UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Privacy in Voice-over-IP

Mitigating the risks at SIP intermediaries

by

Thorsten Neumann

Submitted in partial fulfillment of the requirements for the degree

Magister Scientiae (Computer Science)

in the

Faculty of Engineering, Building Environment and Information Technology

at the

University of Pretoria

June 2009

© University of Pretoria

Summary

Telephony plays a fundamental role in our society. It enables remote parties to interact and express themselves over great distances. The telephone as a means of communicating has become part of every day life.

Organisations and industry are now looking at Voice over IP (VoIP) technologies. They want to take advantage of new and previously unavailable voice services. Various interested parties are seeking to leverage the emerging VoIP technology for more flexible and efficient communication between staff, clients and partners.

VoIP is a recent innovation enabled by Next Generation Network (NGN). It provides and enables means of communication over a digital network, specifically the Internet. VoIP is gaining wide spread adoption and will ultimately replace traditional telephony. The result of this trend is a ubiquitous, global and digital communication infrastructure.

VoIP, however, still faces many challenges. It is not yet as reliable and dependable as the current Public Switched Telephone Network (PSTN). The employed communication protocols are immature with many security flaws and weaknesses.

Session Initiation Protocol (SIP), a popular VoIP protocol does not sufficiently protect a users privacy. A user's information is neither encrypted nor secured when calling a remote party. There is a lack of control over the information included in the SIP messages. Our specific concern is that private and sensitive information is exchanged over the public internet.

This dissertation concerns itself with the communication path chosen by SIP when establishing a session with a remote party. In SIP, VoIP calls are established over unknown and untrusted intermediaries to reach the desired party. We analyse the SIP headers to determine the information leakage at each chosen intermediary. Our concerns for possible breach of privacy when using SIP were confirmed by the findings. A user's privacy can be compromised through the extraction of explicit private details reflected in SIP headers. It is further possible to profile the user and determine communication habits from implicit time, location and device information.

Our research proposes enhancements to SIP. Each intermediary must digitally sign over the SIP headers ensuring the communication path was not be altered. These signatures are added sequentially creating a chain of certified intermediaries. Our enhancements to SIP do not seek to encrypt the headers, but to use these intermediary signatures to reduce the risk of information leakage.

We created a model of our proposed enhancements for attaching signatures at each intermediary. The model also provides a means of identifying unknown or malicious intermediaries prior to establishing a SIP session.

Finally, the model was specified in Z notation. The Z specification language was well suited to accurately and precisely represent our model. This formal notation was adopted to specify the types, states and model behaviour. The specification was validated using the Z type-checker ZTC.

Keywords: Telecommunication, Next Generation Networks, Voice-over-IP, SIP protocol, Privacy, Information Leakage, Trusted Intermediaries, Zed.
Supervisor: Professor Martin S. Olivier
Department: Department of Computer Science
Degree: Magister Scientiae

Contents

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

List of Tables

List of Figures

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 1

Introduction

1.1 Introduction

The Internet has grown since its inception in the 1960s to a large scale recreational and commercial packet-switching network. The Internet experienced this growth primarily because of its openness and unrestricted use. It has become the largest network in the world enabling ubiquitous data exchange between all its connected users.

The continued use of the Internet has spawned new, previously unthought-of services. More recent developments include the addition of voice services to the decentralised communication infrastructure [76]. This allows for the point-to-point transmission of audio signals over the digital network. The technology was more appropriately named Voice over IP (VoIP) with the specific application of speech transmission.

Our research will examine telephony from the vantage point of its historic success. The traditional analog signalling matured into the far reaching Public Switched Telephone Network (PSTN). The current PSTN is secure, reliable and predictable.

VoIP, although still in its infancy, has experienced tremendous uptake. Communication occurs over a packet-switched network has many benefits to offer. The strong adoption of VoIP [92] has led to new mechanisms of enabling traditional communication over the Internet.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The technology itself has advanced through the creation of new protocols and value-added services. Tremendous progress in the creation of new algorithms for audio compression and near real-time network transfer has made VoIP suitable for commercial use [36]. The current technologies allow for the transferring of an *acceptable* quality audio stream across the public Internet. The mechanisms of transferring audio have been standardised and are being fused with instant messaging platforms to provide reliable, instantaneous communication paths. There is a high expectation that VoIP must match the quality of the PSTN infrastructure [20].

Current standards allow for the implementations of technology to create controlled and managed VoIP environments. These take into consideration the components that constitute part of a managed network (firewalls, gateways, devices). These are often only found in corporate networks where it is is possible to provide reliable, secure VoIP services.

VoIP over the public Internet, however, is more complex. It is difficult to integrate with legacy analog telephony systems in that one has to translate signalling and audio between two disparate technologies. VoIP on this Internet is a large, distributed architecture of independent devices. It can be compared to today's email messaging.

There are technical limitations that hinder the migration to a pure VoIP environment. There are flaws in its current implementations, which range from protocol level implementations through challenges in switching logic of VoIP gateways [95]. The lack of guaranteed quality of service and technical complexity are obvious hurdles. The technology is susceptible to denial-of-service attacks, call hijacking and interception without the user's knowledge [6]. Neither signalling nor audio stream are encrypted and there are no guarantees on the data integrity. Calls are commonly "not protected while it transits the provider's core network" [65].

VoIP is made possible through an emerging standard called SIP, a flexible signalling protocol. