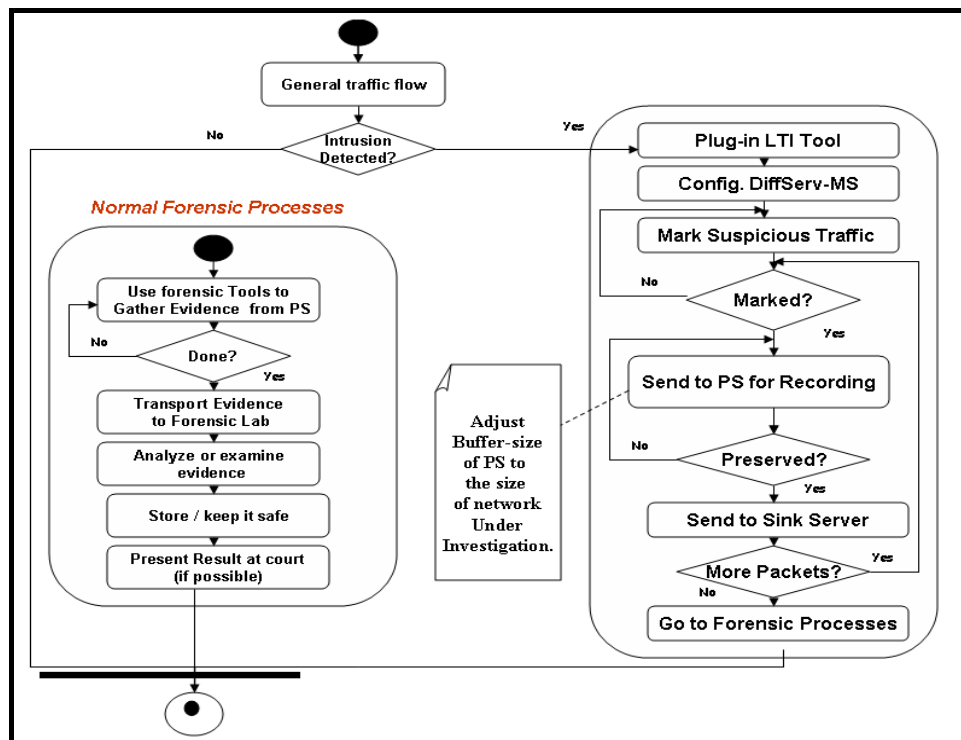


Figure 4: Activity Diagram for the Logical Traffic Isolation system

The findings of such analyses are stored in a place that is adequately safe while waiting for the court date. The final activity is the presentation of evidence in the form of a report to a court of law if this is deemed necessary. The next subsection discusses the class diagram of the LTI model.

### 3.4 The Class Diagram of the LTI Model

A class diagram is formulated from the components mentioned above. Figure 5 depicts the class diagram of the LTI system. Some Object-Oriented design principles [6] that were considered during the modelling of this class diagram are as follows:

*“... strive for loosely coupled design between objects that interact (p. 53); ...open-close principles (p. 86); ... favour composition over inheritance (p. 75)”* [6].

The relationship between the subject and the observers in the observer pattern complies with the design principle for favouring composition over inheritance, while the communication between the subject and the observers is kept loosely coupled. The open-close principle is implemented by the decorator pattern through allowing the behaviour of the traffic generated to be extended without any modification to the entire code. The traffic generator and the sink server objects use the DiffServ object for communication. This reduces the number of messages sent between the objects in the system and DiffServ therefore acts as a mediator.

Three design patterns are used in modelling the LTI architecture, namely the Decorator, Observer and Mediator patterns. The decorator pattern [6] is used to randomly wrap the behaviour of the traffic generated. The observer pattern [6] [7] is interchangeably used in most of the components of the LTI model, including the traffic generator, DiffServ, preservation station and sink server. The mediator pattern [8] [9] is used to coordinate the traffic generator with the preservation station or sink server components.

The Design of a Logical Traffic Isolation Forensic Model

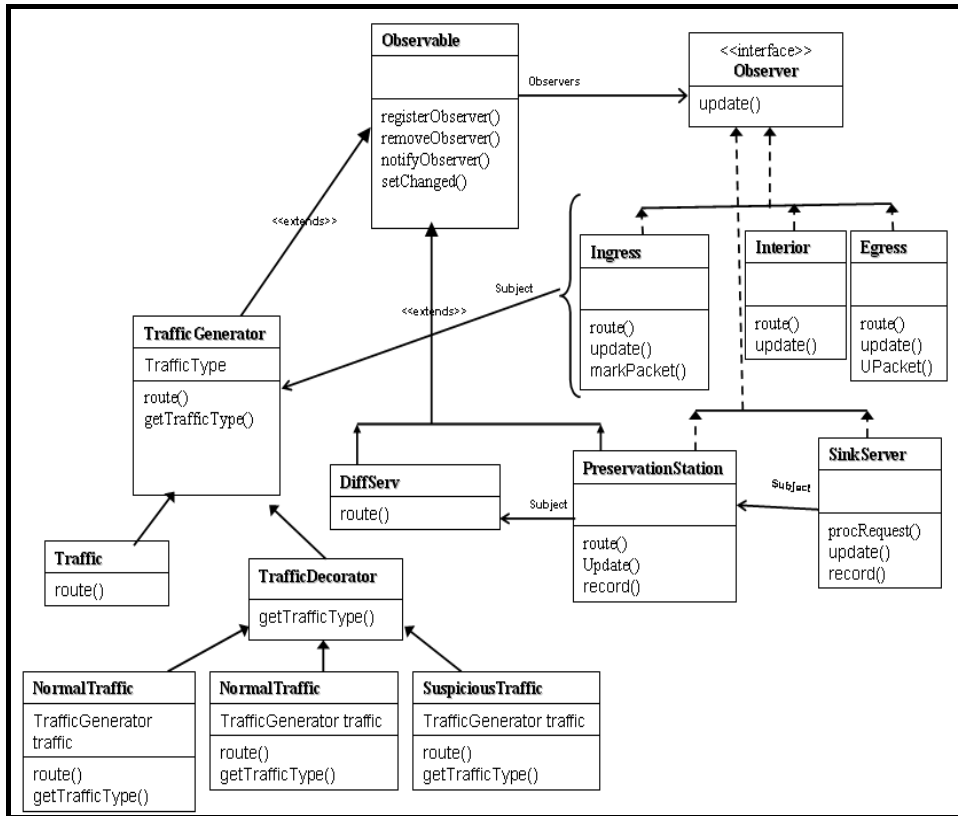


Figure 5: The Class Diagram of the LTI model using DiffServ

#### 4 CONCLUSION

This paper uses the UML design technique in most of the cases to present the LTI model. According to the specified requirements of the system, various design diagrams (the sequence diagram, activity diagram and class diagram) are used to represent the model. These diagrams specify in detail the role of each component of the system and the interaction between investigator and system, as well as the precautions that must be kept in mind when handling each piece of evidence. The use of these diagrams simplifies the LTI model and facilitates its easy implementation. The LTI model is currently in the process of being implemented, and the necessary

performance evaluation and tests should therefore still be carried out in future.

## 5 REFERENCES

- [1] Strauss, T., Olivier, M.S. & Kourie, D.G. 2006, Differentiated Services for Logical Traffic Isolation, in M.S. Olivier and S. Sheno (Eds), *Advances in Digital Forensics II*, pp. 229-237, Springer.
- [2] Corey, V., Peterman, C., Shearin, S., Greenberg, M.S. & Van Bokkelen, J. 2002, *Network Forensics Analysis, Internet Computing*, Volume 6, pp. 60- 66, IEEE.
- [3] Solomon, M.G., Barrett, D. & Broom, N. 2005, *The Need for Computer Forensics*, in L. Newman and W.G. Kruse (Eds), *Computer Forensics Jump Start*, pp. 01-20, SYBEX Inc.
- [4] Kohn, M., Eloff, J. & Olivier, M.S. 2006, *Framework for a Digital Forensic Investigation*, in H.S. Venter, J.H.P. Eloff, L. Labuschagne and M.M. Eloff (Eds), *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, Sandton, South Africa (published electronically).
- [5] Zantyko, K. 2007, *Commentary: Defining Digital Forensics*, *Forensic Magazine*, 20, Vicon Publishing, Feb-March 2007 issue, [Online] Available at: <http://www.forensicmag.com/articles.asp? pid=130>, as on 12 April 2008.
- [6] Freeman, E. & Sierra, K. 2004, *Head First Design Patterns, Volume 1*, O'Reilly Media, Sebastopol (CA), USA.
- [7] Shalloway, A. & Trott, J. 2001, *Design Patterns Explained: A New Perspective on Object-Oriented Design*, Addison-Wesley.
- [8] Bains, K. & Lau, E. 2002, *Mediator Design Pattern*. Available at: <http://sern.ucalgary.ca/courses/SENG/443/W02/assignments/Mediator/>, University of Calgary.
- [9] Black, S. 2004, *Mediator Design Pattern*. Available at: <http://stevenblack.com/PTN-Mediator>. ASP. Steven Black Consulting.
- [10] [GoF] Gamma, E., Helm, R., Johnson, R. and Vlissides, J. 1996, *Design Patterns. Elements of Reusable Object-Oriented Software*. Addison-Wesley. ISBN 0-201-63361-2.

Methodology for Considering Environments and  
Culture in Developing Information Security Systems

# **METHODOLOGY FOR CONSIDERING ENVIRONMENTS AND CULTURE IN DEVELOPING INFORMATION SECURITY SYSTEMS**

Jeffy Mwakalinga, Stewart Kowalski, and Louise Yngström

Department of Computer and System Sciences,  
Stockholm University/Royal Institute of Technology,  
164 40, Kista, Sweden

Tel: +468 161 721 Fax: +468 703 9025

*jeffy@dsv.su.se, stewart@dsv.su.se, louise@dsv.su.se*

## **ABSTRACT**

In this paper we describe a methodology for considering culture of users and environments when developing information security systems. We discuss the problem of how researchers and developers of security for information systems have had difficulties in considering culture of users and environments when they develop information security systems. This has created environments where people serve technology instead of technology serving people. Users have been considered just as any other component in an information system which has resulted in having efficient technical controls but inadequate social controls for security. In this paper we propose a new security framework that considers culture of users and system environments in developing information security systems.

## **KEY WORDS**

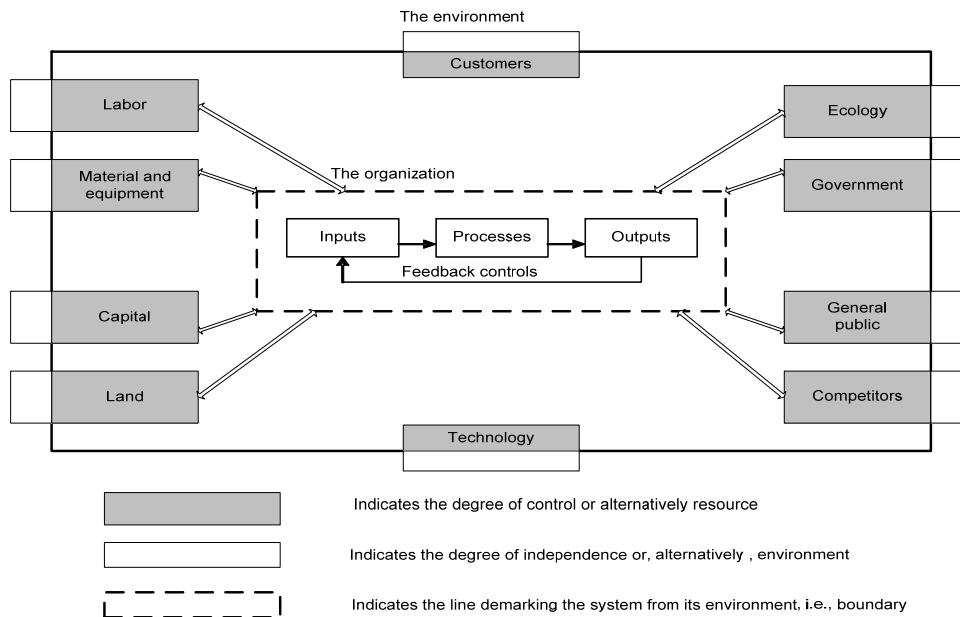
Deterrence, response, recovery, value-based chain, adaptability, environments, and detection

## 1 INTRODUCTION

### 1.1 Information Systems and Environments

Information systems have to learn to adapt to different system environments and to cultural environments. “A system is here defined as a set of objects together with relationships between the objects and between their attributes related to each other and their environment so to form whole” [22]. An information system can be modelled to consist of abstract systems, (information), living systems (people), and concrete systems (technology) [12]. “Churchman defines environment as those factors which not only are outside the system’s control but which determine in part how the system performs” [22]. An environment of an information system is outside of the control of an information system. There are hostile and friendly environments and an information system must be able to learn and adapt in both the hostile and friendly environments. Who defines the boundary between a system and its environment? What are the factors that set this boundary? Every information system has internal and external environments [22]. We suggest that values of people (culture, traditions, laws, policies, and other social issues) and geographical boundaries need also to be considered when an information systems security designer set the boundary between a system and its environment. Currently with information system designers and developers of IT set the boundary between a system and an environment for users without asking their values. Users of information systems cannot really be regarded as system owners as long as their systems cannot be controlled or defended. The organization has the following environments: labour, customers, ecology, public, material and equipment, land, capital, government, competitors, and technology but an organization controls only part of the environments, as shown in figure 1[22].

## Methodology for Considering Environments and Culture in Developing Information Security Systems



*Figure 1: Organization: Its resources and its environment [22]*

### 1.2 Culture and Information Systems

There have been concerns about the role of culture in information systems [20]. Culture has been defined differently by different scholars [10]. Van Dam, Evers and Arts define culture as a set of values, attitudes, and behaviours that people learn or are passed over to them over a period of time [26]. There is a general agreement among information system researchers that culture affects the way individuals' interact with complex information systems [20]. However, a model has not been developed to measure the effect of culture to individuals. They [20] write,

“Science educators, from Japan, India and Africa, appear to share a common understanding that science needs to be perceived in a cultural context and to link the development of scientific literacy with an understanding of worldview.

Between them, they have examined the faiths, philosophies and logic of students from various cultures to examine, within a culture, the conflict between ‘scientific’ and traditional concepts of science. Some have been able to link traditional belief and the understanding of scientific concepts or performance of experimental tasks. Others have also shown that science teachers’ worldviews and their traditional beliefs affect their teaching and thus their students’ learning.”

Another question is how much culture affects the decisions that an individual makes when using computer systems [20]. Further concern is whether a function that is provided by an Internet system is consistent across cultures [20]. Van Dam, Evers, Arts did a survey in three different cultures, Moroccan, Surinamese, and Dutch, on user experiences on e-government sites [26]. The results show that Dutch and Surinamese could notice titles on the left side faster while the Moroccan could notice things on the right sides of pages faster. The Moroccans are sensitive to green and red colours. This is because the Moroccans started to read from right to left. Dutch showed a less degree of uncertainty avoidance and they did not read in details but just browsed. The Moroccan needed confirmation that they are performing alright while Dutch and Surinamese did not need this confirmation. The Moroccan culture is a masculine culture in which recognition of achievement is important to participants. Dutch and Surinamese are feminine and they did not need recognition of achievement. Also the Surinamese and Dutch are neutral in culture, which means that showing emotion is regarded as unprofessional. The Moroccan culture is affective which implies that showing of emotion is regarded as normal. The Moroccan is a collectivist culture and it believes that the government website can not have mistakes and so the Moroccans blamed themselves for the mistakes. The Dutch and Surinamese are individualists and they blamed the system for the mistakes. The conclusion was that people with different culture backgrounds experience different problems in using e-government applications.



## Methodology for Considering Environments and Culture in Developing Information Security Systems

We have created a new security framework [17] [30] that is based on the Systemic-Holistic approach and the Immune system. The new security framework is a function of the deterrence, protection, detection, response, recovery value-based chain functions. The new security framework applies the system theory and holistic approach to provide security for information. The new security framework applies the principles of the immune system to make systems learn to adapt to environments. We apply the software agents to provide security services in analogy to B-cells and T-cells in immune systems.

## **2 THE STEPS TO TAKE WHEN CONSIDERING CULTURE OF USERS AND SYSTEM ENVIRONMENTS IN THE NEW SECURITY FRAMEWORK**

### **2.1 Analyze the threat agent**

In the first step we start by analyzing the threat agent based on the socio-technical economical system [15]. We document the states that an enemy of an information system could control and the states that an information system owner could control. We created the model of the enemy in which we analyze the methods, tools and processes that an enemy to the systems can apply to attack information systems.

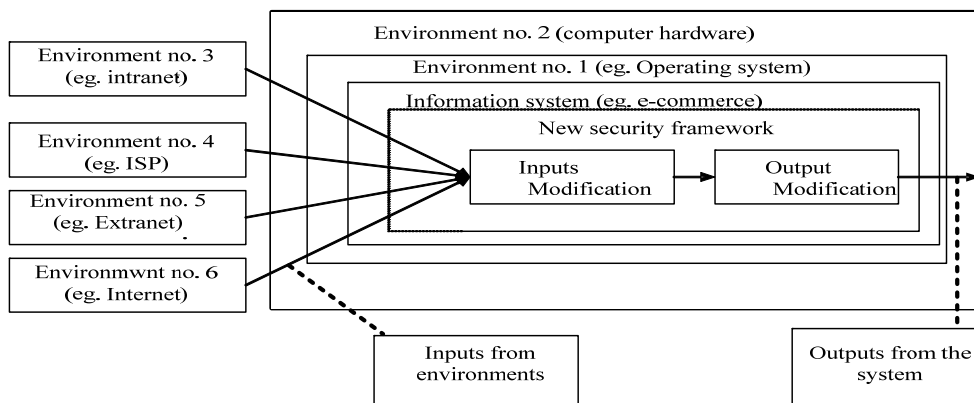
### **2.2 Classify Assets and perform risk management**

The second step is to classify the assets and perform risk management in an information system. We have automated the classification of assets and risk management using software agents. The recovery sub system of the new security framework identifies, assesses, and manages risks. Risk management is based on the Enterprise Risk Management (ERM) – Integrated Framework of the Committee of Sponsoring Organizations of the Tread way Commission (COSO) [21].

### **2.3 Analyze environments where the systems in focus operate**

The third step is to analyze the information system environments in the information system. This involves identifying the local environment, embedded environment, total environment, and predicting future

environments [1] [27]. It also involves classifying the environments, analyzing the levels of security of these environments. We identify the environments where a system will be operating. An observation is made over a period of time to study the inputs that are coming and affecting an information system. Then the sources of the inputs have to be studied and traced. Some inputs could be more complicated as they are a result of several environments integrated together. After identifying the inputs, we have to find ways of modifying the inputs so that they do not affect the general state of information system as shown in figure 2. Modification of inputs and outputs is done using the Cybernetics feedback mechanisms [22]. There are a number of ways in which we could classify environments [22]. In this work, we choose to classify the environments based on their complexities, dynamism and security levels of environments.



*Figure 2: Inputs from Environments*

An environment could be simple and static, simple and dynamic, static and complex, or dynamic and complex [22]. A static and simple environment has: few factors and components; homogenous factors and components; factors and components that do not change; a stable environment [22]. A complex and static environment has: large number of factors and components; heterogeneous factors and components; factors and components that do not change; unstable environment. The simple and dynamic environment has:

## Methodology for Considering Environments and Culture in Developing Information Security Systems

few factors and components; similar factors and components; unstable environment; the state of factors and components that change; rate of change of change could be stable or unstable. A complex and dynamic environment has: large number of factors and components; heterogeneous factors and components; high level of uncertainty; unstable environment; the state of factors and components change and the rate of change could be stable or unstable [22]. Examples of environments affecting information systems include an operating system, computer hardware, intranet, Internet Service Provider (ISP), education, hardware, operating systems, electric power, heating, cooling, floods, earthquakes, fire, and cultural environments. What sets the boundary among different environments? Is it policies, ethics, culture, or laws?

The next step is to analyze, using the Systemic-Holistic Approach, the correctness of an environmental systems (like the operating system where an information system is running) at the theoretical/model, design/architecture, and implementation levels [27]. We apply different standards and criteria to analyze the correctness of environmental systems. We analyze the correctness at the different levels because a standard of a system can be correct but its implementation can be wrong. An example of this is the Wired Equivalent Privacy (WEP) encryption system for wireless systems. This encryption system bases on the stream cipher RC4. The algorithm of RC4 does not have flaws but the implementation, the key scheduling and management facilities, is flawed [2]. Many algorithms are basing on wrong mathematical assumptions, which can lead to vulnerabilities in security systems at the higher levels. Then we need to have proofs of correctness at the design and implementation levels.

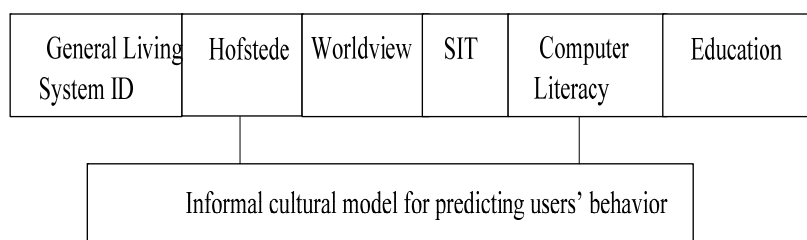
### **2.4 Assess the effects of culture and traditions of users to information security**

The fifth step is to assess the effects of culture and traditions of users to information security in this information system. We apply the informal cultural model, figure 3, to predict the behaviours of users. Chaula and

Yngström made a study in [4], where they examined how human behaviour affects systems security. They found that people with low uncertainty avoidance tend to lack holistic approaches to security which implies that they: lack security in depth measures; “lack attention to details”; tend have “poor risk assessment”; have “poor assumption about motivation, opportunity and methods”; “lack of information classification”, use metrics poorly [4]. Cultures where people have low future orientation have ineffective contingency planning. This affects prediction of disasters and preparation if an attack or a disaster was to occur. Cultures where power distance was high result in poor communication on security issues between upper level management and employees and technicians [3] [4]. In low power distance cultures communication and discussion on security issue was better but readiness to report unethical conduct in security was not high [4].

#### 2.4.1 Informal cultural model

We have established an informal cultural model for predicting the behaviour of users to information security system of different cultures. This cultural model will help developers of security for information systems to predict the behaviour and preferences of users of different cultures. This model consists of the following components: General Living System ID; Hofstede; Worldview; Social Identity theory (SIT); Computer Literacy; and General Education as shown in figure 3.



*Figure 3: Informal cultural model [17]*

## Methodology for Considering Environments and Culture in Developing Information Security Systems

The General living System Identity of an individual contains the cell, organ, organism, group, organization, nation, supranational [16] [27]. The general Living identity will provide among others information about cultural background. For instance if the culture reads from right to left then it means the important instructions or pictures in information security have to be placed on the right side of the pages to be noticed faster. The Hofstede [10] component consists of the values: power distance index; individual vs. collectivism index; uncertainty avoidance index; femininity vs. masculinity index; and long-term vs. short-term orientation index. The next component is the Cobern's worldview theory [5] [20]. This theory consists of how an individual understands the world and other people, classification, causality, relationship, self, time and space. This includes a model of the world, what we should do, how we should reach our goals, where are we heading, what is true and false, etc. The next component is the social identity theory with categorization and identification as sub components [23] [20]. These identities can be at personal, group, national, ideological, and religion levels. Then we have computer literacy, which indicates the practical and theoretical computer knowledge that an individual has. The last component is the general education of the individual.

In cultures where power distance is high there is a tendency of over respecting the older people and people who have higher positions in companies. Therefore, there is higher possibility of breaching security if there is external pressure from older people or people with higher positions in a company. This implies that if a boss wanted to borrow a password or a smart card from an employee, the employee is likely to accept the request, thereby breaching security. Therefore, as developers we need to create an authentication system that will not work in cases when there is a possibility of such external pressure to breach security. In countries with low power distance, this possibility is low. There could be a tendency of making security policies and procedures that are not widely accepted by all employees since high-level discussions do not always involve low-income groups in high power distance cultures. Björck and Jiang made a study to compare the implication of culture on IT security between Sweden and Singapore [3]. The

power distance in Sweden is low, 31%, while in Singapore it is high, 74% [3] [10]. The manager of a company in Singapore commented that he makes the policies and other issues of IT security and then gives them to the IT department to implement. The Manager of a Swedish company commented on the same issue that he identifies the policies and other IT security issues and then calls a meeting with all the employees involved to discuss and solve the issues.

In cultures that value individualism, people tend to make decisions that are more in an individual's interests than group's interests. This means that a security manager will tend to choose the security decisions of self-interest in the first hand, while security managers from cultures that value collectivism will tend to make security decisions favouring group interests. Another example from the same study [3] is that Sweden scores 71% in the individualism collectivism index, while Singapore scores 20% [10]. It was observed that in Singapore employees consider themselves as an extended family and so they share passwords with each other and they do not consider this as a security breach, while in Sweden people do not share passwords. It was also noted that employees in the Singapore could access even resources that they do not need while in Sweden employees could access only the resources they needed. Hofstede [10] comments that in societies that value collectivism people consider themselves as an extended family, which implies that they trust each other and share responsibilities. This implies in the IT Security world that if for some reasons an employee is not at the workplace now, the employee can ask a colleague to access resources on her behalf by providing all the necessary authentication and authorization credentials. It was also noted that when employees leave companies in Singapore their accounts could remain for a long time without being terminated, while in Sweden when an employee leaves a company for another company the accounts are terminated immediately [3].

In societies where there is the index of uncertainty avoidance is high people tend to be protected against unknown situations and do not always allow their children to experience unknown situations. Students usually expect teachers to have all the answers to their questions [19]. People prefer

## Methodology for Considering Environments and Culture in Developing Information Security Systems

to have rules, laws and regulations in most areas where environments are structured [19]. In societies where this index is, low people are not protected against unknown situations and they allow children to experience unknown situations. In information systems security people would tend to take more risks and so leave parts of the information systems unsecure.

### **2.5 Apply Socio-Technical measures where culture and traditions create weak links in information security**

The sixth step is to apply social-technical measures [12] where culture and traditions create weak links in information security. Knowledge is applied to understand, to explain, to predict and to control. The informal model will be applied in form of procedures to control. Control can be used to control negatively or positively. The different actions will be assigned values. If the consequence of a certain action or value is negative then this action will be forbidden. If the consequence of a certain value or action is positive then the action will be allowed.

### **2.6 Provide features to make an information system learn to adapt to environments**

In this step we provide measures for making an information system and information security system learn to adapt to environments. Ashby proposed two types of adaptations [25]. The first is to make the system adapt to an environment. The second adaptation is to make the system learn to adapt when the environment changes. We apply the Cybernetics feedback mechanisms [22] and digital immune system [9], variety and regulation [9] and Cybernetic structural models [11] [9] for the first type of adaptation. We apply the Viable System Model, VSM, [9] [1] for the second type of adaptation. Different nations and enterprises apply the VSM [9]. The major application of this model [9] was in Chile during the times of president Salvador Allende. The intelligent forces were trying to destabilize the economy because Allende was a dictator but Chile applied the Viable System Model [30] to stabilize the economy of the country. The environmental disturbances came from the intelligence agencies and the VSM was regulating the disturbances to stabilize the economy [25]. We apply this model to make





## Methodology for Considering Environments and Culture in Developing Information Security Systems

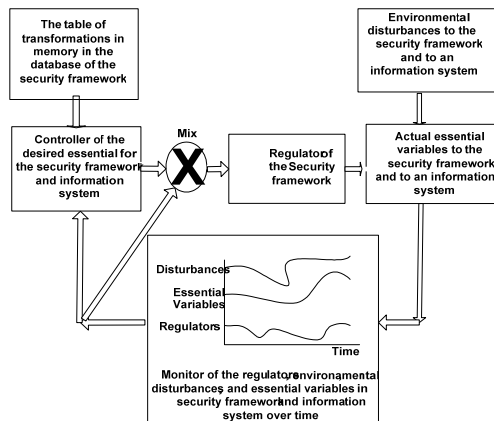


Figure 5: Variety and regulation [9]

Every subsystem 1 has a local environment embedded in another environment. This embedded environment is part of a total environment, which contains a future environment. Subsystem 2 is responsible for stabilizing subsystem one. Subsystem 3 monitors the behaviours' of subsystems 1 and 2 and is concerned with internal operational controls of subsystem 1 [9]. It also audits the subsystem 1 to make sure that it performs in accordance to the plans given to it through subsystem 2. Subsystem 4 is concerned with the outside and future of a system. The controller of the desired essential variables mixes them with variables from the monitors to produce the harmless inputs to the information systems. There are two types of feeding: feed forward in which the regulator receives the disturbances and acts before the information security system; in the negative feedback, the information security system receives the environmental disturbances and then the regulator regulates the disturbances via the transformer. For every environmental disturbance, there is a corresponding response as shown in the outcome matrix in Figure 6. The new security framework receives environmental disturbances through the deterrence, detection, prevention, response, recovery sub systems. The adaptability system of the security

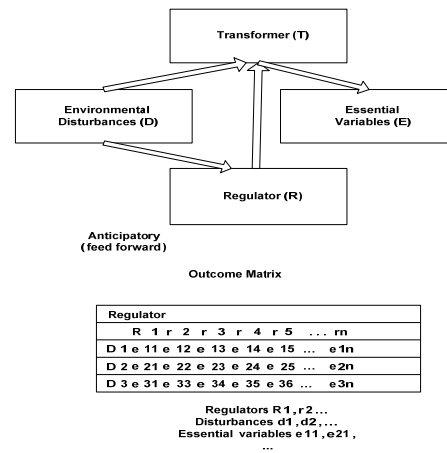


Figure 6: Cybernetic structural model [9]

framework monitors and records the environmental disturbances, essential variables, and regulators over time as shown in figure 5. The adaptability system applies these recorded data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the whole security framework and the information system will react to those future disturbances.

There is a table of transformations in memory of environmental disturbances, essential variables and regulatory disturbances. The controller of the desired essential variables for the security framework and the information system mixes them with variables from the monitors to produce the harmless inputs to the information systems. The implication to information security systems is that the regulator (R) must be able to produce as many responses as the number of disturbances (D) from an environment [9], as shown in Figure 6.

## 2.7 Compare allocates of economical resources to the different security value-based chain functions

In this step, we do an analysis of how to allocate economical resources to the different security value-based chain functions deterrence, prevention, detection, response, and recovery [13]. In the same way, we analyze to determine how to allocate economical resources to each sub system the new security framework. We have used the Delphi method [28] to construct an ideal security value chain for an information security system in an abstract situation [29] as shown in table 1.

*Table 1: Allocation of economical resources on sub systems*

Sub system	Deterrence subsystem	Prevention Subsystem	Detection Subsystem	Response subsystem	Recovery Subsystem
Average distribution	18.75%	24.38%	23.13%	14%	19.38%

### **Analysis of allocation deviation using Chi- square**

We analyzed the deviation in allocation of economical resources, shown on table 1, to the security value-based chains using Chi-square [18]  $\chi^2$

$$\chi^2 = \sum_{i=1}^c \frac{(O_i - E_i)^2}{E_i}$$

We applied the formula for Chi-square in which  $O_i$  is the observed economical allocation on each sub system;  $E_i$  is Expected economical allocation on each security value-based function.  $E_i = 20000$ . The number of observations,  $c$ , is five. We set the degree of freedom to be four. The degree of freedom is the number of observations minus one. The null hypothesis [8] was the deviation from the expected allocation of economical resources to the security value-based chain functions is not significant. We applied the graphpad chi square calculator [7]. The result is that Chi-squared equals 3136.890 with four degrees of freedom. We calculated the probability,  $P$ , and found  $P(\chi^2 > 3136.890) = 0.0001$ . We applied significance level of Probability = 05%. This significance level was established by Fisher [8] who wrote, “The value for  $P=0.05$ , or 1 in 20, is 1.96 or nearly 2; it is convenient to take this point as a limit in judging whether a deviation ought to be considered significant or not.” In this observation, we have received the  $P$  value to less than 0.0001. This difference is extremely statistically significant. The deviation of the allocation of economical resources to the security value based chain functions deterrence, prevention, detection, recovery, and response from the expected allocation is significant and would indicate that the security culture is different.

### **2.8 Educate users of information systems in social engineering and about the security framework**

The ninth step is to educate users of information systems in the information system in social engineering and about the security framework. This could be done physically, electronically using mobile agents or knowledge bots [24] [14].

## 2.9 Evaluate the outcomes of the implementation of the new security framework

The last step will be to evaluate continuously the outcomes of the implementation of the new security framework and follow the plan, do, check, act process for continuous security improvement outlined in ISO27001 [6].

## 3 CONCLUSION AND LIMITATION

We have proposed a new security framework in which we describe a methodology for considering culture of users and environments where information systems operate in developing information security systems. The methodology is also aimed at creating environments where technology serves people instead of people serving technology. We show the importance of applying both socio and technical controls in strengthening weak links that have been created by culture of users. The new security framework provides adaptability features that make information systems learn to adapt to environments. The limitation is that the framework has never been applied in its totality and consequence there is no data to either validate the framework or compare this framework with other information security frameworks.

## 4 REFERENCES

- [1] Beer, S. (1981). *Brain of the Firm*. Great Britain: John Wiley & Sons Ltd.
- [2] Bishop, M. (2003). *Computer Security Art and Science*, Addison-Wesley, Boston, USA.
- [3] Björck, J., & Jiang, K. W. B. (2006). *Information Security and National Culture Comparison between ERP system security implementations in Singapore and Sweden*. Retrieved November, 2008, from: [www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-396.pdf](http://www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-396.pdf)
- [4] Chaula A. J. (2006). *A social-Technical Analysis of Information security systems Assurance. A case study for Effective Assurance*, Report 06-016. Doctoral thesis. Computer and Systems Sciences. Stockholm University, Sweden.
- [5] Cobern, W. (1991). *The Cultural Nature of the Concept "Scientific Worldview"*, Department of Teaching, Learning & Leadership, Western Michigan University, USA. Retrieved January 19, 2009, from: <http://www.ouhk.edu.hk/~rcwww/misc/cobern.htm>.
- [6] ISO 27001 standard, <http://27001.denialinfo.com/pdca.htm>

## Methodology for Considering Environments and Culture in Developing Information Security Systems

- [7] Graphpad, (2009). The Chi Square calculator, retrieved February, 2009, from: <http://www.graphpad.com/welcome.htm>
- [8] Fisher, R. A (1926). *Statistical Methods and Scientific Inference*, New York: Hafner, p 44
- [9] Herring, C. E. Jr, (2002). *Viable Software for the Intelligent Control Paradigm for Adaptable and Adaptive Architecture*, Doctoral thesis, University of Queensland, Brisbane, Australia.
- [10] Hofstede, G.H., (2001). *Culture Consequences: International Differences in Work-related Values*, Sage, London.
- [11] Howland, D. (1990). *The Cybernetic Modeling of Soviet Systems*, Washington, DC: Defense Intelligence Agency, US Air Force War Defense. Retrieved December, 2008, from: <http://www.scribd.com/doc/1486511/US-Air-Force-infowarpre97>.
- [12] Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Doctoral thesis, Department of Computer Systems Sciences. Stockholm University and Royal Institute of Technology. Stockholm, Sweden.
- [13] Kowalski, S., & Edwards, N. (2004). A security and trust framework for a Wireless World: A Cross Issue Approach, *Wireless World Research Forum no. 12*, Toronto, Canada.
- [14] Kowalski, S. (2008). Lectures Research in Information systems security. *Scientific methodology course*. Department of Computer systems sciences. University of Stockholm and Royal Institute of Technology Stockholm Sweden.
- [15] Kowalski, S., Nohlberg, M. & Mwakalinga, J., (2008). A systemic model for security and risk management in telecom networks. The 12th World Multi-Conference on Systemic, Cybernetics and Informatics: WMSCI 2008, Jointly with The 14th International Conference on Information Systems Analysis and Synthesis: ISAS 2008, June 29th - July 2nd, 2008 – Orlando, Florida, USA.
- [16] Miller, J. G. (1978). *Living Systems*, Great Britain: McGraw Hill.
- [17] Mwakalinga, J., Yngström, L., & Kowalski, S (2009). A holistic and immune system inspired security framework. Proceedings for the 2009 International Conference on information Security and Privacy (ISP-09), Orlando, FL, USA.
- [18] Plackert, R.L. (1983). Karl Pearson and the Chi-Squared Test. *International Statistical Review*, 51(1), 59-72.
- [19] Slay J, (2002). Human activity systems: A theoretical framework for designing learning for multicultural settings. *Educational Technology & Society* 5 (1).
- [20] Slay, J., Darzanos, K., Quirchmayr, G., & Koronios, A. (2003). Towards a mature understanding of “culture” in information systems security research. Insights from Research. University of South Australia, School of Computer and Information Science, Mawson Lakes, Australia; Universität Wien, Institut für Informatik und Wirtschaftsinformatik, Austria.

Proceedings of ISSA 2009

- [21] Steinberg, R.M., Everson, M.E.A., Martens, F.J., & Nottingham, L. E. (2004). Enterprise Risk Management (ERM) – Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved February, 2009, from: [http://www.coso.org/Publications/ERM/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf)
- [22] Schoederbek, P. G., & Kefalas, A., (1990). *Management Systems. Conceptual Considerations*: Boston: Irwin. P 13, 203.
- [23] Tajfel, H. (1978). *Differentiation between Social Groups*, Cambridge, UK: Cambridge University Press.
- [24] Wallace, R. (2008). *ALICE Artificial Intelligence Foundation*. Retrieved January, 2009, from: <http://www.alicebot.org/>.
- [25] Umpleby, S. A. (2008). *The Viable System Model. Research Program in Social and Organizational Learning*. The George Washington University. Washington DC, USA. Retrieved August 2008, from: <http://www.aea-dc.org/resources/2008-8-13-Viable-System-Model-Stuart-Umpleby.doc>.
- [26] Van Dam, N., Evers, V., Arts, F. (2003). Cultural user experience, issues in e-government: Designing for a Multi-cultural society. Digital Cities 3, University van Amsterdam, Netherlands.
- [27] Yngström, L. (1996). *A systemic-Holistic Approach to academic programs in IT Security*, Doctoral thesis, Department of computer system sciences, Stockholm University / Royal Inst. of Technology ISRN SU-KTH/DSV/R--96/21--SE.
- [28] Rowe and Wright (1999): The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, Volume 15, Issue 4
- [29] Mwakalinga, J. (2009). *Investigating a new security framework based on the principles of the Systemic-Holistic approach and of the immune system*. Doctoral thesis, department of computer system sciences, Stockholm University / The Royal Institute of Technology, Sweden.
- [30] Raul, E (2007). *Cybersyn: Foundings and convergence between art science and technology in Chile* [http://www.metaphorum.org/proyecto\\_cybersyn\\_ingles.pdf](http://www.metaphorum.org/proyecto_cybersyn_ingles.pdf)

## 5 PERMISSIONS

Jeffy Mwakalinga, Stewart Kowalski and Louise Yngström are the authors of this paper. This work is original and does not violate any copyrights, rights and privacy of others. We retain the right all or part of this paper in our future work. We grant the ISSA 2009 organizers the right to publish this paper in the ISSA 2009 proceedings.

The State of the Art of Spam and Anti-Spam Strategies  
and a Possible Solution using Digital Forensics

# **THE STATE OF THE ART OF SPAM AND ANTI-SPAM STRATEGIES AND A POSSIBLE SOLUTION USING DIGITAL FORENSICS**

**Author and co-authors**

**Franscois R. van Staden<sup>1</sup>, H.S. Venter<sup>2</sup>**

<sup>1,2</sup>Information and Computer Security Architectures (ICSA) Research  
Group Department of Computer Science University of Pretoria South  
Africa

ruan.vanstad@up.ac.za

Room 5-1.7, Natural Sciences 2, Hatfield Campus, Pretoria, 0001  
+27(12)420-4690

hventer@cs.up.ac.za

Room 4-23, Information Technology, Hatfield Campus, Pretoria, 0001  
+27(12)420-3654

## **ABSTRACT**

Electronic communication such as email is an efficient and cost effective communication medium in today's connected world. This paper looks at the strategies employed by spam and anti-spam and shows the co-evolution of these strategies. Anti-spam software makes use of intelligent filtering based on content scanning, block lists, black lists, white lists and mailbox authentication. Spammers have been able to get past anti-spam software by using picture content, mailbox- spoofing and anonymous emailing.

Spammers use the strategy of creating botnets to send spam. Honeypots, systems employed to gather information on unusual system

Proceedings of ISSA 2009

activity, track and ultimately stop the activities of botnets. The paper looks at honeypots as part of information gathering in a digital forensic process. Digital forensic science has been employed to authenticate email authors and back trace email paths. This paper proposes two strategies for the detection of botnet activity and the tracing of botmasters.

#### KEY WORDS

Spam, Blacklisting, White listing, Bayes, Chi-squared, Botmaster Botnet, Spam-zombie, Honeypot.



# **THE STATE OF THE ART OF SPAM AND ANTI-SPAM STRATEGIES AND A POSSIBLE SOLUTION USING DIGITAL FORENSICS**

## **1 INTRODUCTION**

Spam is an inconvenience to electronic communication. Before an email can be profiled as spam, the Internet Service Provider (ISP) has to download the spam because anti-spam strategies are implemented either on the user's mailbox or on the company's mail servers. The downloading of spam has a direct impact on the bandwidth use of a company. The harmfulness of spam can be calculated in monetary value. The implementation of anti-spam strategies also has its own cost implications. Spam can clog up the electronic communication lines of a company to such an extent that there is a loss of service and therefore a loss of revenue. According to BBC News, the Microsoft security report for 2008 fourth quarter states that 97% of all email sent through Microsoft email servers, is spam (Waters, 2009). Symantec reported that 73.3% of all email sent in February 2009 were spam (InternetNews, 2009).

The state of the art anti-spam strategy makes use of intelligent filtering. Intelligent filtering is build on all the anti-spam strategies developed to date and includes content scanning, black-listing and white-listing. With each strategy developed there are still situations where intelligent filters gives false positives and false negatives. False positives occur when legitimate email is marked as spam e.g. medical correspondence, including black-listed words. False negatives are when spam is not detected by the spam filter because of picture content or misspelling of black-listed words.

The state of the art spam strategy employed is botnets. Botnets are infected PCs, known as zombies, that work together to aid in cyber crimes. The botmaster controls these botnets from a central point. The problem of eliminating botnets and botmasters is firstly to find zombies in the botnet and then to trace them to the botmaster. It is possible to trace botnet activity and trace the activity back to the botmaster, by using digital forensics.

The remainder of the paper is constructed as follows; section 2 gives background information on spam, anti-spam and digital forensics, section 3 looks at the current state of the art of spam and anti-spam strategies and section 4 proposes implementation strategies that use digital forensics to augment anti-spam efforts. Section 5 is the conclusion of the paper and also discusses future work needed.

## **2 BACKGROUND**

This section discusses spam, anti-spam and digital forensics. The discussions are an overview of the different concepts used in this paper.

### **2.1 Spam and anti-spam strategies**

Spam is defined as unsolicited commercial email (Lueg, et al., 2006) or unsolicited bulk emails (O'Brien, et al., 2003). Anti means to be strongly opposed to a person, action or event (University Press). Anti-spam is defined as an application used by an email user or an email server administrator, to reduce the amount of spam the user receives (Network-Dictionary). Anti-spam is defined by the author, as strategies employed to oppose spam. These strategies can be employed separately or together. In the following sections the author explains the technology strategies employed by anti-spam software and the strategies that spammers use to get past the anti-spam strategies. There are also training and awareness strategies but those are outside the scope of this paper.

## The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics

### 2.1.1 Content Scanning

Content scanning is implemented as an application on the email server and as an application addition to the users' email application client (spam-site, 2006), (Mueller, 2009). To give email content a spam probability rating, content scanners use a statistical analysis algorithm such as Bayes or Chi-squared (O'Brien, et al., 2003). The algorithm uses key words and key phrases to calculate the spam probability rating. We also refer to these key words and phrases as patterns. This rating categorises the email as spam, possible spam or non-spam. Spam is stopped at the email server. Possible spam is marked with a spam tag but is still sent to the user. Non-spam is seen as normal email.

To get past content scanners, spammers use techniques like picture content, HTML tag inlay and misspelling of patterns (spam-site, 2006) (Naidoo, 2007). Picture content is a series of pixel values and cannot be scanned the same way as text. When content scanners try to scan text, the scanner ignores the pictures. Email servers can be set so that the ISP will only download picture content if the user gives permission for the action. With the advent of mail clients being able to parse HTML, spammers started using tag inlay like "Vi<b></b>agra", to hide patterns. Content scanners can scan content before and after HTML parsing. Misspelling patterns, replacing characters but still making it recognizable to the reader e.g. "Vi@gra" or "V1@gra" for Viagra, causes content scanners to ignore the patterns. Users need to add these alternative patterns to the lists of the content scanner to block the mail.

### 2.1.2 Block list, black list, white list and mail box authentication

A block list is build by individual users (spam-site, 2006). Users block email senders or email domains from the users' own mail application. Block lists block email from being downloaded to a user's mailbox in future. A black list is generated at ISP or DNS level where email traffic is monitored for indications of bulk mail originating from a single source (spam-site, 2006), (Lueg, et al., 2006). The ISP or DNS will blacklist email domains suspected of sending bulk mail. White listing is when users set up a list of allowed email accounts and email domains to be downloaded to their email boxes. Mailbox authentication relies on the fact

that spammers falsify or spoof the “From” and “Reply-to” tags of an email. A message is sent to the mailbox in the “From” or “Reply-to” tag. If either the “From” or “Reply-to” mailbox does not exist, the mailbox cannot be authenticated and the email is marked as spam.

To get past email block lists and mail box authentication, spammers replace the “From” tag with the “To” tag in the email header (spam-site, 2006), (Mueller, 2009). According to the email profiler, the mail appears to originate from the users’ own mailbox. The spam email bypasses the block list since it is assumed that the user would not block its own mail address or domain. As long as the user’s domain is not blacklisted, the spam email bypasses the black list. The spam email bypasses the white list because the white list automatically adds the user’s address when it creates the list. Since the user’s mailbox does exist, the spam email’s “From” mailbox is authenticated.

Faynberg, et al. (2004) proposed a method for authenticating email. Each gateway and relay server authenticates email by sending a query to the originating mail server, asking if the email received originated from the specified mailbox. Each email forwarded needs to be logged before the email it is forwarded. This log checks if the respective server sent the mail, when there is a query about the sent mail. An addition to the proposal is to make use of an Authentication, Authorization and Accounting (AAA) server that is trusted to verify an email server. This server certifies that an email server being queried can be trusted to give a true answer. If the AAA server returns with a negative response, the server drops the email regardless of what the sending server’s response. When a server drops mail, the server’s log notes that the drop action has been performed on the mail.

### **2.1.3 Intelligent Filters**

Intelligent filters are software applications that are installed as part of a user’s mail application or as part of a mail server or both (spam-site, 2006), (Mueller, 2009). Intelligent filters use a set of anti-spam strategies to improve the success of the filter. Intelligent filters can be trained to reduce the amount of false negatives and false positives. The idea is that the user or groups of users give input to the filter to train it.

## The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics

Anti-spam software vendors claim that intelligent filters can be trained to block 99.9% of all spam (spam-site, 2006), (Mueller, 2009). From the claims made it can still be deduced that not all spam can be blocked at all times. Most of the weaknesses, discussed with regard to the other anti-spam strategies, are present in intelligent filters.

### **2.2 Digital Forensics**

Digital forensic science is a relatively new field of study that evolved from forensic science. According to the Oxford Dictionary (University Press), digital forensic science is the systematic gathering of information about electronic devices, which can be used in a court of law. Digital forensic science is more popularly called digital forensics and sometimes also called computer forensics. Palmer (2002) defines digital forensics as "the use of scientifically derived proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events". Palmer's definition describes the digital forensic process. The Oxford dictionary describes digital forensic science. The Digital Forensic Process Model (DFPM) by Kohn, et al. (2009) captures the definition of digital forensic science and states that any digital forensic process must have an outcome that is acceptable by law.

#### **2.2.1 Digital forensics and email**

Digital forensics has been used to verify the author of an email or to authenticate a user while the user is using their email application (de Vel, et al., 2001), (Gupta, et al., 2004). Digital forensics has also been used to trace the origin of email messages. Spammers make use of spoofing, open proxy servers and open mail relays, to send anonymous emails.

A proxy server is a computer process that relays a protocol between client and server systems by appearing to be the client to the server, and appearing to be the server to the client (Network-Dictionary, 2009) (Obied, 2006). Proxy servers allow communication between two computer systems by relaying information back and forth between the two

connected proxy servers. An open proxy server allows unauthenticated systems to communicate through it. Email cannot be sent straight from one server to the next, it has to pass through a series of Email relay servers (Obied, 2006). Open mail relays are mail servers that are not properly configured to authenticate the origin of an email or to authenticate the email's path. By using an open proxy server or a series of open proxy servers before routing an email through an open mail relay server, the sender of an email can stay anonymous because it appears that the email originated from the last open proxy server the mail was sent through.

### **2.2.2 Honeypots**

Even (2000), states “honeypot systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system”. Spitzner, according to Obied (2006), defines a honeypot as information system resources whose value lies in unauthorized or elicit use of that resource. The author defines a honeypot as a trap set to detect, deflect, or in some other manner counteract attempts at unauthorized use of information systems. The information gathered by the honeypot is used to track where the authorized access originated and what exploits were used. If the honeypot is not accessed, it is of no use. A honeypot logs access information in accordance with digital forensic information gathering techniques. The design, implementation, placement and monitoring of a honeypot is crucial to the effectiveness of the honeypot.

Honeypots have been deployed as open proxy servers and open mail relays, to gather information about the spammers that use them (Obied, 2006). Honeypots have also been employed to gather information on botnets (Obied, 2006). The next section discusses the history of botnets, as well as advances made in the development of new strategies to trace and combat botnets.

## **3 BOTNETS**

According to Network-Dictionary (2009)“a botnet, also known as a zombie army, is a computer connected to the Internet, that has been set up to forward transmissions (including spam or viruses) to other computers

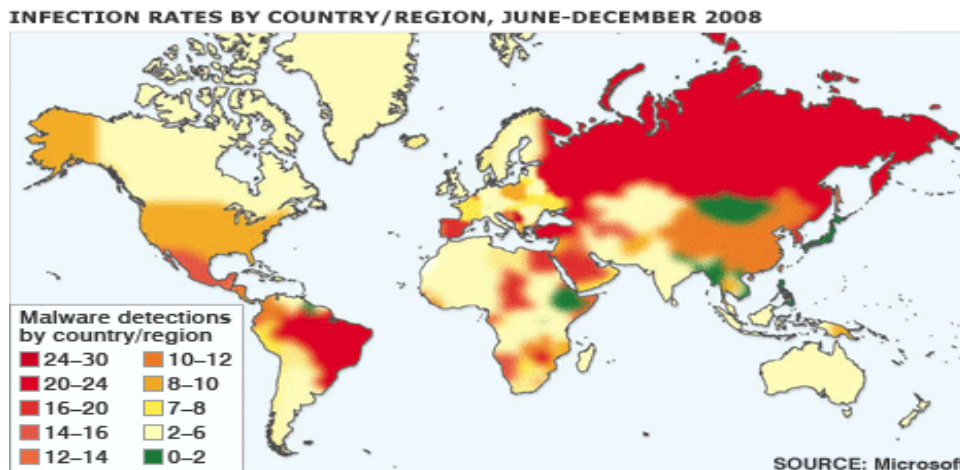
## The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics

on the Internet, without the knowledge of the computer owner.” ESET (2009) defines a botnet as “a group of bot infected PCs that are all controlled by the same command and control center”. According to the author, a botnet can be defined as a group of infected computers or zombies, that are controlled from a single controller or botmaster and used to facilitate electronic crime.

Botnets are created by infecting computers with Trojans. Once a computer is infected, the Trojan creates a SMTP (Simple message transfer protocol ) account on the local machine. This account is used to send spam and any other electronic content. The Trojans in a botnet used IRC (internet Relay Chat) connections to receive information from the controller. According to InternetNews (2009), the new tactic is for the bots to communicate with each other using Peer-to-peer connections, set up in a family tree fashion to relay information and commands. The IRC method of communication hard codes the address of the controller into the Trojan. The controller's address is extracted from the Trojan during the dissection process. The family tree method of control is when no “child” Trojan knows any of its ancestors other than its direct “parent”. The family tree method makes it harder to find the controller.

Since closing, McColo (News, 2009), a US-based ISP accused of being a major hub for spammer activity, spammers have learned to hide their activity behind the same technology used for secure networking. The biggest botnet, called Sirbizi, closed in late 2008. According to Waters (2009), the infection rates across the world are increasing. Figure 1 shows the number of infected PCs per 1000 for all the world regions. InternetNews (2009), states that MessageLabs is currently monitoring a number of botnets, including Xarvester, Cutwail and Mega-D. Spammers use botnets to create low-volume-high-node-count mail senders. Low-volume-high-node count means that the nodes are only used to send a small subset of the mails to be able to stay under the radar of bulk mail detectors. Mega-D was detected because it over utilised its bots.





*Figure 1 Infections per 1000 PCs for world regions (Waters, 2009)*

According to Obied (2006) Microsoft used a zombie machine as a honeypot to detect and trace spam activity. The machine was infected with a botnet's trojan and quarantined. Activity to and from the zombie was monitored. The information gathered by the zombie honeypot helped to track the command and control source of the botnet. This tracking information was used in a lawsuit against 13 spam operations. Using a zombie as a honeypot is only possible if the controller of the botnet is unaware that one of the zombies is being used as a honeypot.

Botnets employing P2P connections between the different zombies makes it harder to use the zombies to track the controller. The next section discusses a proposed state of the art botnet architecture and proposes strategies to combat this state of the art botnet.

#### **4 PROPOSED STRATEGY TO COMPLEMENT ANTI-SPAM USING DIGITAL FORENSIC STRATEGIES**

As anti-spam strategies evolve, spammers evolve new strategies to bypass anti-spam. The challenge for anti-spam is to get ahead of the evolution curve and start developing strategies that combat possible future developments in spam strategies. Wang, et al. (2009), suggests that, to effectively protect against new developments in botnet technology and its



## The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics

uses, state of the art botnets should be developed to find ways of combating.

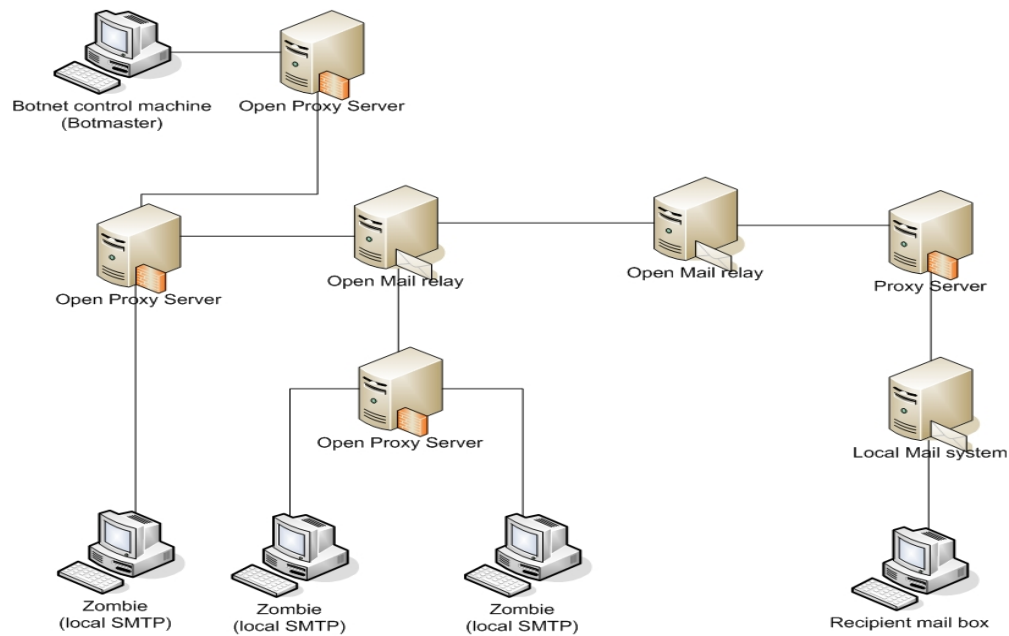
Wang, et al. (2009) presents the design of an advanced hybrid peer-to-peer botnet. The botnet uses advanced techniques to hide its activity by means of encryption and a traffic control algorithm. The botnet uses decentralised control mechanisms to hide the controller and ensure that zombies in the botnet cannot be traced by use of other zombies. The zombies are autonomous. Finding and removing those zombies found, does not impair the rest of the botnet.

The following sections discuss the implementation of an experimental environment. This environment will be used to deploy the botnet and gather information on the working of the botnet. Section 4.1 discusses the implementation of the experimental environment. Section 4.2 discusses the implementation of honeypots, in the experimental environment, as an information-gathering tool. Section 4.3 discusses the creation of a digital forensic profile of the botnet. In the real world, a botnet profile can detect and categorise botnet activity.

### **4.1 Experimental implementation of botnet**

Combating the botnet will require the implementation of the botnet in an experimental environment. The experimental environment needs to consist of open proxy servers, open mail servers, a botnet control machine and a set of workstations used as zombies. Previous studies thought us that spammers use open proxy servers and open mail servers to hide the origin of the spam that they send (Obied, 2006). To enable us to gather the most relevant information about the operation of the botnet we will need to implement the most spammer friendly environment. Figure 2 shows the proposed implementation of the experimental environment.

Proceedings of ISSA 2009



*Figure 2 Depiction of the experimental environment implementation*

Figure 2 shows the botmaster in its own network connected to the common network with an open proxy server. A second proxy server connects the botmaster to an open mail server. The configuration of the botmaster and open proxy servers creates an open proxy server chain. The open proxy servers are positioned to indicate the borders of the smaller networks within the larger environment. To simulate the real world mail relay environment, two open mail relays are connected to each other and placed in the centre of the experimental environment. The local SMTP service on the zombies is there because of the Trojan infection. The local mail server will have a known set of mail accounts that will receive e-mail from the zombies. The recipient e-mail box will monitor all the mailbox activity on the local mail server.

The State of the Art of Spam and Anti-Spam Strategies  
and a Possible Solution using Digital Forensics

## 4.2 Honeypot implementation

Honeypots will be deployed to gather information about the activity inside the experimental environment. The open proxy servers, open mail servers and zombies will be used as honeypots in the experimental environment. The experimental botnet will make use of log-files to capture true activity of the botnet. The true activity can be compared to the activity recorded with help from the honeypots. Using the comparative information recorded, an effective design and deployment strategy for a production environment, can be determined.

## 4.3 Profiling

The disadvantage of using honeypots in the experimental environment is that botmasters can create detection methods to detect honeypots and avoid them. Honeypots are used more and more as a general information gathering technique. A new information gathering technique is needed that cannot be detectable by botnets and cannot be bypassed.

Organisations create sub-networks with the use of VPN's over WAN links to connect IT resources together. A botnet creates a sub-network within a greater network, in the same way. A profile of what the botnet sub-network activities might look like is set up, using the experimental information collected during the botnet testing. The creation of a network diagram for all the sub-networks within the greater network will allow for the creation of an activity profile of the sub-networks. By comparing the activity profile of a sub-network with the know activity profile of a botnet, it will be possible to detect the botnet.

The information contained in the profile will consist of normal activity information. This paper defines normal botnet activity as the activity involved with the sending and receiving of control information and the sending of spam messages. The activity of infecting new machines is included in the activity of sending spam messages.

## 5 CONCLUSION

This paper looks at the strategies employed by spam and anti-spam and shows the co-evolution of these strategies. Anti-spam software makes use of intelligent filtering based on content scanning, block lists, black lists, white lists and mailbox authentication. Spammers have been able to get past anti-spam software by using picture content, mailbox spoofing and anonymous e-mailing.

Digital forensic science has been employed to authenticate email authors and back trace e-mail paths. The latest development in digital forensic information gathering is the use of honeypots. Spammers use botnets to send unsolicited electronic communication that can bypass anti-spam strategies.

This paper proposed two strategies for the detection of botnet activity and the tracing of botmasters. The first strategy consists of an implementation of honeypots to detect botnet activity. The second strategy employs digital profiling to detect the activity of botnets. The challenge for future developments, with regard to anti-spam strategies, will be to improve information gathering, botmaster tracing and botnet detection.

No one can win an evolutionary war. The co-evolution between spam and anti-spam is likely to continue indefinitely. To win the war, anti-spam strategies will need to get ahead of the evolutionary curve and start to develop new ways of detection, information gathering and tracing, proactively.

The State of the Art of Spam and Anti-Spam Strategies  
and a Possible Solution using Digital Forensics

## 6 REFERENCES

**de Vel, O, et al. 2001.** Mining Email Content for Author Identification Forensics. *SIGMOD Record*. December, 2001, Vol. 30, 4.

**ESET. 2009.** Botnet Definition. <http://www.eset.com/>. [Online] 2009. [Cited: 27 April 2009.] <http://www.eset.com/threat-center/threats/botnet.php>.

**Even, Loras R. 2000.** Intrusion Detection FAQ: What is a Honeypot? <http://www.sans.org/resources/idfaq/honeypot3.php>. [Online] SANS Institute, 12 July 2000. [Cited: 27 April 2009.] <http://www.sans.org/resources/idfaq/honeypot3.php>.

**Faynberg, Igor, et al. 2004.** *Method and Apparatus for Reducing E-mail Spam and Virus Distribution in a Communications Network by Authenticating the Origin of Email Messages*. US2005/0203985A1 United States of America, 29 April 2004. 709/200.

**Gupta, Gaurav, Mazumdar, Chandan and Rao, M. S. 2004.** Digital Forensic Analysis of Emails: A Trusted Email Protocol. *International Journal of Digital Evidence*. Spring, 2004, Vol. 2, 4.

**InternetNews. 2009.** Report Says Spam Arms Race Escalating. <http://www.ironport.com/>. [Online] IronPort In the News, 16 March 2009. [Cited: 16 March 2009.] [http://www.ironport.com/company/pp\\_internet\\_news\\_03-16-2009.html](http://www.ironport.com/company/pp_internet_news_03-16-2009.html).

**Kohn, Michael, Eloff, J.H.P. and Olivier, M.S. 2009.** *UML Modelling of Digital Forensic Process Models (DFPMs)*. [Document] Pretoria : Information and Computer Security Architectures (ICSA) Research Group University of Pretoria, 2009.

**Lueg, Christopher, Huang, Jeff and Twidale, Michael B. 2006.** *Mystery Meat: Where does spam come from, and why does it matter?*

Proceedings of ISSA 2009

[Document] Hamberg, Germany : EICAR, EICAR, 29 April 2006.  
Security in the Mobile and Networked World, Vol. 15.

**Mueller, Scott H. 2009.** spam.abuse.net. *Fight Spam on the Internet!*  
[Online] spam.abuse.net, 18 April 2009. [Cited: 21 April 2009.]  
<http://spam.abuse.net/>.

**Naidoo, Nithen. 2007.** *Introduction to Using Spam Methodology to Initiate Proactive Spam Controls.* [Document] Centurion : SensePost, 2007.

**Nazario, Jose. 2006.** *Botnet Tracking: Tools, Techniques and Lessons Learned.* [Document] Canada : Arbor Networks, 2006.

**Network-Dictionary. 2009.**

<http://www.networkdictionary.com/security/b.php>.

<http://www.networkdictionary.com>. [Online]

<http://www.networkdictionary.com>, 2009. [Cited: 27 April 2009.]

<http://www.networkdictionary.com/security/b.php>.

**O'Brien, Cormac and Vogel, Carl. 2003.** *Spam Filters: Bayesvs. Chi-squared; Letters vs. Words.* [Electronic] Dublin : University of Dublin, 2003.

**Obied, Ahamed. 2006.** *Honeypots and Spam.* [Document] Calgary : UniversityofCalgary, 2006.

**Palmer, G.L. 2002.** *Road Map for Digital Forensic Research.* [Electronic Publication] s.l. : Digital Forensic Research Workshop (DFRWS), Digital Forensic research workshop, 2002.

**spam-site. 2006.** [www.spam-site.com](http://www.spam-site.com). [www.spam-site.com](http://www.spam-site.com). [Online]  
[www.spam-site.com](http://www.spam-site.com), 2006. [Cited: 03 March 2009.] <http://www.spam-site.com>.

The State of the Art of Spam and Anti-Spam Strategies  
and a Possible Solution using Digital Forensics

**University Press, Oxford.** Possible entries for. <http://www.oup.com>.  
[Online] [Cited: 22 April 2009.] [http://www.oup.com/oald-bin/web\\_getald7index1a.pl](http://www.oup.com/oald-bin/web_getald7index1a.pl).

**Wang, Ping, Sparks, Sherri and Zou, Cliff C. 2009.** An Advanced Hybrid Peer-to-Peer Botnet. *TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING*. Monthly, 2009, Vol. 0, 0.

**Waters, Darren. 2009.** Spam Overwhelms Email Messages. *BBC NEWS | Technology* |. [Online] BBC, 8 April 2009. [Cited: 8 April 2009.] <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/7988579.stm?ad=1>.

**www.spam-site.com. 2006.** <http://www.spam-site.com/your-website-blacklisted.shtml>. *www.spam-site.com*. [Online] [www.spam-site.com](http://www.spam-site.com), January 01, 2006. [Cited: March 23, 2009.] <http://www.spam-site.com>.

## 7 PERMISSIONS

All references used in the paper remain the property of the owner of the source that was referenced. Copyright for figure 1, published on BBC NEWS website, belongs to BBC NEWS as referenced in article.

Proceedings of ISSA 2009



Information Security Policies for Governmental Organisations: The Minimum Criteria

# **INFORMATION SECURITY POLICIES FOR GOVERNMENTAL ORGANISATIONS, THE MINIMUM CRITERIA**

**SJ Ngobeni<sup>1</sup> & MM Grobler<sup>2</sup>**

Council for Scientific and Industrial Research (CSIR), Pretoria, South  
Africa

<sup>1</sup>sngobeni@csir.co.za, 012 841 4410

<sup>2</sup>mgrobler1@csir.co.za, 012 841 2838

## **ABSTRACT**

Recent technology advancement has resulted in an era where many organisations become more and more comfortable to use computer systems to process their information. Intruders are making it their mission to break into these computer systems and access valuable information in an unauthorised way.

Information Security policies are seen as not only a counterproposal, but also a solution to Information Security effectiveness. However, a key issue impacting Information Security policies is what should be included in these policies. This study makes an attempt to design a Comprehensive Information Security Policy (CISP) to serve as basis for organisations when designing their own Information Security policies, based on a public survey on IT related governmental Information Security policies.

## **KEY WORDS**

Information Security policies, standards, organisations

# **INFORMATION SECURITY POLICIES FOR GOVERNMENTAL ORGANISATION, THE MINIMUM CRITERIA**

## **INTRODUCTION**

Information can be regarded as a crucial business asset important for business continuity, and consequently needs to be protected. The protection of information is especially important due to the rapid increase of the interconnected business world, exposing information to a variety of threats and vulnerabilities. This information needs to be protected [1].

Information Security is seen as the process of protecting information and information systems from a range of threats and vulnerabilities to ensure business continuity, minimising business risks and maximising return on investments and business opportunities. This protection can be achieved by implementing suitable Information Security policies. These policies need to include relevant key issues impacting Information Security to enable this protection.

This study designs a Comprehensive Information Security Policy (CISP) to serve as basis for organisations when designing their own Information Security policies. This is achieved by first identifying and evaluating the Information Security policies of several IT related governmental organisations, and then formulating a theoretical framework for the evaluation of these policies. The results from the evaluation are then used to design the proposed CISP. The CISP can be adopted by any IT related governmental organisation as a guideline when designing or reviewing their Information Security policies. A literature survey was conducted to gain insight on Information Security policies and various South African IT governmental organisations were contacted to collect their policies.

The paper is structured as follows: Section 2 provides background knowledge on Information Security policies; Section 3 presents a theoretical framework for the evaluation of the policies; Section 4 presents

the evaluation and analysis of the policies and Section 5 presents the proposed CISP. Section 6 concludes this paper and discusses future work.

## **1 BACKGROUND**

This section provides background information on Information Security policies. It presents an overview of Information Security policies and defines the boundaries of such a policy. Lastly, it presents a discussion on the key elements that an organisation needs to consider when designing an Information Security policy.

### **1.1 Overview**

Information Security policies are the cornerstone of Information Security effectiveness. Public and private sector enterprises today are highly dependant on information systems to carry out their mission, vision and business functions [2]. Without a policy on which to base standards and procedures, decisions are likely to be inconsistent and security holes may be present, ready to be exploited by internal and external parties [3]. Accordingly, information must be protected to prevent the exploitation of valuable information, regardless of the information's format.

This study states that the protection of information and its systems can be achieved by employing Information Security policies within the government and the business organisation. Many governmental departments have adopted the use of these policies as the primary way to achieve their goals and business continuity. However, the exact framework of an all-inclusive Information Security policy is still to be decided. This study evaluates the Information Security policies of various IT related governmental organisations and further uses the results of this evaluation to design the CISP.

### **1.2 What are Information Security policies?**

An Information Security policy can be defined as a document that outlines the rules, laws and practices for computer network access [4]. This document regulates how an organisation will manage, protect and distribute its sensitive information (both corporate and client information) and lays the framework for the computer-network-oriented security of the organisation.

Danchev [5] mentions a very important definition of Information Security policy: a plan that outlines the organisation's critical assets and

how the assets must (and can) be protected. The most important aspect of the Information Security policy is to provide security awareness within an organisation, engaging the employees to participate in protecting the organisation's valuable information. Danchev suggests a well designed policy addresses issues such as the acceptable use of the organisation's email system, the proper use of workstations and internet connectivity, how to respond to a security breach, the proper use of IDs and logging information, as well as handling of financial data.

### 1.3 The key Information Security policy elements

A well-written Information Security policy must satisfy the needs of the organisation, be practical and enforceable. This section discusses several essential elements that are necessary when designing an Information Security policy [6].

An Information Security policy should be:

- **Easy to understand.** The policy should be addressed in a manner that will meet the intended audience.
- **Applicable.** The policy must only contain security measures that are specific needs to the organisation.
- **Enforceable.** The policy should maintain a decent balance between being too defensive and too lenient.
- **Proactive.** The policy should state what is expected of employees instead of making pronouncements.
- **Doable.** The policy should be written in a way that will not restrict the objectives of the business.
- **Avoiding absolutes.** The policy should be written in a way that state things in a politically correct and in a diplomatic way.

## 2 A THEORETICAL FRAMEWORK FOR EVALUATING INFORMATION SECURITY POLICIES

Based on preliminary research and results retrieved from the public survey, the Information Security policies collected from IT related governmental organisations were reviewed based on the following characteristics:

- 1) **Access control.** The policy describes rights/permissions and to whom these rights/permissions can be granted with regards to accessing a particular resource within the organisation.
- 2) **Data classification and control.** Data need to be classified according to its level of sensitivity to assist the organisation in determining the extent security needed. Data can be classified as top secret, highly confidential, proprietary, internal use only or public use [7].
- 3) **Risk assessment.** The organisation's information systems need to be assessed to identify vulnerabilities that can affect the confidentiality, integrity and availability of the key information assets.
- 4) **Password and user ID management.** The policy should recommend rules for composing passwords, how to change and reuse passwords, and the need for keeping passwords.
- 5) **Encryption and digital signatures.** The policy need to address the need for encryption and digital signatures as means to achieve data security within the organisation.
- 6) **Instant messaging, PDAs and smart phones.** The policy must provide procedures and regulations regarding the use of Instant Messaging, PDAs and smart phones within the corporate environment [8].
- 7) **Security awareness and training.** The policy needs to facilitate compliance by employees regarding the organisation's stated rules and procedures [9].
- 8) **Data privacy management for employees and customers.** The policy needs to address the privacy relationships between collection and dissemination of information [10].
- 9) **Corporate Governance.** The policy should discuss the procedures by which a business is operated, regulated and controlled. It should also discuss the internal factors defined by the officers, the constitution of the company and external forces such as consumer groups, clients and governmental regulations.

- 10) **Electronic mail, viruses, malicious code protection and social engineering attacks, including phishing scams.** The policy should describe methods of creating, transmitting or storing primary text-based human communications with digital communication systems. It must address the protection of the organisation's networks and information systems from being viruses and social engineering.
- 11) **Identity theft.** The policy needs to address the prevention of identity theft and related attacks.
- 12) **Network security.** The policy addresses the protection of the network and its services, unauthorised modification, destruction and disclosure of information, and assuring that the critical network functions correctly.
- 13) **Firewall.** The policy should address the use of firewalls to prevent unauthorised internet users from accessing the organisation's private networks connected to the internet.
- 14) **Communication security, including telephones and fax machine.** The policy should cover issues related to the security of telephone and fax equipment [11].
- 15) **Website and e-commerce security.** The policy should describe how to protect the organisation's website against security weaknesses such as SQL injections, Denial of Service attacks and spam relaying.
- 16) **Security in third party contracts, including outsourcing and off-shoring of IT project.** The policy should address security in its infrastructure and assets, whilst complying with regulations applicable to third party contracts [12].
- 17) **Document destruction, as well as retention of documents that may be used in courts cases.** The policy should clearly address the destruction and retention of documents.
- 18) **Incident response.** The policy discusses issues concerning how an organisation responds quickly and effectively to a system or network security breach [13].
- 19) **Contingency planning.** The policy needs to address contingency planning, or the disaster plan. This describes the organisation's immediate actions to respond to unexpected business interruptions or accidental disasters [14].
- 20) **Telecommuting and mobile computing.** The policy should address telecommuting as a means to replace work-related travel [15].
- 21) **Intrusion Detection Systems (IDSs).** The policy should describe methods to detect malicious network traffic and computer usage.

### 3 EVALUATION OF INFORMATION SECURITY POLICIES

Table 1 indicates the review of various Information Security policies for four IT related governmental organisations, as provided directly by the governmental organisations. Due to the strict regulations of these participating organisations, the Information Security policies used in this evaluation need to remain anonymous.

The characteristics column of Table 1 indicates what a good policy should contain. This list (identified in Section 3) is not all-inclusive, but based on the literature study done for this specific study. An organisational policy containing a characteristic that corresponds to any of the 21 characteristics identified in the theoretical framework is marked with an “X”, and if it does not contain a corresponding characteristics it is marked with a “-”.

*Table 1: Review of Information Security used in this study*

<b>Characteristic</b>	<b>Organisation A</b>	<b>Organisation B</b>	<b>Organisation C</b>	<b>Organisation D</b>
1. Access control	X	X	X	X
2. Data classification and control	-	X	X	X
3. Risk assessment	X	X	-	-
4. Password and user ID management	X	X	X	X
5. Encryption and digital signatures	X	-	X	X
6. Instant messaging, PDAs and smart phones	X	-	X	-
7. Security awareness and training	X	-	X	X
8. Data privacy management	X	-	X	X

<b>Characteristic</b>	<b>Organisation A</b>	<b>Organisation B</b>	<b>Organisation C</b>	<b>Organisation D</b>
9. Corporate governance	X	X	X	X
10. Electronic mail, viruses, malicious code protection, and social engineering	X	X	X	X
11. Identity theft	X	–	X	X
12. Network security	X	X	X	X
13. Firewall	X	X	X	X
14. Communication security	–	–	X	X
15. Website and e-commerce	X	–	X	X
16. Security in third party contract	X	–	X	–
17. Document destruction and retention	X	–	X	X
18. Incident response	X	X	X	X
19. Contingency planning	X	–	X	X
20. Telecommuting and mobile computing	–	–	X	–
21. Intrusion Detection Systems	X	X	X	X

From Table 1 it can be detained that not all existing Information Security policies are adequate. For example, Organisation A fails to address three of the identified elements and Organisation B fails to address eleven elements. Organisation C has a well formulated policy and addresses all the characteristics identified by the theoretical framework. Organisation D does not address four of the identified elements.

#### **4 THE CISP**

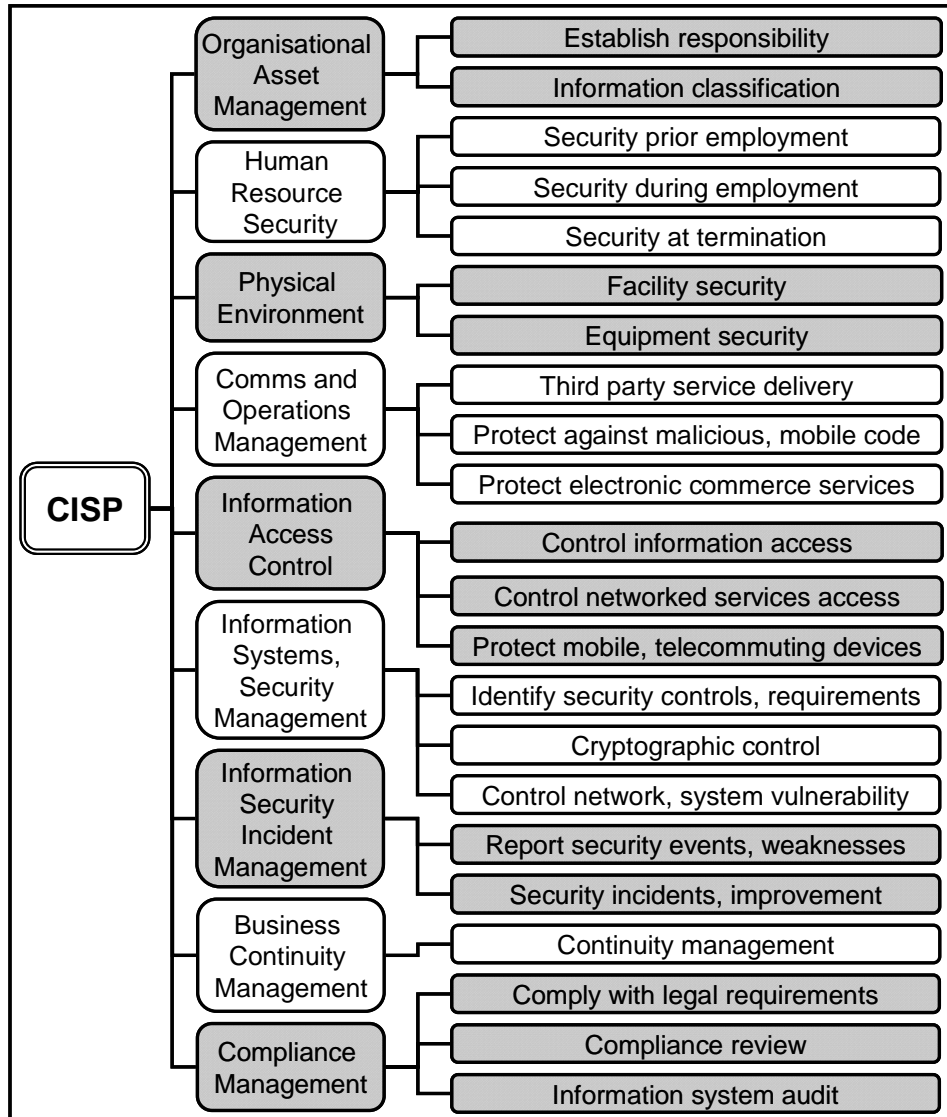
This section presents the proposed CISP. Figure 1 shows the proposed CISP on the next page.



## 5 CONCLUSION

The main goals of this study were to evaluate Information Security policies of various IT governmental organisations and design a resulting CISP. These goals were attained successfully.

The results of this study may not be optimal due to the limited number of Information Security policies that were evaluated. Various IT related governmental organisations were invited to participate in this survey, but had to decline due to organisational privacy requirements. The reviewed policies shows that most of the governmental organisations were found to omit the most significant issues that are supposed to be included in their Information Security policies (refer to Table 1).



*Figure 1: CISP*

The proposed CISP provide organisations with a generic model to use when designing their own Information Security policies. Therefore, any IT governmental related organisation that needs to design or upgrade their Information Security policies may adopt the CISP. Consistent with the changing nature of technology, the Information Security policies will

## Information Security Policies for Governmental Organisations: The Minimum Criteria

be subject to change as well. Accordingly, the CISP may be valid for a set period due to technology improvements and will need to be upgraded.

### REFERENCES

- [1] Berk, DD. 2007. *How do you define Information Security*. Available from: [http://www.linkedin.com/answers?viewQuestion=&questionID=56225&askerID=292188&goback=.hom.mid\\_138471153](http://www.linkedin.com/answers?viewQuestion=&questionID=56225&askerID=292188&goback=.hom.mid_138471153) (Accessed 2 April 2009).
- [2] *Information Security: A Business Manager's Guide*. 2004. Department of Trade and Industry, Available from: <http://www.berr.gov.uk/files/file9981.pdf> . (Accessed 02 February 2009).
- [3] Information Security. 2002. *Draft Position Paper on Information Security*. Available from: <http://www.dpsa.gov.za/documents/acts&regulations/frameworks/e-commerce/POSITION%20PAPER%20ON%20INFORMATION%20SECURITY1.pdf> (Accessed 2 September 2008).
- [4] *Security policy*. 2008. Available from: [http://www.webopedia.com/TERM/S/security\\_policy.html](http://www.webopedia.com/TERM/S/security_policy.html) (Accessed 15 January 2009).
- [5] Danchev, D. 2003. *Building and implementing a Successful Information Security Policy*. Windows Security resources for IT admin, Available from: <http://www.windowsecurity.com/pages/security-policy.pdf> (Accessed 9 October 2008).
- [6] Piscitello, DM. 2009. *Guide to network security*. TechTarget. The IT Media ROI Experts. Available from: [http://searchsecurity.imix.co.za/static/pdf/cisco/Eguide\\_NetworkSecurity.pdf](http://searchsecurity.imix.co.za/static/pdf/cisco/Eguide_NetworkSecurity.pdf) (Accessed 07 April 2009)
- [7] *Data classification*. 2007. Available from: [http://searchdatamanagement.techtarget.com/sDefinition/0,,sid91\\_gci1152474,00.html](http://searchdatamanagement.techtarget.com/sDefinition/0,,sid91_gci1152474,00.html) (Accessed 14 December 2008)
- [8] *7 things you should know about instant messaging*. 2005. Available from: <http://connect.educause.edu/Library/ELI/7ThingsYouShouldKnowAbout/39385?time=1234488280>. (Accessed 5 February 2009).

Proceedings of ISSA 2009

- [9] Wilson, M. & Hash, J. 2003. *Building an Information Technology Security Awareness and Training program*. National Institute of Standards and Technology. Available from: <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf> (Accessed 17 April 2009).
- [10] *Privacy and Data Protection Draft Bill*. 2006. Available from: <http://www.pmg.org.za/node/14653> (Accessed 18 February 2009).
- [11] Rothke, B. 2008. *The lack of Security in Fax Machine and How to Secure it*. Available from: <http://www.brighthub.com/computing/enterprise-security/articles/8262.aspx> (Accessed 13 January 2009).
- [12] Framingham, DD. 2008. *Outsourcing and offshoring: A Security Expert's views, Beware of traps and pitfall*. Available from: <http://computerworld.co.nz/news.nsf/spec/7DE10CD28E670122CC2575070082D737> (Accessed 24 November 2008).
- [13] *Incident Response*. 2002. Available from: <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/ch-response.html> (Accessed 02 February 2009).
- [14] Herricott, L. 1997. *Disaster Recovery Journal*. Available from: [http://www.drj.com/new2dr/w3\\_006.htm](http://www.drj.com/new2dr/w3_006.htm) (Accessed 5 December 2008).
- [15] *Telecommuting*. 2009. Available from: <http://www.webopedia.com/TERM/t/telecommuting.html> (Accessed 2 February 2009).

## **Concealing the Medicine: Information Security Education through Game Play**

**Thomas Monk, Johan van Niekerk and Rossouw von Solms**

Institute for ICT Advancement, Nelson Mandela Metropolitan University

s20520515@nmmu.ac.za, 0848425028, PO Box 77000, School of ICT,  
Nelson Mandela Metropolitan University, 6031

Johan.VanNiekerk@nmmu.ac.za, 0415043048, PO Box 77000, School of  
ICT, Nelson Mandela Metropolitan University, 6031

Rossouw@nmmu.ac.za, 0415043604, PO Box 77000, School of ICT,  
Nelson Mandela Metropolitan University, 6031

### ABSTRACT

Many threats to Information Security can be avoided if proper information security processes are in place. However, one can only counter threats effectively once sufficient knowledge about information security has been attained. Consequently proper information security awareness through education is necessary. The problem with information security education is that many people are not motivated to attend education sessions, study related material or participate in online courses. Educational games have been around for quite some time, although they have been limited to a narrow range of subject matter. This paper will introduce a current, in progress, research project which focuses on the development of a computer game to teach basic information security knowledge to learners.

### KEY WORDS

Information Security, Information Security Awareness, Educational Gaming

## **Concealing the Medicine: Information Security Education through Game Play**

### **1 INTRODUCTION**

The incorrect usage of information technology has become a huge problem in modern society. Securing informational assets is an essential part of proper information technology usage and thus crucial towards protecting users against risks. Being ignorant to these risks may lead to: A loss of assets, ruining company reputations (Ernst & Young, 2008) and businesses closing down.

*Information security* is the term used to describe how one can safeguard information assets. International practices and frameworks do exist that propose countermeasures that can greatly reduce the risks which threaten information (ISO/IEC17799, 2000; COBIT, 2001). Countermeasures often fail because people, in general, are not aware of the risks involved with information technology. People remain the weakest link for information security (Ernst & Young, 2008; Deloitte, 2009).

Numerous businesses have accepted that information security is a problem, but have not yet been able to solve the problem to an acceptable level. Formal ways to educate staff do exist, however it is exceedingly expensive for companies and businesses to send every employee, who works on a computer, for a training session.

Many people believe that the general public knows too little about information security (Siponon, 2001). Educating the general public about information protection may solve several basic problems associated with information security awareness. Problems such as phishing and password protection are essential in this respect, because these threats are a problem for the general public as well as for major corporations.

The main problem this paper addresses is that the general public and employees are generally not motivated to learn about safeguarding information. Companies sometimes use incentives in order to direct their employees' attention towards information security, e.g. a piece of

chocolate with a note attached about password protection (Albrechtsen, 2007). Security campaigns such as this often fail, because the motivation is directed towards the incentive instead of the information. Motivation needs to be linked to information security in such a way to ensure that knowledge is being gained by the employee. In other words, it should not be possible to eat the chocolate without learning about password protection.

This paper proposes the use of an educational computer game in order to motivate people to learn about information security.

## 2 RESEARCH DESIGN

The project will design and implement a game to teach information security concepts. Both qualitative and quantitative methods will be used to determine whether the game is both fun and engaging, as well as educational.

Initially a prototype will be developed. This prototype will conform to the design considerations outlined in the following section. Further prototypes should be developed against which the original game can be compared.

It is impossible to develop a prototype of every single game type known to man and it is also impossible for participants to play and evaluate every type of game. For these reasons it has been decided that only three games should be developed for this study. It is very difficult to evaluate how much fun something is, however, it can be determined what is more enjoyable between a small number of activities. In the same way it is very difficult to determine what game type is the most fun to play, however it is possible to determine which of these three types of games is more enjoyable for a given test audience. A relatively fun game is sufficient for the purposes of this study.

Although the second game will have the same features and lessons as the original game, it will not abide by the recursion principle mentioned in the following section. The game will not be limited to a time period, instead the game will continue until the player has *game points* (money) left. The score will be determined by how long the player had any *game points* left.

This means that money threatening events will happen more often and will affect the player's total amount of *game points* more severely as the game continues. One might argue that this is a better approach to teach someone a lesson.

The third game will also have the same features and lessons as the original game, however the game will explicitly tell the player what to do in order to progress in the game. A story should be linked to a game such as this. It can be argued that a lot of people do not want to guess what is right through experimentation but rather be told what to do. This game will test whether the previous statement is true.

These three games can be compared with each other because essentially it **is** the same game with just different ways of playing it. They can be compared to determine which game is more popular and thus making it more fun. This is accomplished by placing all three games on a network and digitally counting how many times the game was started and how many times the game was completed. It is possible that there will not be a clear-cut winner to the popularity test, in which case it is necessary to consider having multiple games as part of the solution.

After it has been determined which game is the most fun, a survey needs to be conducted to test what the players have learnt and what they thought of the game. At the start of the survey participants will be presented with a questionnaire asking them:

- ♠ How often do they play games?
- ♠ What game genres or style of game play do they like?
- ♠ How much do they know about information security?

Following the questionnaire, this group of participants should play the game a couple of times and answer another questionnaire asking them:

- ♠ What did they think of the game?
- ♠ How much have they learnt about information security?

Note that the questionnaires should not give the impression that the game is an educational game. Questions asking about information security knowledge should be carefully constructed and placed close to general questions which will hide the fact that the survey is mostly about



what knowledge the player has acquired. It is also important to ask the same questions about information security before and after the study to ensure that knowledge is being increased.

A fundamental flaw with the solution proposed in this paper is that some people are not interested in games and thus not motivated to play them. The survey will also address this issue by determining what people who do not like games, thought about the game. The survey might show that those people changed their opinion based on this game or that more research should be conducted to motivate these people.

The main aim of the survey will be to determine whether the game is educational, thus proving that the game is fun and also teaches information security knowledge.

### **3 PROBLEMS IN CURRENT INFORMATION SECURITY EDUCATION AND AWARENESS**

Information is a valuable asset to most businesses. Many ways exist that mitigate risks that threaten the safety of information assets. Several of these risks cannot be prevented if the users of the system are not educated to act securely (van Niekerk & von Solms, 2007). Users are often ignorant of the magnitude of their actions towards information systems.

Common methods that companies use to educate their employees on information security include: posters, training sessions and online tutorials. It can be argued that these methods cause several problems:

- ♠ Posters become part of the office sentry and only temporarily remind employees of a specific information security threat.
- ♠ Training sessions are usually expensive and waste time.
- ♠ Online tutorials are also time consuming and are difficult to govern.

These and other methods have an underlining problem of sometimes not motivating the employees enough for them to fully grasp the awareness aspect of information security.

The general public also suffers from a lack of information security awareness (Siponen, 2001). This is becoming an immense concern partly

Proceedings of ISSA 2009

due to phishing attacks, the increasing use of email passwords and online banking.

Email services and bank websites usually instruct their users what not to do, however there are users who ignore risks thinking that nothing will happen to them. A user who does not care about information risks can be described as looking through rose-coloured spectacles (Siponen, 2001).

Again, the underlying problem can be largely contributed towards a lack of motivation.

In order to understand why motivation is lacking with respect to information security awareness the top information security threats should be identified. The top eight recurring external information security threats as described by (Deloitte, 2009) are:

- ♣ Email attacks, such as spam
- ♣ Phishing/pharming
- ♣ Virus/worm outbreaks
- ♣ Spyware
- ♣ Employee misconduct
- ♣ External financial fraud involving information systems
- ♣ Social engineering
- ♣ Physical threats

(Rothke, 2005) identifies a lot of the same threats stating that these are things that **every employee** should be aware of.

As mentioned earlier, the primary purpose of the research described by this paper is to design an educational game that will hopefully help address the motivational problems surrounding information security education.

The following section of this paper explains the process which should identify a suitable type of game to motivate people about information security. The process extends in order to prove that this game will make them aware of the top eight information security threats. This should play a role in the solution of widespread information security awareness.

#### 4 EDUCATIONAL GAMES

Video games have been very successful in the last couple of years. Good games generate enough fun and enjoyment for the player to remain engaged for long periods of time. Educational games are games that have an added goal in mind: They also attempt to teach the player about a certain topic.

Educational games have been described as “edutainment” (Moreno-Ger & Burgos & Martinez-Ortiz & Sierra & Fernandez-Manjon, 2008) and “Serious Play” (de Castell & Jenson, 2003) and they have been used as a motivational tool for educators. Unfortunately some of them have also been described as neither fun nor educational (de Castell & Jenson, 2003). Being neither fun nor educational should constitute an educational game as being a complete failure.

There are mixed views of educational games in research, which indicate that although it is a good idea in principle, it is, however, not always implemented well enough. Here are two examples of security related educational games which have been successful.

- ♠ CyberCIEGE as described by (Cone & Irvine & Thompson & Nguyen, 2007) is an educational game that teaches the correct use of computer networks. The game uses a 3D environment to closely match what would happen in real life. CyberCIEGE has been used successfully to teach the US navy about proper network usage. This game shows that security can be taught through game play, however it does not address our problem that relates to information security awareness.
- ♠ Anti-Phishing Phil as described by (Shreng, et al) is an educational game that teaches players to recognise potential phishing attack URLs. This piece of research produced fascinating results when it is compared to more traditional methods of phishing education. The research proves that a video game can be more effective at teaching phishing awareness than existing training material. However, the game is very specific and only teaches security prevention from phishing attacks. The game is also limited when it comes to further investigation by means of additional research.

## 5 THE GAME DESIGN

This paper proposes the design and development of a money management game to motivate people to learn about information security. The players will start the game with a small amount of money, after which they will be faced with decisions that affect the total amount of money they own. These decisions could be: investment decisions, banking decisions or job opportunities. Some decisions will result in gaining money while some decisions will result in spending money. Events are also prevalent where the game attempts to steal your money. These events can be mitigated if proper security processes are in place.

This is where information security awareness comes into play. Most of the threats on the player's money will be related to information security. However, the game will not explicitly mention information security (the medicine). This is what is meant by "Concealing the medicine". This technique is used because of the negativity surrounding information security and educational games (Moreno-Ger, 2008).

The game will be presented as a regular game with only one goal: To be entertaining. The players should be oblivious of the fact that it is indeed an educational game about information security.

In order to keep the game engaging while exposing content the following principles are proposed:

- ♠ The process of playing the game should directly relate to learning the educational content in the game. As explained in the above paragraph, in order to become good at the game the player must successfully secure his/her assets, which can only be done by having an understanding of information security. How tightly integrated the learning process is to the game play should directly relate to the overall appeal of the game. This also ensures that someone cannot "cheat" their way out of learning, in other words, to become good at the game is to become information security aware!
- ♠ The fact that the game is an educational game should be hidden from the player. This is called *stealth learning* (Prensky, 2001) or

Concealing the Medicine: Information  
Security Education through Game Play

*concealing the medicine* by this author. As previously stated the player should feel more comfortable thinking that the aim of the game is to be entertaining. In the game money will represent information assets while many of the risks involved will deal with information security. It is not impossible that the player notices that educational content is being exposed through the game which is not a problem. The biggest goal of this principle is not to give a negative first impression of the game.

- ♠ Learning should be gained through recursion and experimentation. A good way to learn something is to discover it yourself after gaining some experience. Making the game quick and easy will motivate the player to play it again and again, which is what is meant by recursion. Giving the player the option to do something the wrong way and clearly explaining why it is wrong will give the player a sense of experience as they experiment with their options. This process should make the learning experience more memorable because the student has learnt something by himself/herself and uses his/her findings several times.

However, some threats will not always penalise the player. In the game, if someone suspicious offers you a business proposal (pyramid scheme or otherwise), by buying into it will not necessarily cause a loss of money, but might bring the player high returns. This is essential to the overall appeal of the game because it keeps the player guessing by changing the game every time. This also maps closer to the real world. Indeed, to learn the lesson a high percentage of suspicious business proposals will be scams, thereby revealing that it is in fact a huge risk. What is being learnt by using the system is being aware of risks, which will still be accomplished by playing this kind of game.

- ♠ The game should make mundane tasks fun. Irritating events can spoil a good game, by making these events fun it can stimulate the players while they are learning. Password protection could be one such event. In the real world it is quite frustrating to enter one's password into the computer every time you use it. Why should the same action put into a game be any different? Password protection is an important lesson to be learnt. Thus by making the process

more fun, it should make the overall game play better while giving a positive reflection on tasks such as password protection.

- ♠ The game should make use of a points system. The player will have points added when they do things correctly and points deducted when they do things incorrectly. In the game presented above *money* will serve as these points. On completion of the game the final score (total amount of money) will be presented to him/her. The player can clearly deduce whether this score is better than his/her previous scores and whether this score is better than their friends' or colleagues' scores. What often follows is that the newly acquired score is less than the comparable scores, resulting in a desire to play the game again in order to receive a better score.

Note that these principles can be applied to other educational games, thus enabling further research being conducted, on these principles, in the future.

## 6 CONCLUSION

Information security awareness is a big problem. By implementing an educational game to spread awareness might be a big step in the right direction. Using techniques such as “Concealing the medicine” can be a key towards improving the quality of these educational games.

In order to test whether this educational game is successful, one has to test whether it is fun and whether it exposes educational content.

Not all people like video games, in this case the authors are “concealing the medicine in chocolate” for people who “do not have a sweet tooth”. However, it is the author’s opinion that good game principles can result in a game where quality may result in “chocolate” that may be irresistible to virtually anyone.

## 7 REFERENCES

- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security* 26 ( 2007 ) 276 – 289.
- COBIT. (2001) Governance, control and audit for information and related technology (COBIT). 3rd ed. *IT Governance Institute, ISACA, ISACF, ISBN 1-893209-13-X.*
- Cone. B. & Irvine. C. & Thompson. M. & Nguyen. T. (2007). A video game for cyber security training and awareness. *Computers & security* 26 ( 2007 ) 63 – 72.
- de Castell, S., & Jenson, J. (2003). Serious play. *Journal of Curriculum Studies*, 35(6), 649–665.
- Deloitte. (2009). The 6th Annual Global Security Survey.
- Ernst & Young. (2008). Global Information Security Survey.
- ISO/IEC177799. (2000). Information security management – part 1: code of practice for information security management.
- Moreno-Ger, P., & Burgos, D., & Martinez-Ortiz, I., & Sierra, J., & Fernandez-Manjon, B. (2008). Educational game design for online education. *Computers in Human Behavior* 24 2530–2540.
- Prensky. M. (2001). Digital Game-Based Learning.
- Rothke, B. (2005). Computer security: 20 Things every employee should know, Second edition.
- Siponen, T. (2001). Five Dimensions of Information Security Awareness. *Computer and Society.*
- Sheng, S., & Magnien, B., & Kumaraguru. R., & Acquisti. A., & Cranor. L., & Hong. J., & Nunge. E. (2007). *ACM International Conference Proceeding Series; Vol. 229 88-99*
- van Niekerk, J., & von Solms, R. (2007). A web-based portal for information security education.

Proceedings of ISSA 2009



Management, Processing and Analysis of Cryptographic Network Protocols

## MANAGEMENT, PROCESSING AND ANALYSIS OF CRYPTOGRAPHIC NETWORK PROTOCOLS

<sup>1</sup>Bradley Cowie, <sup>2</sup>Barry Irwin and <sup>3</sup>Richard Barnett

Rhodes University

<sup>1</sup>g06c5476@campus.ru.ac.za

<sup>2</sup>b.irwin@ru.ac.za

<sup>3</sup>barnettrj@acm.org

### ABSTRACT

The use of cryptographic protocols as a means to provide security to web servers and services at the transport layer, by providing both encryption and authentication to data transfer, has become increasingly popular. However, we note that it is rather difficult to perform legitimate analysis, intrusion detection and debugging on cryptographic protocols, as the data that passes through is encrypted. In this paper we assume that we have legitimate access to the data and that we have the private key used in transactions and thus we will be able to decrypt the data. The objective is to produce a suitable application framework that allows for easy recovery and secure storage of cryptographic keys; including appropriate tools to decapsulate traffic and to decrypt live packet streams or precaptured traffic contained in PCAP files. The resultant processing will then be able to provide a clear-text stream which can be used for further analysis.

### KEY WORDS

Cryptographic, network, protocols.

## MANAGEMENT, PROCESSING AND ANALYSIS OF CRYPTOGRAPHIC NETWORK PROTOCOLS

### 1 INTRODUCTION

This paper describes research in the field of cryptographic protocols, currently being performed in the REMOVED. While this research is not entirely novel, as it makes use of elements from existing research in the detection of encrypted applications [2], we consider a generic solution to the given problem of analysing encrypted traffic with the intention of later extension to provide support for multiple protocols and performing further analysis than application detection. This paper provides a starting point for further research into the evaluation and analysis of supposedly secure applications and suggests an outline for the development of a framework which could perform this.

Cryptographic protocols are a vital component of information security [9] as a means of securing modern networks against would-be attackers by providing data integrity, encryption and authentication to network traffic at the transport layer [12]. Sensitive information, such as banking details, that transverse networks will most likely do so through an encrypted tunnel provided by the cryptographic protocol; it is thus imperative that both the protocol itself is secure and the applications use of the protocol is correct and sensible. A recent paper by Lee *et al.* shows that in a study of over 19000 web servers, 98.36% of the servers provided support for TLS and 97.92% provided support for SSLv3.0 and 85.37% provided support for SSLv2.0 [4]. These statistics serve to show the prevalence of SSL/TLS and the need to support these protocols.

We now present cases for the need for such research and the development of a framework that allows for the decryption of encrypted traffic.

HTTPS has become prevalent as a means to communicate with a web server securely; however if an attacker were to use HTTPS as a means to perform an attack, it becomes difficult to detect such an attack due to the encrypted nature of the traffic. It would be useful if a system existed to

## Management, Processing and Analysis of Cryptographic Network Protocols

decrypt this traffic and then perform analysis. This is highlighted by work done by Marklinspike [5] in developing a tool, SSLStripper, that removes the secure components of a connection allowing for a new form of MITM (man in the middle) attack where the user believes that his connection is secured (using HTTPS) but in reality messages are passed through HTTP, and are intercepted by a third-party. Furthermore the SANS institute announced “Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites” as the top security menace in the “Top Ten Cyber Security Menaces for 2008” with “Web Application Security Exploits” in 8th position [7].

Wang *et al.* [14] comment that in the long term, software development cannot afford to consider implementing security only after the application has been developed or late in the development cycle as irreparable security compromises may already exist and that attempts to correct them would require significant resources. Further we consider that security is one of the core metrics in McCall’s Software Quality Checklist [1]. However, software development is notorious for being over budget and far exceeding its expected completion date; as a result we often find that security is left until late in the development cycle and sometimes even after the application has been built [14]. Often this causes poorly implemented security and this only serves to degrade the quality of the system built as it provides the user with a false sense of security; further an insecure application that passes and receives sensitive information is as equally unusable as an application that fails to meet its specifications in terms of correctness [14]. We could argue that the reason why security is not part of many development cycles in earlier stages is due to the difficulty and tedium of checking the correctness of security [10, 11]. To put this in context, if we consider that between January 2004 and December 2008, there have been 26139 reported security vulnerabilities [6]. It would be useful if there existed a framework that decrypted data and then provided some analysis on issues pertaining to the implemented security.

The remainder of this paper will consider the construction of such a framework, with the following sections. Section 2 contains related work, while Section 3 provides a brief of overhead of the architecture involved for SSL. Section 5 details the approach to be taken and Section 4 highlights the expected goals on completion.

## 2 RELATED WORK

The analysis of cryptographic protocols is a subject that has been extensively researched with algebraic models to provide descriptions of protocols and techniques such as, BAN Logic and Running Mode Analysis, to provide formalizations to determine whether a protocol is correct in terms of achieving its goals of authentication and data integrity. Research into security and software development is also widely available for discussion of implementations of security into development lifecycles and evaluation of implemented security mechanisms. Furthermore there are a number of systems which, to some degree, provide some of the features already discussed. In this section of the paper we discuss some of the related work around existing software that could possibly be used to perform the functionality outlined in Section 1. We will consider some research that may be beneficial when considering such a framework.

### 2.1 Running Mode Analysis

Running Mode Analysis is a technique for the formal analysis of cryptographic protocols. It makes use of conclusions derived from model checking. The central component of Running Mode Analysis involves creating a system including an attacker, a protocol and two parties attempting communication and then discovering all of the possible modes the system can enter. For example, in a three-principal security system there are seven running modes; if we can show that these seven modes do not exist then the protocol is deemed to be safe within the system. When working with complex protocols, such as SSL, it is a matter of decomposing the more complex protocol into a number of smaller protocols and then performing Running Mode Analysis on each of the simpler protocols. This sort of analysis is often done by hand and provides an interesting means of the verification of the correctness of a protocol. In a by paper Zhang and Liu [15], running mode analysis is performed on the SSL Handshake protocol. While it may not be important to perform such an analysis, as such research already exists; it's important to understand that many protocols are fundamentally flawed and identification of such flaws when providing analysis of application security would be a useful addition.

## 2.2 Practices in SSL/TLS

It has already been mentioned that cryptographic protocols are a popular method of securing web servers. We need to consider that simply providing support for cryptographic protocols is not sufficient to provide adequate security. Lee *et al.* [4] produce a tool, the PSST (probing SSL Security Tool), to perform analysis of over 19000 web servers employing SSL/TLS. They conclude from their results that in 2006, 85.37% of the over 19000 web servers still provided support for SSLv2.0, a fundamentally flawed protocol due to weakness to Man in the Middle (MITM) attacks, while 66.55% of servers still supported DES-40 encryption even though the US export laws limiting the key length of DES to 40 bits is no longer in effect. It is unwise to still provide support for SSLv.2.0 as its well documented that MITM attacks can force the adoption of a weak encryption protocol like DES-40 creating a large and exploitable vulnerability for brute force attacks. While adaption of new algorithms such as AES, is prevalent, the rate at which old standards are no longer being supported is not sufficiently rapid; it is, therefore, important that these issues are highlighted when performing analysis of a systems security.

## 2.3 Detection of encrypted applications

The use of libraries such as openssl provides a means to add encryption to generic traffic; this creates a problem for the analysis of network traffic as the traffic is now encrypted. For example, most common torrent clients provide a means to encrypt traffic or by means of using an encrypted tunnel provided through SSH as a means to avoid the content blocking of p2p applications. This makes it difficult to block or limit certain types of traffic which may be the goal of a network administrator. Bernaille and Teixeira [2] suggest a system for the early recognition of encrypted applications is outlined and developed with a high degree of success in terms of identification of applications within an SSL connection. They take the approach of using specific parts of the TCP payload to identify the SSL connection by studying said traffic in detail and then producing patterns to be used in detection methods. A similar methodology of analysing the TCP payloads could be incorporated into the research topic.

## 2.4 Related tools

A number of tools exist that provide means to analyse SSL; these include SSLDump and SSLSniffer. SSLdump [8] is an SSL/TLS network protocol analyzer which identifies TCP connections on the chosen network interface and attempts to interpret them as SSL/TLS traffic. When it identifies SSL/TLS traffic it decodes the records and displays them in a textual form to stdout. If given the cryptographic keys involved it can be used to decrypt the traffic passing through. SSLSniffer [3] provides similar functionality as SSLDump with the exception that it can act as a SSLv3/TLS and SSLv2 proxy server. The issue with these sorts of tools is two-fold, they don't provide any security analysis and further they are protocol specific.

## 3 ARCHITECTURE OF SSL/TLS

It is important to understand the underlying architecture for each of cryptographic protocols for implementation is intended. We will consider the architecture of TLS focusing solely on the Handshake Phase, as it is the most significant to the development of the framework. Extension to other protocols would require similar understanding. Firstly, we consider some of the goals of SSL/TLS as these goals dictate the structure of TLS [12]. TLS aims to provide a secure connection between two parties with interoperability, extensibility, allowing for incorporation of encryption algorithms or hashing functions and efficiency provided by caching. We will consider the basic architecture of TLS as it is very similar to the architecture of SSLv3.0. For our purposes, we need only to consider the Handshake phase of SSL.

### 3.1 The Handshake

During this phase decisions are made as to what cryptographic parameters are to be used for the actual TLS connection. This include deciding on the protocol version, selecting a cipher suite and performing some secret key exchange.

The client sends a client hello message to the server. The server then possibly responds with a server hello message. If there is no response then a fatal er-

## Management, Processing and Analysis of Cryptographic Network Protocols

ror occurs and the connection is closed. These hello messages establish: the protocol version to be used, session ID, cipher suite to be used, compression algorithm to use, clientHello.random and ServerHello.random. The actual key exchange may consist of up to four messages containing: the Server Certificate, the Client Certificate, the Server Key Exchange and the Client Key Exchange. If the Server Certificate is to be authenticated it is sent after the hello messages phase. Following that the Server Key Exchange message may be sent if necessary. If the server passes the authentication, it may request the Client Certificate (if the client has one and if it is required by the cipher suite). The server then sends a Hello Done message back to the client indicating the end of the Hello Message part of the handshake is complete. The server then waits for a for a client response. If the certificate request message was sent then the client needs to respond with a certificate. The client will then send its Client Key Exchange message with the contents dependant on the public key encryption algorithm chosen. After the exchanges have taken place a Change Cipher Suite Message is sent from the client to server. The client then sends new messages containing the new algorithms and keys. The server responds by sending a Change Cipher Suite Message back with the new keys and algorithms. The handshake is then complete [12].

## 4 RESEARCH OUTCOMES

The authors intend to develop a framework that could be used to evaluate the correct implementation of security protocols in software and other analysis of encrypted network traffic. In this regard the framework needs to be able to decrypt traffic that has been encrypted by a specific algorithm, further it needs to be able to determine which algorithm has been selected to provide encryption; in the case of SSL/TLS this is a case of inspecting packets sent during the SSL handshake. Once plain-text has been obtained the developer can inspect the payload of the messages being sent was and can use this to perform a form of manual debugging. Seeing as a number of security related parameters can be derived from examining the SSL handshake , it would be useful to alert the user to possible security issues such as the use of keys generated on the Debian platform during the Debian/OpenSSL security breach [13] or suggesting that certain cryptographic algorithm be removed from the cryptographic algorithms supported during negotiation in the case

of SSL/TLS. For example 40-bit DES is considered to be extremely insecure as it is weak to brute-force attacks or even suggesting that support of SSLv2.0 is a security risk as SSLv2.0 is well-documented as a flawed protocol. It would also be useful to check the entropy of the cryptographic keys used. Once the system has been developed some form of assessment needs to be performed on the usefulness of such a system; this could be performed by distributing the system to a number of users and collecting feedback or by developing a number of test applications with glaring security flaws and then evaluating the output produced. In this way we can further determine if the system is of any practical use to developers.

## 5 APPROACH TO RESEARCH

Firstly, we assume legitimate access to the data or network connection and that the private keys used are available. As this system would be used in a legitimate context, there is no reason for the private keys to not be available for use; attempting to recover private keys is outside of the scope of the research context of this paper. The objective is to produce a suitable application framework that permits easy recovery and secure storage of cryptographic keys; including appropriate tools to decapsulate traffic and to decrypt live packet streams or precaptured traffic contained in PCAP files. The authors propose the development of a system to capture packets, filtering for TCP packets only (or to parse a dump files for TCP packets only) mostly likely written as a simple C++ application and making use of *libpcap* or *WinPcap* (implementation dependant). This application then removes the headers of the packet and considers the SSL/TLS handshake that has occurred, so as to recover the public key and cipher suites used. The resultant processing will then be able to provide a clear-text stream which can be used for further analysis. The framework should be implemented for protocols that use the standardized hybrid cryptographic protection system such as IPSec, TLS, SSL 3.0 and SSHv2. An issue of concern is the recovery of the nonce, which could either be retrieved by changing the server applications or more practically by having another trusted system holding a second copy of the private key. An investigation as to how to sensibly store cryptographic keys is also required as they form a central component of this system. Figure 1 illustrates this in diagramatic form.



## Management, Processing and Analysis of Cryptographic Network Protocols

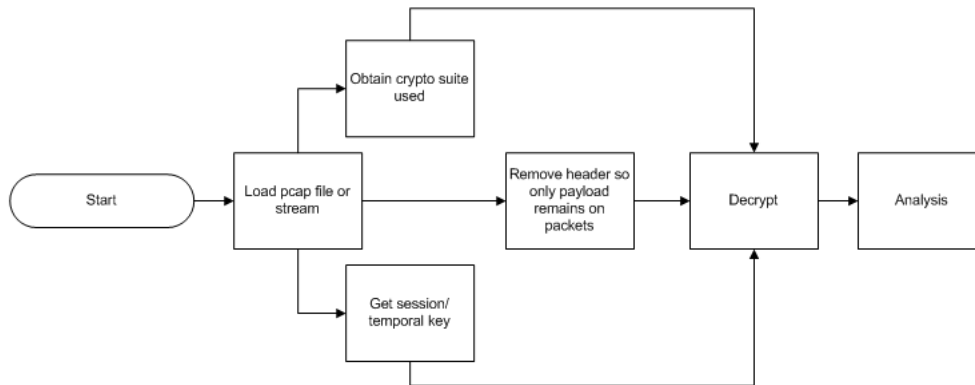


Figure 1: Diagram of Proposed System Design

## 6 CONCLUSION

This paper has discussed the need for a framework to provide a means to decrypt encrypted traffic for debugging needs within software development and also as a means to provide analysis of encrypted traffic and has outlined the system to be developed. At this stage, the research is still in its formative stage. We expect that if the system is developed correctly, and is adopted as a component in system development, that it may provide a standard to ensure correctly implemented security systems and that it would also be useful to network analysts. The system could later be extended for development with other protocols, possibly including IPsec and SSH.

## ACKNOWLEDGEMENT

The authors would like to acknowledge the support of REMOVED.

## References

- [1] Reesa E. Abrams. A checklist for developing software quality metrics. In *ACM 82: Proceedings of the ACM '82 conference*, pages 5–6, New

Proceedings of ISSA 2009

- York, NY, USA, 1982. ACM.
- [2] Laurent Bernaille and Renata Teixeira. Early recognition of encrypted applications. pages 165–175. 2007.
  - [3] Eu-Jin Goh. Sslsniffer. Online: <http://crypto.stanford.edu/~eujin/sslsniffer/index.html>.
  - [4] Homin K. Lee, Tal Malkin, and Erich Nahum. Cryptographic strength of ssl/tls servers: current and recent practices. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 83–92, New York, NY, USA, 2007. ACM.
  - [5] Marlinkspike. New tricks for defeating ssl inpractice. 2009.
  - [6] NIST. National vulnerability database. Online: <http://nvd.nist.gov/>.
  - [7] Alan Paller. Top ten cyber security menaces for 2008. 2008.
  - [8] Eric Rescorla. Ssl dump. Online: <http://www.rtfm.com/ssldump/>, 2005.
  - [9] Schneier. *Applied Cryptography*. Wiley and Sons, 1996.
  - [10] B. Schneier. Security in the real world: How to evaluate security. *Computer Security Journal*, v 15, pages 1–14, 1999.
  - [11] Bruce Schneier. Why cryptography is harder than it looks. Online: <http://www.schneier.com/essay-037.html>, 1997.
  - [12] C. Allen T. Dierks. The tls protocol version 1.0. *RFC Editor*, 1999.
  - [13] Debian Security Team. Debian security advisory:dsa-1571-1 openssl – predictable random number generator. Online: <http://www.debian.org/security/2008/dsa-1571>.
  - [14] Huaiqing Wang and Chen Wang. Taxonomy of security considerations and software quality. *Commun. ACM*, 46(6):75–78, 2003.
  - [15] Yuqing Zhang and Xiuying Liu. Running-mode analysis of the security socket layer protocol. *SIGOPS Oper. Syst. Rev.*, 38(2):34–40, 2004.

## Mobile Communications Security Research at CSIR-MDS

### Research in Progress

## Mobile Communications Security Research at CSIR-MDS

**Anna BAdimo** & **Fisseha Mekuria (PhD.)**

Competency Area Manager      Principal Research Scientist

[abadimo@csir.co.za](mailto:abadimo@csir.co.za)

[fmekuria@csir.co.za](mailto:fmekuria@csir.co.za)

**CSIR Modelling & Digital Sciences, Information Security Unit**

**CSIR Pretoria 0001, South Africa**

### **Abstract:**

The explosive growth of mobile communications technology and services in emerging markets has resulted that access to information resources and storage of sensitive information using mobile phones is increasing. At the same time the capabilities of mobile terminals and bandwidth of mobile networks is improving. To protect the information stored in mobile phones and to make it possible for mobile phone owners to utilize the vast amount of different mobile ICT services, it is important that security mechanisms with scalable encryption and authentication keys is available. The need for such security mechanisms is increasing proportionally with the explosive growth in mobile wireless communications. South Africa as one of the progressive emerging markets needs to address mobile security issues with the aim to develop the mobile enterprise and consumer services sector. Therefore CSIR modelling and digital sciences department, as a main stakeholder in the mobile ICT technologies and services in South Africa, have started a mobile communications security research group in collaboration with research institutes locally and abroad.

This paper will present the case study for and the proposed mobile communications security research. The mobile security research is based on several years of work in mobile wireless communications area and is composed of three parts:

- **Secure mobile terminal platforms:** Mobile data security and low power encryption and authentication mechanisms.
- **Next generation mobile wireless network security:** Radio access and handover security. (MS ↔ BTS,APs), and End-to-end security issues.
- **Secure Mobile Services :** Scalable security architectures for the vast amount of mobile services expected.

The research proposal also encompasses a human capital development aspect where several research proposals in collaboration with research universities and institutes, is expected to result in several research PhDs and the development of research and educational curriculum in the areas of mobile wireless communications security. The idea with this paper is to highlight and promote awareness to mobile-wireless security research and promote formation of collaborative research projects with research institutes in South Africa. The following section discusses one of the areas that the group at the CSIR is currently involved in. The research effort is focused to build a scalable platform to make mobile services secure and usable.

**Research in Progress I:**

***A Scalable Platform for Secure Mobile Services***

Nowadays mobile phone users are able to access a large number of services requiring some form of authentication. Making mobile services reliable is possible only by building security and authentication mechanisms, so that confidence and trust is built between service providers and customers. At the same time secure mobile services reduce fraudulent and unauthorized access to mobile broadband content and services, promoting the continued growth of mobile broadband technology and services. Secure mobile services require the development of security aware mobile platforms and network protocols. Depending on the type of services on demand the dimensions and rigor of security mechanisms can vary. As shown in figure 1 below, mobile services such as financial transactions (M-Banking, M-Payment) and mobile enterprise services will require high security, while public information access such as an M-E-Government application might need a low security level. Another important aspect that needs research is the interplay between strong/low security and less/better usability aspect of mobile services.

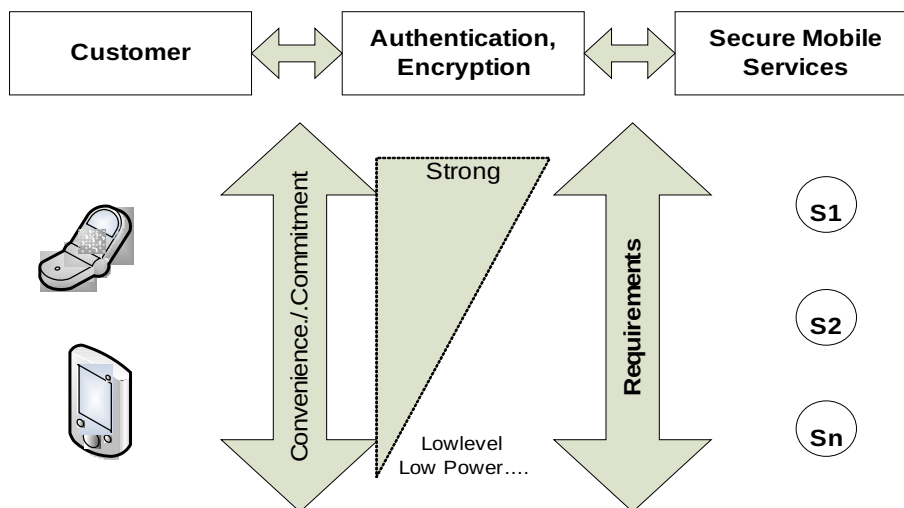


Figure 1, Security Dimensions of Mobile Broadband Services

**References:**

- 1- 3GPP Technical Specification: "Generic Authentication Architecture." 3GPP TS 33.222, 2007.
- 2- ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional Architecture", ETSI ES 282 007 V1.1.1, March 2006.
- 3- F. Mekuria, I.Rai "Issues in Next Generation Wireless Network Technologies & Services for Developing Regions", Proc. of Mobicom-08, WiNS-DR, Sept. 15-19,2008, San Francisco, USA.
- 4- Lu et.al., "A secure and Service-oriented Network Control Framework for WIMAX Networks.", IEEE Communications Magazine, Vol, 45, May 2007.

## Chapter 8

# A FORENSIC READINESS MODEL FOR WIRELESS NETWORKS

Sipho Ngobeni, Hein Venter and Ivan Burke

**Abstract** Over the past decade, wireless mobile communications technology based on IEEE 802.11 wireless local area networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cyber crime, where criminals deliberately and actively break into WLANs with the intent to cause harm or access sensitive information. WLAN digital forensics is seen not only as a response to cyber crime in wireless environments, but also as a means to stem the increase of cyber crime in WLANs. The challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile devices and conduct a proper digital forensic investigation. This paper attempts to address this issue by proposing a wireless forensic readiness model designed to help monitor, log and preserve wireless network traffic for digital forensic investigations. A prototype implementation of the wireless forensic readiness model is presented as a proof of concept.

**Keywords:** Wireless local area networks, digital forensic readiness

## 1. Introduction

Wireless technologies have become very popular around the world. Wireless local area networks (WLANs) or “hotspots” blanket public places such as convention centers, airports, schools, hospitals, railway stations, coffee shops and other locations to provide seamless public access to the Internet [15]. These hotspots provide several advantages over hard-wired networks, including user mobility and flexible Internet access. However, due to their open nature, WLANs have become a major target for cyber criminals.

WLAN digital forensics involves the application of methodologies and tools to intercept and analyze wireless network events for presentation



as digital evidence in a court of law [9]. As such, WLAN digital forensics is complementary to intrusion prevention – when intrusion prevention fails, WLAN digital forensics is useful for obtaining information about the intrusion. However, the primary challenge in WLAN digital forensics is to acquire all the digital evidence related to a crime [6]. This challenge arises from the fact that the devices participating in a WLAN environment are mobile. Furthermore, since the devices are not always connected to the network, it is difficult to attribute criminal activity to a particular device.

This paper proposes a wireless forensic readiness model for monitoring, logging and preserving wireless network traffic for digital forensic investigations. The wireless forensic readiness model builds on the work of Rowlingson [7] related to traditional forensic investigations. A prototype implementation of the readiness model is presented as a proof of concept.

## 2. Wireless Local Area Networks

WLANs represent a ubiquitous technology that provides seamless high-speed Internet connectivity at public locations. Unlike traditional LANs, WLANs connect computers to the network without physical (wired) connections. WLANs offer tremendous user mobility, enabling users to access files, network resources and the Internet [8].

### 2.1 Criminal Misuse of WLANs

The lack of a physical connection between a WLAN and its participating mobile devices causes crimes to remain discreet, especially since the mobile devices are potentially far removed. This fact needs to be considered when digital evidence is identified and collected in an investigation involving wireless traffic. Potential criminal misuse of WLANs include [12, 14]:

- **WLAN Detection and Connection:** This type of misuse involves an intruder using the wireless medium as a tool to commit other criminal activities (e.g., unauthorized use of the WLAN or use of the WLAN as a launch pad for other criminal activities).
- **Concealment of Digital Evidence:** This type of misuse involves hidden wireless devices or hidden wireless networks (e.g., fake access points).
- **WLAN as an Attack Vector:** This type of misuse involves attacks against the networked (mobile) devices originating from the wireless network, and attacks against the WLAN medium itself.

## 2.2 Sources of Digital Evidence

WLANs typically incorporate 802.11-based wireless devices. The locations where digital evidence is stored on devices and the extraction of evidence are dependent on the specific wireless device. However, the fundamental problem with 802.11-based wireless devices is their lack of a physical footprint, which is the most crucial issue in the identification of these devices [14].

It is imperative to locate all the relevant wireless devices in a digital forensic investigation. Various open source and commercial tools (e.g., Wireshark, Kismet and AirCapture) may be used by a digital forensic investigator to identify wireless networks within range, the devices connected to the wireless networks and, possibly, the locations of the wireless devices [13]. The principal drawback of these tools is the high packet drop rate [1]. The large volume of network traffic makes it difficult for the tools to accept and store all the packets; some packets may be dropped, resulting in the loss of evidence.

## 2.3 WLAN Digital Forensics

Digital forensics deals with the investigation of computers and other digital devices believed to be involved in criminal activities [5]. WLAN digital forensics involves the application of methodologies and tools to capture and analyze wireless network traffic that can be presented as evidence in a court of law [9]. A WLAN digital forensic methodology is a digital forensic process; the tools are software systems that intercept and analyze network traffic. A digital forensic process is a procedure that is followed to investigate a particular criminal activity involving digital evidence [2]. Every digital forensic investigation must go through the following phases of the digital forensic process:

- Define the scope and goals of the investigation.
- Determine the work and materials.
- Acquire the images of the devices to be examined.
- Perform the digital forensic analysis.
- Prepare the report.

Currently, EnCase and FTK are the most popular tools used in digital forensic investigations. The phases of the digital forensic process for EnCase are preview, imaging or acquisition, verification, recovery and analysis, restoration and archiving; the phases for FTK are detection,



Table 1. Digital forensic phases for EnCase, FTK and WFRM.

EnCase	FTK	WFRM
1. Preview	1. Detection	1. Monitoring
2. Imaging	2. Identification	2. Logging
3. Verification	3. Analysis	3. Preservation
4. Recovery and Analysis	4. Preservation	4. Analysis
5. Restoration	5. Reporting	5. Reporting
6. Archiving		

identification, analysis, preservation and reporting. Table 1 lists the phases for EnCase and FTK along with those for the wireless forensic readiness model (WFRM), which is described in the next section.

According to Table 1, only the analysis phase is common to EnCase, FTK and WFRM. The preservation and analysis phases are common to FTK and WFRM. However, it is worth noting that the digital forensic processes for FTK and EnCase are essentially the same as far as the general digital forensic process is concerned. This suggests that the phases correlate although they are named differently. The inconsistent naming of phases is due to the fact that the digital forensic processes for forensic tools are not standardized. In this paper, we adopt the general digital forensic process described by Casey [2].

Researchers have studied various issues related to wireless network forensics. Yim, *et al.* [16] proposed a WLAN forensic profiling system for collecting digital evidence after denial-of-service attacks on WLANs. Turnbull and Slay [14] consider the potential sources of digital evidence in 802.11-based wireless networking environments. Then [11] discusses methods for examining wireless access points to determine if the devices of interest are connected or were connected to a wireless network. While these efforts and others are useful, a digital forensic readiness approach for WLANs has yet to be articulated.

## 2.4 Digital Forensic Readiness

The purpose of digital forensic readiness is to reduce the effort involved in performing an investigation while maintaining the level of credibility of the digital evidence being collected [4]. The decrease in effort includes reductions in the time and the cost of incident response. An organization that is “forensically ready” can respond to an attack rapidly and efficiently. In general, reducing the time involved in incident response reduces the cost of the investigation.



Tan [10] discusses an incident in which an intruder took approximately two hours to launch an attack, but digital forensic experts required 40 billable hours to respond to the incident. The response took such a long time because the organization was not forensically prepared for the incident. Organizations deploying WLANs that are at a high risk of cyber attack should be ready to collect digital evidence before an incident occurs. The model presented in the next section addresses the concept of digital forensic readiness in WLANs.

### 3. Wireless Forensic Readiness Model

The most salient characteristic of the wireless forensic readiness model (WFRM) is that it monitors wireless network traffic at access points. The monitored traffic is stored in a log file and the integrity of the stored information is preserved. Thus, the information needed by digital forensic investigators is readily available should the need arise. The availability of the information reduces the cost of conducting the digital forensic investigation because a major portion of the digital forensic process (monitoring, logging and preservation) has already been conducted based on the WFRM.

Figure 1 shows the five phases of the digital forensic process corresponding to the WFRM. As listed in Table 1, the phases are monitoring, logging, preservation, analysis and reporting.

Phase 1 (monitoring) shows several mobile devices (MDs) connected to a WLAN through different access points (APs). The mobile devices use the access points to connect to the Internet. In addition to providing Internet connectivity, the access points are modified (for the purposes of this model) to monitor all the traffic generated by the mobile devices. For security reasons, the monitoring component uses a firewall to filter inbound and outbound wireless traffic. Filtering is the process of controlling access to the WLAN by screening packets based on the content of their headers [15].

Phase 2 (logging) records all the traffic monitored by the access points. Each access point has its own capture unit (CU) that logs the traffic passing through it. The log file is divided into separate storage areas, each consisting of (for example) 1 MB of data. When the buffer of a capture unit is full, a fixed-size block of data is moved to permanent storage. For example, B1 in Phase 2 represents a block of data consisting of 4 MB.

In Phase 3 (preservation), the capture unit sends the accumulated blocks of data to the evidence store (ES). The capture unit computes a hash value for each block of data, which is saved in the hash store

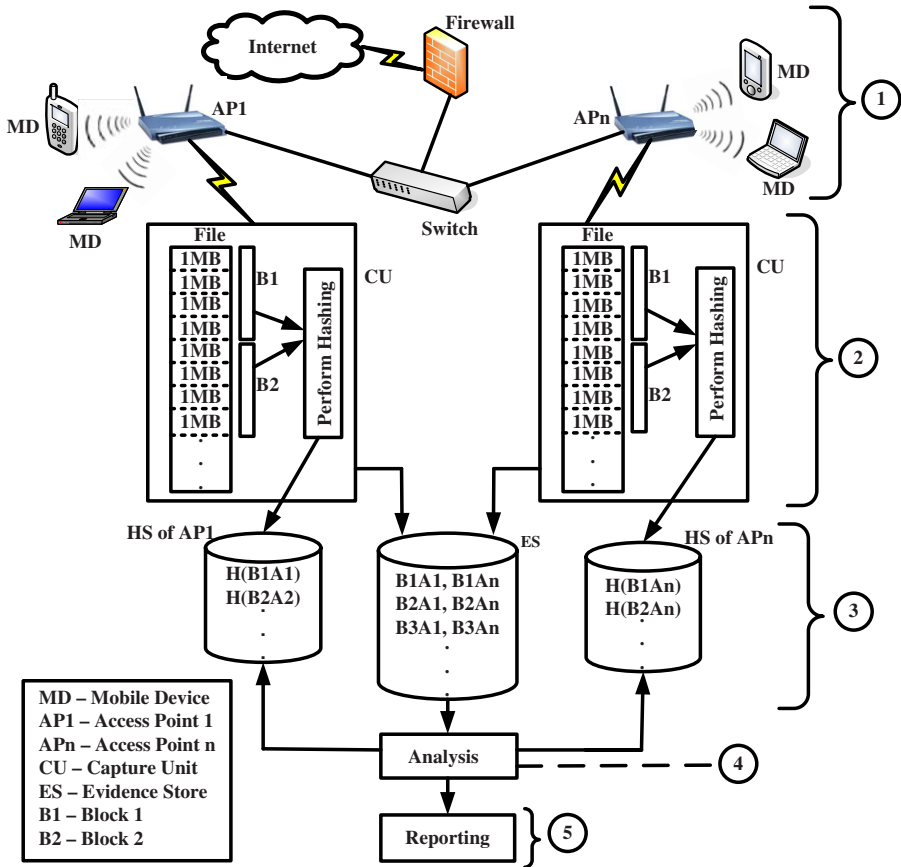


Figure 1. Wireless forensic readiness model (WFRM).

(HS) for integrity checking purposes. Phase 4 involves the analysis of the stored data and Phase 5 involves the creation of a report.

#### 4. WFRM Simulation

The WFRM prototype was simulated using AnyLogic Professional (version 6.0) [3], a Java-based, multi-paradigm, hybrid simulation tool capable of modeling systems as a combination of discrete events, system dynamics and agents. The simulation is designed to validate the use of the WFRM for implementing digital forensic readiness in WLAN environments.

Figure 2 shows a graphical representation of the WFRM before the simulation starts. The *MobileDevice* component generates random simu-

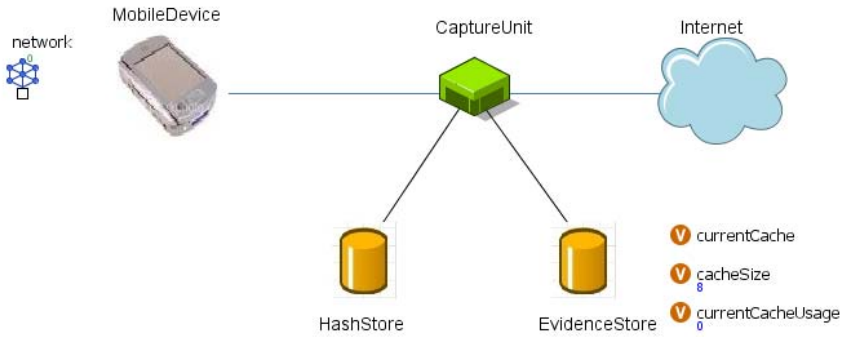


Figure 2. WFRM before the simulation.

lated messages containing source and destination IP addresses, message transmission date and time, and message content.

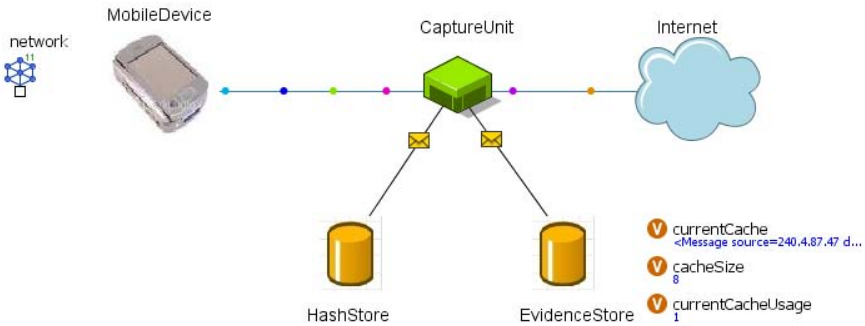


Figure 3. WFRM during the simulation.

Figure 3 shows the simulated messages flowing through the network during the simulation. The simulated messages correspond to the packets that pass through the network from various devices in the WLAN.

*CaptureUnit* contains the variables *currentCache*, *cacheSize* and *currentCacheUsage*. The *currentCache* variable represents the log file in our model, which works like a buffer; *currentCache* can store up to eight packets (based on the *cacheSize* in Figure 3). The eight captured packets are put together to form a single message; this represents a created block of data in our model. *CaptureUnit* computes the hash value of the formed message and stores the value in the *HashStore*; also, it passes the



1	2
1	Date
2	Tue Aug 11 09:14:15 2009 <Message source=132.143.132 destination=164.95.99.99 protocol="FTP">USER anonymous lrin 331 Guest login ok lrin PASV lrin 227 entering passive mode lrin RETR file.txt</Message>
3	
4	
5	Tue Aug 11 09:36:11 2009 <Message source=132.143.133.137 destination=164.95.99.176 protocol="SMTP">EHLO mail.live.com lrin 250-Welcome! Please send your message lrin MAIL FROM:<hacker1@badSMTP.com lrin TO: zombieNET@hostPC.org lrinlrin Commence the attack lrin RSET lrin 205flashed lrinQUIT lrin 221</Message>
6	
7	
8	
9	Tue Aug 11 09:52:24 2009 <Message source=132.143.133.120 destination=164.95.99.3 protocol="HTTP">GET / HTTP/1.0 lrin HOST: www.google.com lrin Date: Tue, 11 Aug 2009 09:52:24 lrin <?xml version="1.0" encoding "utf-8"> lrin<HTML xmlns="http://www.w3.org/1999/xhtml"><BODY><p>Welcome to google</p></BODY></HTML></Message>
10	
11	
12	
13	Tue Aug 11 10:01:56 2009 <Message source=132.143.133.5 destination=164.95.99.255 protocol="ARP">Who is 164.95.99.99 lrin</Message>
14	
15	Tue Aug 11 10:22:24 2009 <Message source=132.143.133.169 destination=164.95.99.115 protocol="HTTP">GET / HTTP/1.0 lrin HOST: www.illegalSite.com lrin Date: Tue, 11 Aug 2009 10:22:24 lrin <?xml version="1.0" encoding "utf-8"> lrin <HTML xmlns="http://www.w3.org/1999/xhtml"><BODY><p>Do not go here</p></BODY></HTML></Message>
16	
17	
18	
19	Tue Aug 11 10:39:12 2009 <Message source=132.143.133.12 destination=164.95.99.99 protocol="FTP">USER iDaniels lrin Password required lrin PASS 1675 lrin 230 iDaniels login ok lrinlrin 200 LS lrin 200 file.txt secrets.bat lrin 200 code.cpp lrin QUIT lrin 221 Goodbye</Message>
20	
21	
22	Tue Aug 11 10:50:23 2009 <Message source=132.143.133.115 destination=164.95.99.57 protocol="HTTP">GET / HTTP/1.0 lrin HOST: www.google.com lrin Date: Tue, 11 Aug 2009 10:50:23 lrin <?xml version="1.0" encoding "utf-8"> lrin <HTML xmlns="http://www.w3.org/1999/xhtml"><BODY><p>Welcome to google</p></BODY></HTML></Message>
23	
24	
25	
26	Tue Aug 11 11:11:21 2009 <Message source=132.143.133.159 destination=164.95.99.53 protocol="HTTP">GET / HTTP/1.0 lrin HOST: www.wikipedia.org lrin Date: Tue, 11 Aug 2009 11:11:21 lrin <HTML xmlns="http://www.w3.org/1999/xhtml"><BODY><p>Wikipedia your free online encyclopedia</p></BODY></HTML></Message>
27	
28	

Figure 4. Evidence store.

formed message to the *EvidenceStore* for storage. The variable *currentCacheUsage* keeps track of the number of times that *currentCache* was filled with the eight packets that are combined to form a single message.

Figure 4 presents sample data in *EvidenceStore*. The message in Row 2 shows that an anonymous user with IP address 132.143.133.122 is attempting to log into a remote host via FTP. The fact that this machine is anonymous could be of interest to a digital forensic investigator. The message in Row 5 contains data such as “Please send your message,” “hacker1@badSMTP.com” and “zombieNET@hostPC.org.” This data seems suspicious and constitutes potential digital evidence.

The message in Row 9 shows that a machine is using HTTP to access Google; this does not appear to indicate any malicious activity. The message in Row 13 shows that the machine with IP address X is asking the machine with IP address Y if it knows the machine with IP address Z; this does not appear to be malicious. However, if Machine Y responds to Machine X that it is not aware of Machine Z, then it is possible that Machine Z is not part of the network and could be an intruder who intends to sniff network traffic between Machines X and Y. The message in Row 15 shows that a machine with IP address 132.143.133.169 is accessing a suspicious website named “www.illegalSite.com;” an error message “Do not go here” pops up when this website is accessed. The message in Row 19 shows that a machine is providing its login details to a website and downloading a suspicious file named `secrets.bat`.

Figure 5 presents the *HashStore* corresponding to the captured simulated messages. Every time a message is captured, a copy of the original

	1	2
1	<b>Date</b>	<b>Hash</b>
2	Tue Aug 11 09:14:15 2009	?? ?Y@?W???@.Q?f□???
3	Tue Aug 11 09:52:24 2009	T?z?-?'?G□?□??□P?^??
4	Tue Aug 11 10:01:56 2009	□?t□??□?□?NA?? ??□
5	Tue Aug 11 10:22:24 2009	??#r?□??0??□?EO?□?E
6	Tue Aug 11 10:39:12 2009	□Bj□?g□?????□zE??
7	Tue Aug 11 11:11:21 2009	v□??z??h□Or?0.????□
8	Tue Aug 11 11:27:01 2009	?□?/???□?□xns??h????
9	Tue Aug 11 11:43:31 2009	??u□!gL?????i_?????
10	Tue Aug 11 11:56:18 2009	?????2?i?□??K?'??□
11	Tue Aug 11 09:38:48 2009	?D? ??#?(□??e□??L???

Figure 5. Hash store.

captured message is hashed and transferred to the *HashStore*. The main reason for hashing the captured information and keeping a separate copy of the original information is to verify the integrity of the captured information and to determine whether or not it was tampered with. The integrity of any message can be verified by extracting and computing the hash value ( $y$ ) of the message stored in the *EvidenceStore*. The hash value ( $y$ ) for the particular message block is then retrieved from the *HashStore*. If the hash values  $x$  and  $y$  match, the content of the original captured message was not tampered with and the integrity of the captured message in the *EvidenceStore* is verified. The integrity checking mechanism was built into the prototype because the integrity of evidence is a crucial requirement in any digital forensic investigation [2].

## 5. Discussion

In the simulation described in the preceding section, the simulated packets were logged (by *CaptureUnit*) and preserved (by *EvidenceStore* and *HashStore*). However, note that traffic monitoring was not implemented in the prototype because it is performed by the access point mainly for security reasons. After the traffic generated by the mobile devices that have connected to the WLAN has been captured and preserved, the data is ready for analysis in a digital forensic investigation. Because this data is forensically ready and forensically sound, the time and cost involved in conducting the digital forensic investigation are reduced considerably. In fact, the data needed for the investigation is readily available and the bulk of the digital forensic process (i.e., monitoring, logging and preservation) has been completed.

One disadvantage of the WFRM simulation is that the traffic is preserved in the *EvidenceStore* and *HashStore*, which potentially requires a large amount of storage space. This is not a serious problem be-



cause storage is becoming ever cheaper. Nevertheless, we are working on compression techniques that will facilitate the preservation of the entire stream of wireless network traffic. Since this might not be an optimal long-term solution to the problem, further research is needed to address the storage issue.

Finally, we note that the digital forensic processes for EnCase, FTK and WFRM (Table 1) are essentially equivalent. However, since our emphasis in this paper is the design of a readiness model, the practical implementation of the digital forensic process employed for WFRM is different from the conventional digital forensic process models for EnCase and FTK.

## 6. Conclusions

The wireless forensic readiness model helps address the twin challenges of intercepting and preserving all the communications generated by mobile devices in WLANs. In general, WLANs are not forensically prepared to gather digital evidence for use in ensuing investigations. The forensic readiness model focuses on the monitoring, logging and preservation of wireless network traffic. This covers the bulk of the general digital forensic investigation process, reducing both the time and the cost of forensic investigations.

Our future research will focus on several issues. One issue, as mentioned above, is the efficient storage of data in the hash store and evidence store. Another key issue is the analysis of potentially large amounts of data gathered as a result of the application of the wireless forensic readiness model. Other issues involve evidence management and the consideration of infrastructure requirements, admissibility requirements and retention requirements.

## References

- [1] J. Broadway, B. Turnbull and J. Slay, Improving the analysis of lawfully intercepted network packet data captured for forensic analysis, *Proceedings of the Third International Conference on Availability, Reliability and Security*, pp. 1361–1368, 2008.
- [2] E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, San Diego, California, 2002.
- [3] Coensys, AnyLogic 6: Multi-Paradigm Simulation Software, Cherry Hill, New Jersey ([www.coensys.com/anylogic.htm](http://www.coensys.com/anylogic.htm)).

- [4] B. Endicott-Popovsky, D. Frincke and C. Taylor, A theoretical framework for organizational network forensic readiness, *Journal of Computers*, vol. 2(3), pp. 1–11, 2007.
- [5] G. Francia and K. Clinton, Computer forensics laboratory and tools, *Journal of Computing Sciences in Colleges*, vol. 20(6), pp. 143–150, 2005.
- [6] R. Newman, *Computer Forensics: Evidence Collection and Management*, Auerbach Publications, Boca Raton, Florida, 2007.
- [7] R. Rowlingson, A ten step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), 2004.
- [8] K. Scarfone, D. Dicoi, M. Sexton and C. Tibbs, Guide to Securing Legacy IEEE 802.11 Wireless Networks, NIST Special Publication 800-48, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2008.
- [9] R. Siles, Wireless forensics: Tapping the air – Part one, Symantec Corporation, Mountain View, California ([www.securityfocus.com/infocus/1884](http://www.securityfocus.com/infocus/1884)), 2007.
- [10] J. Tan, Forensic readiness: Strategic thinking on incident response, presented at the *Second Annual CanSecWest Conference*, 2001.
- [11] C. Then, Examining wireless access points and associated devices, Forensic Focus ([www.forensicfocus.com/downloads/examining-wireless-access-points.pdf](http://www.forensicfocus.com/downloads/examining-wireless-access-points.pdf)), 2006.
- [12] B. Turnbull and J. Slay, The 802.11 technology gap – Case studies in crime, *Proceedings of the IEEE Region 10 Conference*, 2005.
- [13] B. Turnbull and J. Slay, Wireless forensic analysis tools for use in the electronic evidence collection process, *Proceedings of the Fortieth Annual Hawaii International Conference on Systems Sciences*, 2007.
- [14] B. Turnbull and J. Slay, Wi-Fi network signals as a source of digital evidence: Wireless network forensics, *Proceedings of the Third International Conference on Availability, Reliability and Security*, pp. 1355–1360, 2008.
- [15] E. Velasco, W. Chen, P. Ji and R. Hsieh, Wireless forensics: A new radio frequency based location system, *Proceedings of the Pacific-Asia Workshop on Cybercrime and Computer Forensics*, pp. 272–277, 2008.
- [16] D. Yim, J. Lim, S. Yun, S. Lim, O. Yi and J. Lim, The evidence collection of DoS attack in WLAN by using WLAN forensic profiling system, *Proceedings of the International Conference on Information Science and Security*, pp. 197–204, 2008.



## The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks

**Sipho Ngobeni**

(Council for Scientific and Industrial Research, Pretoria, South Africa  
sngobeni@csir.co.za)

**Hein Venter**

(University of Pretoria, Pretoria, South Africa  
hventer@cs.up.ac.za)

**Ivan Burke**

(Council for Scientific and Industrial Research, Pretoria, South Africa  
iburke@csir.co.za)

**Abstract:** Over the past decade, wireless mobile communication technology based on the IEEE 802.11 Wireless Local Area Networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cybercrime. WLAN digital forensics is seen as not only a response to cybercrime in wireless networks, but also a means to stem the increase of cybercrime in WLANs. The challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation. This paper attempts to address this issue by proposing a wireless digital forensic readiness model designed to monitor, log and preserve wireless network traffic for digital forensic investigations. Thus, the information needed by the digital forensic experts is rendered readily available, should it be necessary to conduct a digital forensic investigation. The availability of this digital information can maximise the chances of using it as digital evidence and it reduces the cost of conducting the entire digital forensic investigation process.

**Keywords:** Wireless Local Area Network, Digital Forensics, Digital Forensic Readiness, Access Point, Digital Forensic Process, Cyber Forensic Experts, Hash Value, Digital Evidence, Traffic.

**Categories:** H.3.1, H.3.2, H.3.3, H.3.7, H.5.1

### 1 Introduction

Wireless technologies have become immensely popular around the world. Wireless Local Area Networks or “hotspots” blanket public places such as convention centres, airports, schools, hospitals, railway stations, coffee shops and other locations to provide seamless public access to the Internet [Velasco, 08]. These hotspots provide several advantages over hard-wired networks, including user mobility and flexible Internet access. However, due to their open nature, WLANs have become a major target for a massive quantity of security attacks [Nguyen, 08].

WLAN digital forensics involves the application of methodologies and tools to intercept and analyse wireless network events for presentation as digital evidence in a



court of law [Siles, 10]. As such, WLAN digital forensics is complementary to intrusion prevention; whenever such prevention fails, WLAN digital forensics is useful for obtaining information about the intrusion. However, the primary challenge in WLAN digital forensics is to acquire all the digital evidence related to any potential crime such as Denial of Service (DoS) attacks, man-in-the-middle attack, session hijacking, attack against the WEP and may others [Newman, 07]. This challenge arises from the fact that the devices participating in a WLAN environment are mobile. Furthermore, since the devices are not always connected to the network, it is difficult to attribute a criminal activity to a particular device.

This paper proposes a wireless digital forensic readiness model for monitoring, logging and preserving wireless network traffic for digital forensic investigations. The proposed model builds on the work of Rowlingson [Rowlingson, 04] with regard to traditional digital forensic investigations. A prototype implementation of the proposed model is presented as a proof of concept.

The remainder of this paper is structured as follows: Sections 2, 3 and 4 present the background information on WLANs, digital forensics and digital forensic readiness respectively. The paper then proceeds to present the proposed Wireless Digital Forensic Readiness Model (WDFRM) and its related components in Section 5. A prototype implementation of the readiness model is presented in Section 6 as a proof of concept. A general discussion of the advantages and disadvantages of the proposed model and legal issues pertaining to WLAN traffic monitoring is presented in Section 7, while Section 8 concludes the paper and discusses future research work.

## **2 Wireless Local Area Networks**

The IEEE 802.11 specification defines two types of WLANs: the ad-hoc mode and infrastructure mode. The ad-hoc mode is characterised by the lack of access point (AP), where stations communicate with one another in a peer-to-peer fashion. This type of configuration is termed Independent Basic Service Set (IBSS). An IBSS is a short-lived network with a small number of stations created for exchanging data with a vendor in a lobby of the company's building [Ilyas, 05]. On the other hand, the infrastructure mode of WLAN comprises an access point through which all communications from the mobile clients go. The infrastructure mode is the key focus of this study.

In an infrastructure network, all mobile stations communicate with the access point, which logically connects the mobile stations to the wired LAN [Yang, 05]. In general, the access point is analogous to a base station in cellular phone networks. A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS) and is depicted in Figure 1.

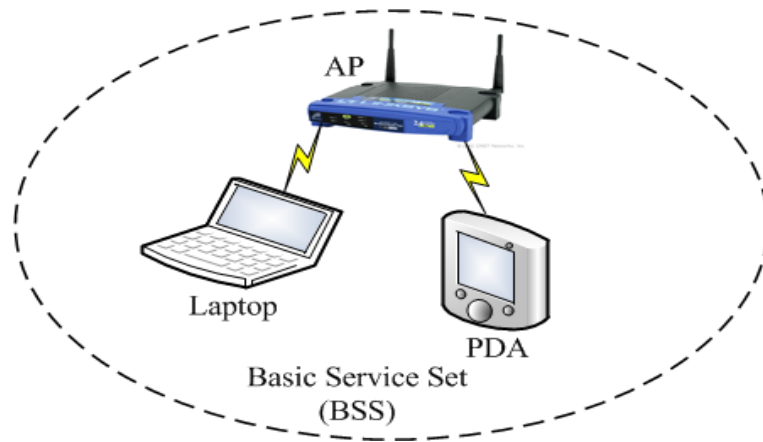


Figure 1: Basic Service Set

When more than one access point is connected to the network to form a single sub-network, it is called an Extended Service Set (ESS). An ESS is a collection of BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The AP performs all the communications through an abstract layer called the Distribution System (DS). The DS enables mobile station support in a WLAN by providing the logical services that are necessary to perform address-to-destination mapping and seamless integration of multiple BSSs [Mullet, 06]. Figure 2 contains a diagrammatical illustration of an ESS.

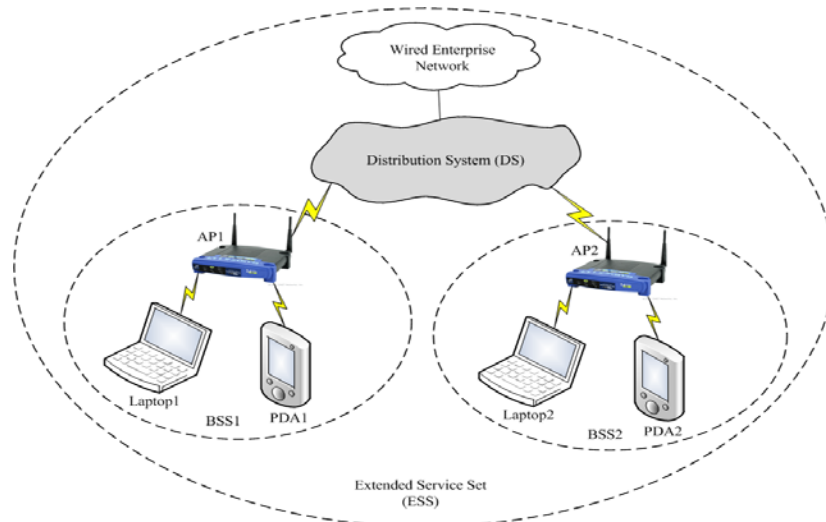


Figure 2: Extended Service Set

Having discussed the basic components that constitute a WLAN, the next section presents background information on digital forensics and the related digital forensic process.

### 3 Digital Forensics

Digital forensics is defined as a scientifically proven method for the investigation of computers and other digital devices believed to be involved in criminal activities [Francia, 05]. A digital forensic investigation should follow proper digital forensic procedures or process models for its evidence to be admissible in a court of law. However, to date, there is no standardised or consistent digital forensic investigation process model. In this section, the authors compare and contrast three particular digital forensic investigation process models, and finally deduce a process model suitable for the proposed wireless digital forensic readiness model.

A number of scholars have attempted to create rudimentary digital forensic process models. For example, the Digital Forensic Research Workshop (DFRW) is one of the significant participants in taking an initiative to develop a digital forensic process model [DFRW, 01]. Their process model includes the steps as listed in Table 1. The most challenge about this process model is that, analytical procedures and protocols are not standardised nor do practitioners and researchers use standard terminology [Reith, 2002].

The US Department of Justice (DOJ) also made an attempt to propose a digital forensic process model, where their steps are listed in Table 1. The significant challenge about this process model is that, the US DOJ does not make a distinction between digital forensics applied to computers or other electronic devices. Instead, it attempts to build a generalised process model that will be applicable to most electronic devices [US DOJ, 2001].

Lastly, Mandia et al also made an attempt to define a viable digital forensic process model as listed in Table 1 [Mandia, 2003]. They refer to their process model as incident response methodology. The key challenge about this methodology is that, it only focuses on computer crime and does not address the digital forensic process in terms of other digital devices such as personal digital assistant, smart appliances and other future electronic devices.

Despite the fact that several digital forensic process models exist (as indicated above), consensus has not yet been reached about a single, standardised digital forensic process model that can be adopted internationally. Table 1 summarises the phases of the three digital forensic process models mentioned above and deduce a process model applicable to the WDFRM.

From Table 1, one should be able to note that the logging, analysis, and reporting phases of the WDFRM directly correlate with that of the DFRW, US DOJ and Mandia et al. However, the logging phase of the WDFRM can be viewed as the collection phase in the other three process models. This is because logging wireless network traffic can also be viewed as data collection. The preservation phase of the WDFRM only correlates with that of the DFRW process model. The monitoring phase of the WDFRM does not directly correlate with the other three process models. In a bid to try and align the process models into a process model that would suit our

WDFRM, the phases of the WDFRM were deduced from those process models as indicated in Table 1.

<b>Digital Forensic Process Models</b>			
<b>DFRW</b>	<b>US DOJ</b>	<b>Mandia et al</b>	<b>WDFRM</b>
1. Identification	1. Collection	1. Pre-incident preparation	1. Monitoring
2. Preservation	2. Examination	2. Detection of incident	2. Logging
3. Collection	3. Analysis	3. Initial response	3. Preservation
4. Examination	4. Reporting	4. Formulate response strategy	4. Analysis
5. Analysis		5. Investigate the incident (data collection and analysis)	5. Reporting
6. Presentation		6. Reporting	
7. Decision		7. Resolution, recovery and implement security measures	

*Table 1: A comparison of the digital forensic process models*

It should be noted that coming up with the process model as depicted in the WDFRM is not the main focus of this paper. The main focus is rather on building digital forensic readiness into a process model that would be fit for a wireless LAN environment, in order for a digital forensic readiness model to be incorporated.

Having defined digital forensics, compared and contrasted various digital forensic process models with our deduced WDFRM, the next section presents digital forensic readiness.

#### **4 Digital Forensic Readiness**

The goal of this section is to show, through a digital forensic expert's opinion, that it is costly to conduct a digital forensic investigation within an organisation that is not forensically ready. We investigated as to how much it would cost to log wireless traffic in a public WLAN environment consisting of an IEEE 802.11g Access Point (AP) and clients connected to it. We first present an overview of digital forensic readiness, followed by a discussion on the performance and characteristics of 802.11g products. The calculation of the average data rate of the 802.11g products is also presented.

#### 4.1 Overview of Digital Forensics Readiness

The purpose of digital forensic readiness is to reduce the effort involved in performing a digital forensic investigation. This is done by taking the necessary prior steps to be ready for any investigation, while maintaining the level of credibility of the digital evidence that is collected [Endicott-Popovsky, 02]. The decrease in effort is the result of the WLAN being in a state of readiness, which reduces the time and cost involved in incident response. An organisation that is ready in terms of digital forensics can respond to an attack rapidly and efficiently. In general, reducing the time involved in incident response can greatly reduce the cost of the entire digital forensic investigation.

Tan [Tan, 01] discusses an incident in which it took the intruder approximately two hours to launch an attack, but the digital forensic experts required almost 40 billable hours to respond to the incident. Their response took so long because the attacked organisation had not been digital forensically prepared for the incident.

#### 4.2 IEEE 802.11g Performance and Characteristics

Table 2 shows a comparison of maximum data rate, modulation, data rate, and frequencies of different IEEE 802.11 specifications [WLAN, 03].

Specifications	802.11.a	802.11b	802.11g
Maximum data rate	54Mbps	11Mbps	54Mbps
Modulation	OFDM	DSSS	OFDM and DSSS
Data rate	6,9,12,18,24,36,48,54 Mbps	1,2,5.5,11 Mbps	DSSS:1,2,5.5,11 OFDM:6,9,12,18,24,36,48,54 Mbps
Frequencies	5GHz	2.4GHz	2.4GHz

Table 2: IEEE 802.11 specifications

Theoretically, the data rate of an 802.11g AP is 54Mbps, however, practically, we assume an average data rate of 24Mbps is achievable due to factors such as interference and collision, as well as the fact that the AP is not always utilised 100% [WLAN, 03]. Of course, this data would be achievable if the AP's associated clients are also 802.11g products, also taking into consideration the range between the AP and its associated clients.

#### 4.3 Average Data Rate of an IEEE 802.11g AP

Now that we know an 802.11g network would have an average data rate of 24 Megabits per second (Mbps), we can then calculate the average data rate it would produce in 8 hours in order to simulate a common business day). We first find the average data rate (ADR) an AP would produce in one minute.

ADR per minute = 24 Mbps \* 60"  
ADR per minute = 1440 / 8 bits  
ADR per minute = 180 Mega Bytes (MB)

The ADR of an AP per minute is 180 MB. Now that we know the ADR produced by the AP per minute, we can calculate the ADR of the AP per hour as follows:

ADR per hour = 180 MB \* 60'  
ADR per hour = 10800 MB ~ 10.8 Gigabytes (GB)

The ADR of an AP per hour is 10.8 GB. To calculate the ADR per day (which in our case is 8 hours), we multiply 10800 MB by 8, which is as follows:

ADR per day = 10800MB \* 8hr  
ADR per day = 86400 MB ~ 86.2 GB

If a particular public WLAN, e.g. a shopping mall, has five 802.11g APs where clients can connect to them, then, the whole network would generate an average data rate of 431 GB per day. It should be noted that this value is very optimistic in the sense that we doubt that so much data will be generated over the said period, yet we need to cater for such scenarios. The average data rate may vary depending on the factors such as the number of clients associated with each AP, the range between an AP and the clients, and other factors.

#### 4.4 Expert opinion

To show that a digital forensically ready organisation would minimise effort and save cost as Tan suggests [Tan, 01], we then requested Risk Diversion [Risk Diversion, 2012] to quote us how much will it cost to log such wireless traffic in a public wireless LAN environment with five 802.11g APs, assuming they have the necessary legal clearance to do so. Risk Diversion is a (Pty) Ltd company specialising in information security audits as well as computer, cell phone, and network forensic investigation and analysis. According to Risk Diversion, logging wireless traffic in an 802.11g network with five AP for 8 hours would cost about \$2000 when hiring a full forensic team.

This shows that if an organisation were to log wireless traffic and store it in a forensically ready manner, say for five days, it would save them up to \$10000 compared to hiring a full forensic team. Rather, it would cost the organisation approximately 2TB of storage in order to store all the data, boiling down to about \$100 in cost. Even if data needs to be retained for a full year, the storage cost would amount to significantly less. All that would be required is to have a reliable RAID system with a few drives that would be able to accumulate data for about a week, after which the data can be written to tape drives and securely stored for periods as long as required by particular retention policies and laws. Therefore, this cost is much cheaper than carrying out a fully-fledged digital forensic investigation. The point we want to make is simply that it would be cheaper and it would be a once-off expenditure.

Organisations deploying WLANs that are at a high risk of cyber-attacks should be ready to collect digital evidence before an incident occurs. The model presented in the next section addresses the concept of digital forensic readiness in WLANs.

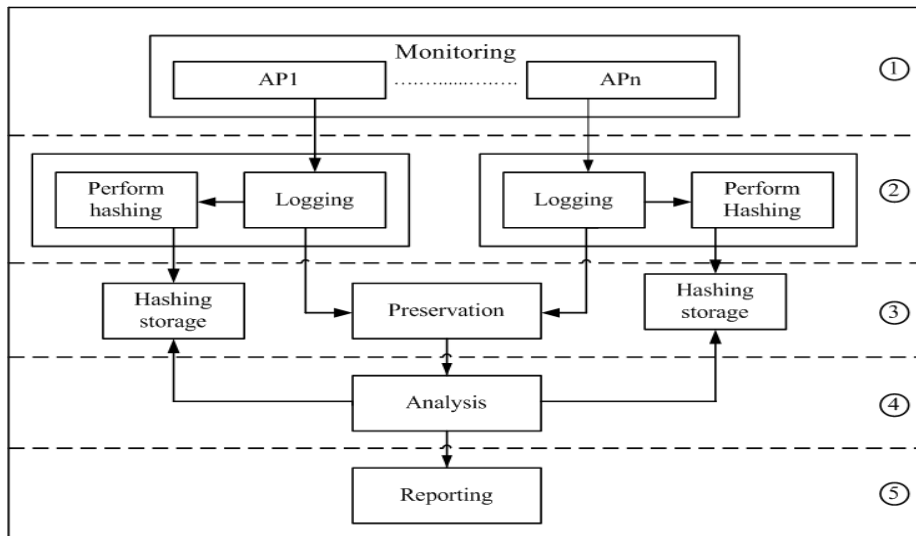
## 5 Wireless Digital Forensic Readiness Model

This section starts by presenting an overview of the proposed Wireless Digital Forensic Readiness Model (WDFRM) in the form of a block diagram. The components of the model are discussed separately, followed by a discussion of the model as an integrated whole.

### 5.1 Overview of the WDFRM

The principal concept addressed by the WDFRM is that it monitors wireless network traffic from various access points (APs). The monitored traffic is logged in a log file and then preserved to maintain its integrity. The information needed by cyber forensic experts is therefore readily available should it become necessary to conduct a digital forensic investigation.

The mere fact that this digital information is now available maximises the chances of it being used as evidence and reduces the cost of conducting an entire digital forensic investigation. This is simply because a large part of the digital forensic process (i.e. the monitoring, logging and preservation) has now already been conducted. Figure 3 indicates in a block diagram how the components of the WDFRM interact with one another.



*Figure 3: A block diagram of the WDFRM*

The circled numbers 1 to 5 on the right-hand side of the block diagram in Figure 3 represent the phases or components of the digital forensic process of the WDFRM as indicated in Table 1. Thus, 1 represents the monitoring phase, 2 represents the logging phase, 3 represents the preservation phase, 4 represents the analysis phase and 5 represents the reporting phase.

## 5.2 Components of the WDFRM

This section discusses each of the five components of the Wireless Digital Forensic Readiness Model separately in its own subsection. As indicated in Table 1, the components are monitoring, logging, preservation, analysis and reporting.

The shaded area in each of the block diagrams below (from Figure 4 up to Figure 8) indicates the component that is described in more detail in the particular subsection.

### 5.2.1 Traffic Monitoring

Figure 4 demonstrates the traffic monitoring component whereby Mobile Devices (MDs) are associated to a WLAN through various access points (APs). This can be denoted as  $AP_i = \{AP_1, AP_2, AP_3, \dots, AP_n\}$ , where  $AP_i$  denotes a set of APs from  $AP_1$  up to  $AP_n$ . In general, there can be many APs in a single WLAN environment. Each AP monitors all the traffic generated by the MDs that are connected to that particular AP.

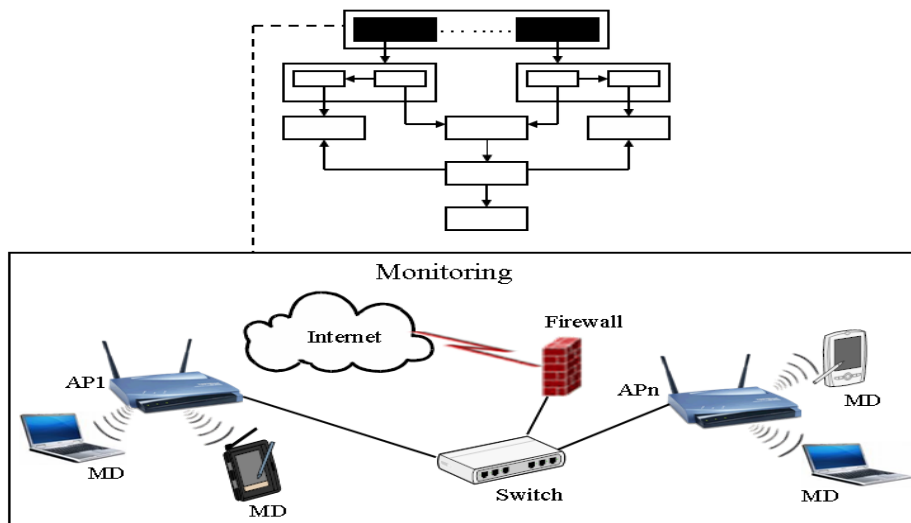


Figure 4: Traffic monitoring component

For security purposes, the monitoring component uses a firewall to filter both inbound and outbound wireless traffic. Filtering is defined as the process of controlling access to the WLAN by examining all the packets based on the content of their headers. However, a firewall cannot detect all the misconduct in a WLAN since

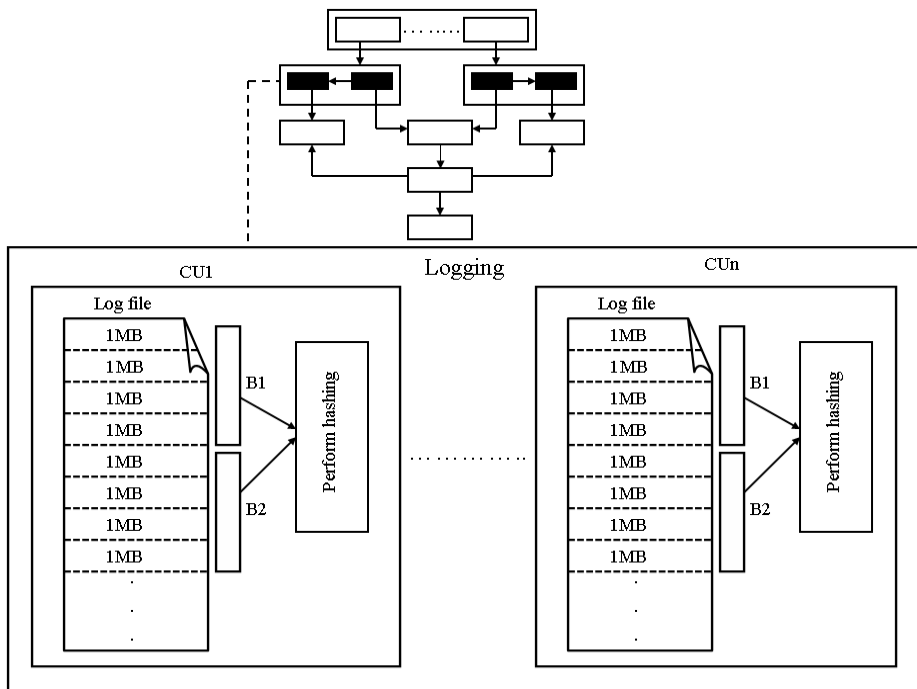


some MDs may obscure their identities and will appear as if they are legitimate users of the network. For this reason our proposed model employs a component called the Capture Unit (CU) that records or logs all the monitored traffic. The CU is discussed in detail in the next subsection.

### 5.2.2 Logging

The CU logs all the traffic monitored by the different APs in order to gather potential evidence. Each AP has its own associated CU that logs the traffic passing through that AP. The CU logs the traffic in a log file as indicated in Figure 5. The log file is divided into separate storage areas with each storage area consisting of, for example, 1 Megabyte (4 MB) of data. As traffic through the AP is monitored and stored in a log file, the storage area of the log file becomes satiated. Therefore, the CU creates a block of data of several MBs, for instance B1 in Figure 5 represents a block of data consisting of 4 MBs. A block is a fixed-size unit of data that is transferred as a whole to a permanent storage area (see Section 5.2.3).

For the purpose of our model, the logged traffic is the packets. Therefore, whenever this paper refers to ‘traffic’, it means all the packets passing through the APs. Finally, the CU sends the accumulated blocks of data to the Evidence Store (ES) for analysis purposes and creates a hash value for each block of data that is sent to the hashing storage area for the purpose of preserving evidence (see Section 5.2.3).



*Figure 5: Logging component*

### 5.2.3 Preservation

The primary goal of evidence preservation in WLANs is to ensure that absolutely no changes are made to the logged data once it has been collected [Endicott-Popovsky, 02]. Figure 6 demonstrates how the log files are preserved in the proposed model. The Evidence Server (ES) stores all the blocks of data received from various CUs. In general, the ES acts as a central storage area for all the data monitored by the APs. The ES logs the blocks of data in chronological order. These blocks of data are stored according to the AP from which the traffic was monitored. For example, in the ES, B1AP1 means that block 1 represents the first block of traffic monitored from the first AP, whereas B1APn means that block 1 represents the first block of the traffic monitored from the n<sup>th</sup> AP.

It is worth noting that the data stored in the ES is needed for analysis purposes only. Analysis of this data will only take place if a particular incident has been reported on the WLAN, which then needs to be investigated.

The hash values of the blocks of data created in the ‘perform hashing’ subcomponent within the CU is transferred to the hashing storage areas represented as “HS of AP1” (Hashing Storage of AP1) and “HS of APn” (Hashing Storage of the n<sup>th</sup> AP) (see Figure 6). There is a hashing storage area for each AP on the WLAN. The H(B1AP1) in HS of AP1 shown in Figure 6 represents the hash value of the first block from the first AP, and H(B1APn) in HS of APn represents the hash value of the first block, from the n<sup>th</sup> AP and so on.

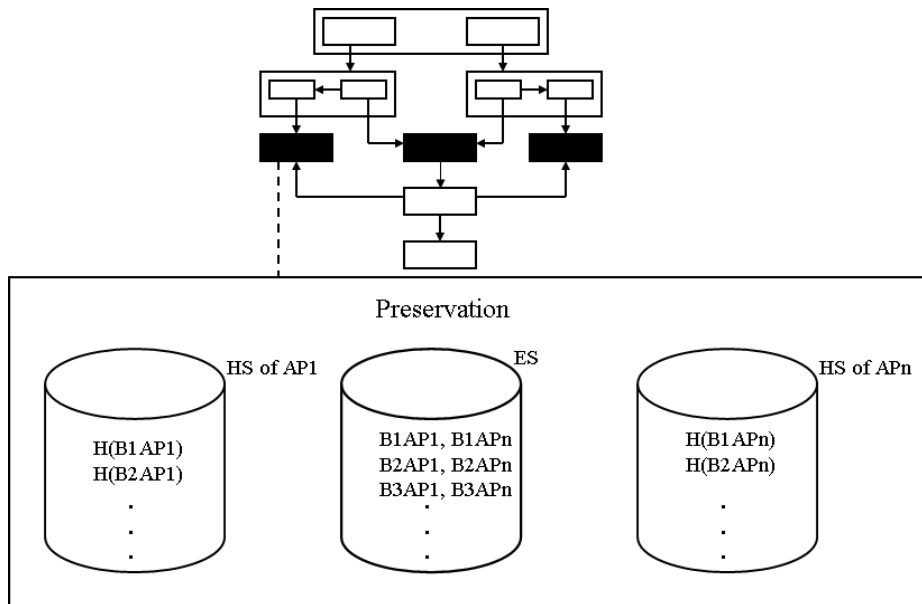


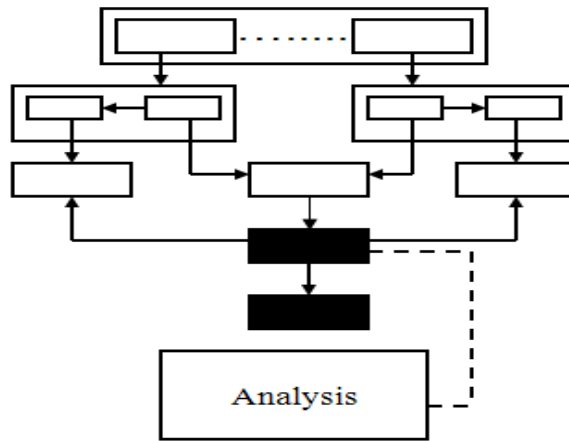
Figure 6: Preservation component

Our proposed model adopts the MD5 and SHA-1 hashing techniques. Hashing is described as a mathematical function that creates a unique fixed-length string from a

message of any length [Endicott-Popovsky, 02]. The result of a hash function is a hash value, sometimes called a message digest. It is worth noting that the hashed blocks of data will only be used to check that the logged data on the ES has not been altered during the course of a digital forensic investigation. Preserving the integrity of digital evidence is an absolute requirement of the digital forensic process [Casey, 02].

**5.2.4 Analysis**

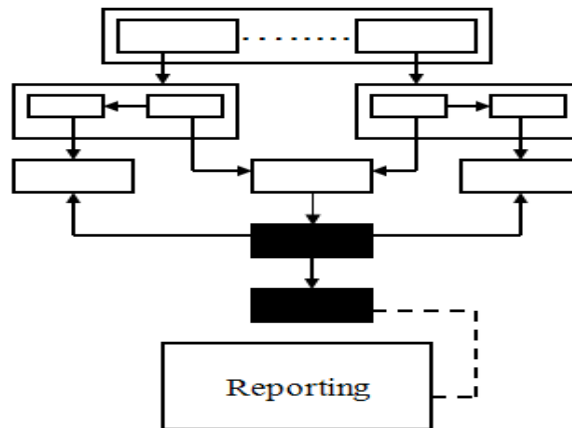
The main purpose of the analysis phase of the WDFRM is to mine and extract the data from the ES in an attempt to come up with evidence that can associate a particular adversary with a criminal activity committed on the WLAN. This process is represented in Figure 7. Although it is not within the scope of this study to discuss data mining in detail, the use of data-mining techniques should not be overlooked during the process of conducting a digital forensic investigation. The analysed data is next passed on to the reporting phase.



*Figure 7: Analysis component*

**5.2.5 Reporting**

During the reporting phase, the final evidence is prepared for the entire digital forensic investigation. The data is used by cyber forensic experts when they testify in a court of law that an intruder should be found guilty due to the evidence that they have gathered in their digital forensic investigation. The prosecutor in a court of law has to decide whether the intruder is guilty or not, based on the evidence presented by the cyber forensic experts concerned. Figure 8 indicates the reporting phase.



*Figure 8: Reporting component*

### 5.3 The WDFRM as an integrated whole

In this section the components discussed in the previous section are integrated. The WDFRM is depicted with all its components/phases as explained in the preceding section. Figure 9 shows how wireless traffic is monitored in the WLAN, how the monitored traffic is logged, how the digital evidence is preserved and how it is stored for analysis purposes so as to render information that is forensically ready to be used by digital forensic experts.

Figure 9 shows all the components of the WDFRM, with circled numbers 1 to 5 representing the five phases or components of the digital forensic process. Four mobile devices (MDs) and two access points (APs) are involved in the monitoring component. Two of the MDs are connected to each of the APs. These MDs probably have Internet access in a particular hotspot. In terms of the WDFRM our study assumes that a particular device is deployed closer to the WLAN. This device has a number of capabilities – i.e. monitoring wireless traffic, logging the monitored traffic, preserving the traffic, and analysing the traffic. The component that does the logging receives all the monitored wireless traffic from an AP and stores the data in a log file. The log file is divided into separate storage areas of, say, 4 MB. The reason for choosing the 4 MB storage capacity is that, larger file sizes will reduce the number of records in the database (DB) which means during reconstruction, fewer records need to be extracted from the DB. However, devices have a limited file storage space. Larger data files mean there will be less transmission to the server. As the log file accumulates data, every fourth block, for example, is merged as a block of data. These blocks are then transferred to the Evidence Server (ES), which constitutes the preservation component. Our study also assumes that the ES is a sufficiently large mass storage device. The hash values of each of these blocks are next created and transferred to the hashing storage area. In this way the integrity of the data that flows through the WLAN is preserved.

Let us assume that an incident is being reported on the WLAN. Responding to the reported incident will not require much effort because the digital data is already

forensically ready. The cyber forensic experts will simply extract the data from the ES and do the necessary analysis. The integrity of the analysed data can be proven beyond any doubt by creating hash values of each block from which the evidence was extracted, and matching those with the original hash values of each block as stored in the hashing storage. If the hash values match, it proves that the extracted digital evidence was in fact the original evidence, thus proving that the original evidence was not altered or tampered with.

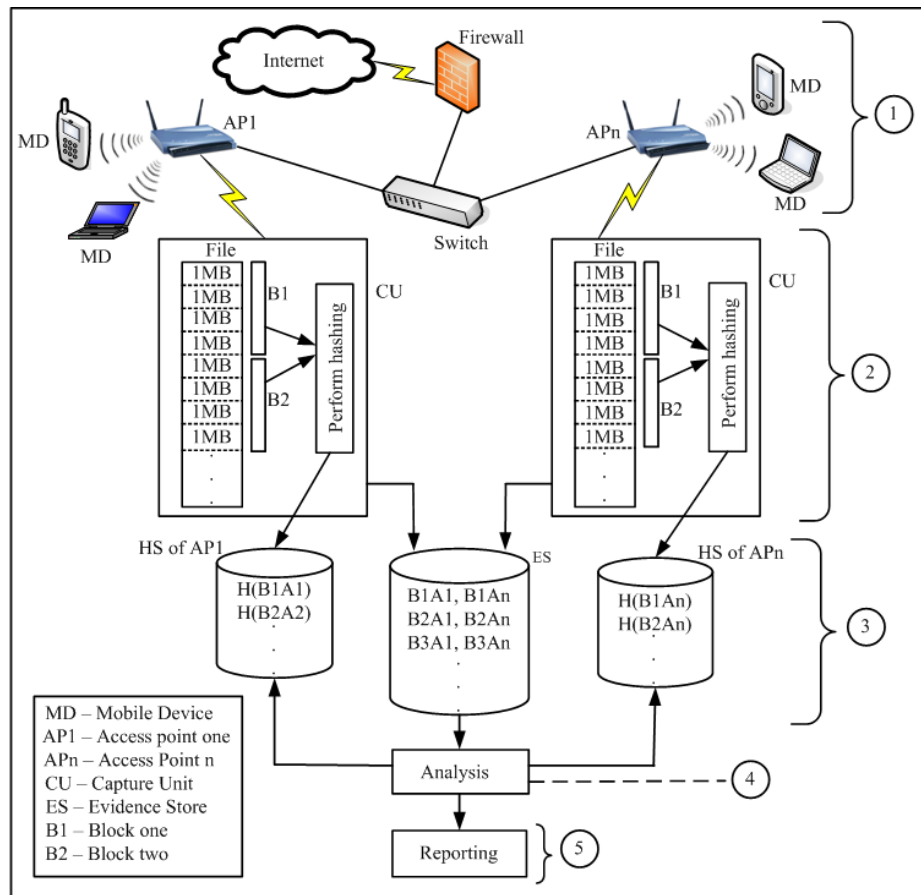


Figure 9: The Wireless Digital Forensic Readiness Model

This section introduced the WDFRM in the form of a block diagram. The components of the WDFRM were initially presented separately, after which the proposed model, in which all the components were combined, was discussed. The next section presents a prototype of the WDFRM as a proof of concept.

## 6 WDFRM Prototype

This section presents the prototype of the WDFRM. It first gives an overview of the development environment and why the prototype was developed. The section proceeds to present the prototype development in detail.

### 6.1 Overview of the Prototype

The WDFRM prototype was developed using Code::Blocks (version 10.06), which is an open source, cross platform, and free C++ Integrated Development Environment (IDE). Though it was designed for the C++ programming language, it uses plugins that enables it to support many other programming languages (Code::Blocks, 11). The prototype is developed to validate the use of the WDFRM for implementing digital forensic readiness in a WLAN environment.

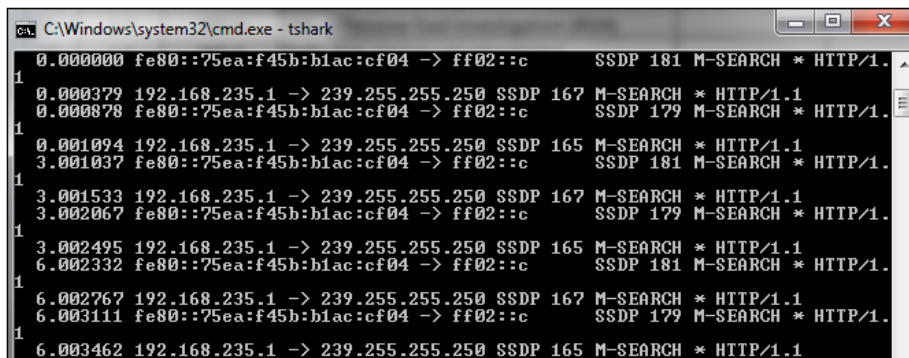
### 6.2 Prototype Development

This section discusses how the live wireless network traffic was captured and stored in a forensically sound manner.

#### 6.2.1 Tshark

The prototype uses Tshark [Tshark, 10] to capture raw packets as they traverse the live wireless network. This includes the source and destination address, source and destination ports, protocol used, packet size, as well as the message header of every packet. Figure 10 shows a sample Tshark dump in console. The general format of the Tshark output as extracted from line 2 of Figure 10 is explained as follows:

[TimeStamp: 0.00037] [MAC Sender: fe80::75ea:f45b:b1ac:cf04] [MAC Receiver: ff02::c] [Protocol: SSDP] [Size: 167] [TCP Message Header: M-SEARCH \* HTTP/1]. It should be noted that though the source and destination address appears in Figure 10 they can be resolved to MAC addresses.



```

C:\Windows\system32\cmd.exe - tshark
0.000000 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.1
1
0.000379 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
0.000878 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.1
1
0.001094 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
3.001037 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.1
1
3.001533 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
3.002067 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.1
1
3.002495 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
6.002332 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.1
1
6.002767 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
6.003111 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.1
1
6.003462 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1

```

Figure 10: Sample Tshark dump in console



## 6.2.2 Pcap File

The Tshark output is written to a Pcap file. A Pcap file is a data file created by Tshark containing packet data created during a live network capture [Pcap, 12]. The Pcap file is set to have a maximum storage capacity of 4 MB (as specified by the model), by using the -a flag provided by Tshark. Once the Pcap file is filled with the 4 MB of traffic, Tshark stops writing into the current Pcap file and create a new file to be written to. Figure 11 shows a sample Pcap file opened in Wireshark [Wireshark, 12].

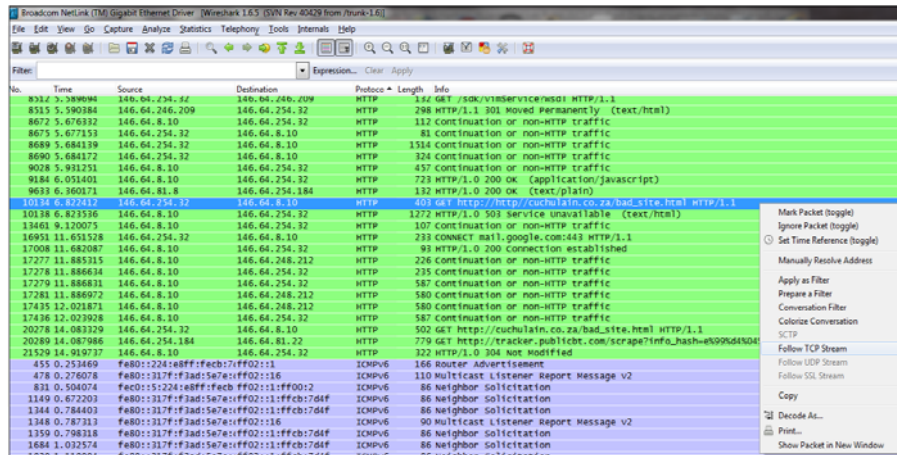


Figure 11: Sample Pcap file opened in Wireshark

The reason for using Wireshark to open the Pcap file is to reproduce the raw packet in the Pcap file into a more readable format. For example, the information about each packet, that is, the source and destination address, port address, packet size and message header is reconstructed into a more meaningful way compared to the example in Figure 10.

It should be noted that, by following the Transmission Control Protocol (TCP) stream, one can uncover whom requested which site in the network and what content the server returned. Figure 12 shows TCP stream content as a result of right-clicking on the contents of the packets in Figure 11 and choosing the option “Follow TCP Stream”.

The red text in Figure 12 represents a client's request to an apache server indicated in blue text. The user makes an http GET request to the apache server. The server is located on the remote host www.cuchulani.co.za. In this example, the client uses a Firefox web browser as can be seen by referring to the user-agent string in Figure 12. The server sends an http acknowledgement with “200 Ok” meaning that it has received the client's request. All this information might be used as digital evidence to show that the particular client in this example did receive a certain request, should there be a need for such a digital forensic investigation. Similarly, any other digital evidence of potential investigative value can be extracted in this way.

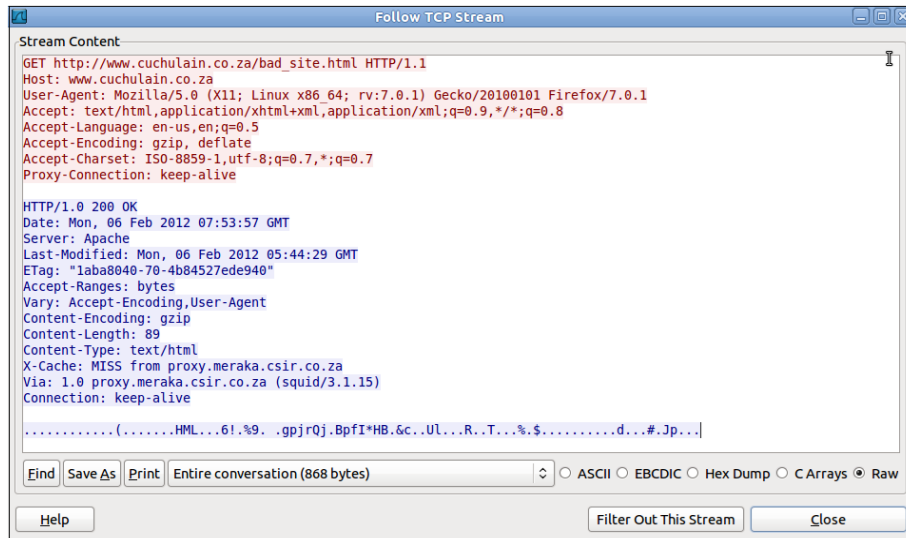


Figure 12: Follow TCP stream

### 6.2.3 The TCP Dump Log Table

The filled Pcap file is sent to a storage database called “TCP dump log table” through the network in a separate channel to prevent collision and duplication of data captured by the Tshark application. Figure 13 depicts the TCP dump log table with packets as they were captured from the live wireless network. It should be noted that this data will only be used for analysis purposes if an incident has been reported and a digital forensic investigation is required. The data in Figure 13 represents the same data as stored in the ES in Figure 9.









	ID	Timestamp	Raw Dump	SensorID
 	0	2012-02-01 14:53:17	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor
   	1	2012-02-02 15:35:43	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor
 	2	2012-02-03 01:53:17	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor

Figure 13: TCP dump log table

### 6.2.4 Hash Table with Both MD5 and SHA-1 Hashes of all TCP Dumps

The prototype also takes the same filled Pcap file of 1MB and creates MD5 and SHA-1 hash of it and saves the hash values in database called “Hash Table”. Figure 14 depicts the hashing storage with hash values of the Pcap file. It should be noted that this is done to preserve the integrity of the captured wireless traffic. To verify the integrity of the data in the “TCP dump log table”, we create MD5 and SHA-1 hashes of the data stored in the “TCP dump log table”. If the output stream is the same as that of the hashes stored in the corresponding “Hash Table” entry, then it shows the data



in the “TCP dump log table” was not tampered with. The data in Figure 14 represents the same data as stored in the HS in Figure 9.

	ID	Timestamp	MD5	SHA-1	SensorID
Bearbeiten  Direkt bearbeiten  Kopieren  Löschen	0	2012-02-01 14:53:19	f06fcb5bb5a31c19021cbe24bb264187	864d29dc58c0499238adb35dd9668f707b9fef8	CSIRSenSor
Bearbeiten  Direkt bearbeiten  Kopieren  Löschen	1	2012-02-02 15:35:45	ee08a276eb74bcb0ea115a210d73f0c	66c7e5e32b0bc3eae2470c3b941fc6f4c0f9c8ed	CSIRSensor
Bearbeiten  Direkt bearbeiten  Kopieren  Löschen	2	2012-02-03 01:53:13	a4534d0b3928b4ab7d10c4c48aa5f04	1f4b769515c53d660a48ad4f0a8b5c0e2aa1c983	CSIRSensor

Figure 14: Hash table of TCP dumps

While this section discussed the prototype development of the WDFRM to prove its viability for implementing forensic readiness in WLAN, the next section discusses pros and cons of the proposed model with regards to traffic monitoring.

## 7 Advantages and disadvantages of the WDFRM and legal issues pertaining to WLAN traffic monitoring

This section discusses the WDFRM by outlining its advantages and disadvantages. It then proceeds to a discussion of traffic-monitoring issues in a WLAN environment.

Once the traffic generated by the mobile devices that connect to a WLAN has been monitored and preserved, the data concerned is ready to be analysed and used by cyber forensic experts to conduct the actual digital forensic investigation. Seeing that this information is digitally ready and forensically sound, the cyber experts’ time and thus the cost of conducting the entire digital forensic investigation is considerably minimised. In fact, the information needed for the investigation has been made readily available and the first phases of the digital forensic process, i.e. the monitoring, logging and preservation, have been completed. A disadvantage of the WDFRM, however, may be the fact that the traffic monitored from the APs and captured by the CUs requires a large amount of storage, and this may prove to be expensive. However, we are not too concerned about this disadvantage since storage space becomes ever cheaper. Nevertheless, the authors are working on introducing compression on the WDFRM as a mechanism to minimise the amount of storage area required to log the entire stream of traffic that passes through the WLAN.

It was mentioned earlier that one of the functions of the WDFRM is to monitor wireless network traffic. Traffic monitoring may also be referred to as interception of communication as presented in the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICCA). Although the RICCA Act, Act No. 70 of 2002 [RICCA, 02], prohibits the interception of communication, section 6(2)(bb) makes provision for a person to intercept communication for the purpose of investigating or detecting unauthorised use of that communication system. Section 5(2)(a) states that the interception of communication may only take place if the entity that does the interception has received prior consent in writing from the applicable law enforcement authorities.

## 8 Conclusions

The proposed Wireless Digital Forensic Readiness Model helps address the twin challenges of intercepting and preserving all the communication generated by mobile devices in WLANs. In general, WLANs are not digital forensically prepared or equipped to gather digital evidence for use in ensuing digital forensic investigations. Our digital forensic readiness model therefore focuses on the monitoring, logging and preservation of wireless network traffic, as this covers the bulk of most digital forensic investigations. A prototype implementation of this model was presented as a proof of concept.

## 9 Future Work

Future research will focus on analysis of potentially large amounts of data gathered as a result of the application of the Wireless Digital Forensic Readiness Model (key issue). Other issues involve digital evidence management and the consideration of requirements in respect of infrastructure as well as the admissibility and retention of digital evidence.

### Acknowledgements

This work was funded by the Council for Scientific and Industrial Research (CSIR) and University of Pretoria, South Africa. Special thanks goes to Prof. Hein Venter (University of Pretoria) and Ivan Burke (CSIR) for their continuous support and significant contribution towards the success of this work.

## References

- [Casey, 02] Casey, E.: Handbook of Computer Crime Investigation, Forensic Tools and Technology, Academic Press, San Diego, California, 29 January 2002.
- [Cohen, 10] Cohen, F.B.: Fundamentals of Digital Evidence, 2007.
- [Endicott-Popovsky, 02] Endicott-Popovsky, B., Frincke, D., Taylor, C.: A theoretical framework for organizational network forensic readiness, Journal of Computers, Vol. 2(3), May 2007, 1-11.
- [Francia, 05] Francia, G., Clinton, K.: Computer forensics laboratory and tools, Journal of Computing Sciences in Colleges, Vol. 20(6), June 2005, 143-150.
- [Ilyas, 05] Ilyas, M., Ahson, S.: Handbook of Wireless Local Area Networks, Applications, Technology, Security and Standards, Taylor and Francis Publication 2005, Boca Raton, Florida, USA, 25 May 2005.
- [Mullet, 06] Mullet, G.J.: Wireless Telecommunications Systems and Networks, Thomson 2006, Springfield, MA, August 2006.
- [Nguyen, 08] Nguyen, T.D.; Nguyen, D.H.M., Tran, B.N., Vu, H., Mittal, N.: A lightweight solution for defending against de-authentication/disassociation attacks on 802.11 networks, In Proc. Int. Conf. on Computer Communications and Networks (ICCCN), 3-7 August 2008.

[Newman, 07] Newman, R.: Computer Forensics: Evidence Collection and Management, Auerbach Publications, Boca Raton, Florida, 9 March 2007.

[Rowlingson, 04] Rowlingson, R.: A ten step process for forensic readiness, Int. Journal of Digital Evidence, Vol. 2(3), February 2004, 1-28.

[Siles, 10] Siles, R.: Wireless forensics: Tapping the air – Part one, Symantec Corporation, Mountain View, California, 2010, <http://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one>

[Tan, 01] Tan, J.: Forensic readiness: Strategic thinking on incident response, Second Annual CanSecWest Conf., 30 March 2001.

[US.Doj, 01] The U.S. Department of Justice, Electronic Crime Scene Investigation- A Guide for First Responders, July 2001, [www.nwfa.org/NIJGuideforFirstResponders.pdf](http://www.nwfa.org/NIJGuideforFirstResponders.pdf)

[Velasco, 08] Velasco, E., Chen, W., Ji, P., Hsieh, R.: Wireless Forensics: A new radio frequency based location system, Intelligence and Security Informatics, 17 June 2008, 272-277.

[WLAN, 03] The New Mainstream Wireless LAN Standard, White Paper, IEEE 802.11g, 07 February 2003, [http://www.dell.com/downloads/global/shared/broadcom\\_802\\_11\\_g.pdf](http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf)

[Yang, 05] Yang, L., Zerfos, P., Sadot, E.: Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP), 16 November 2005, <http://rfc-ref.org/RFC-TEXTS/4118/index.html>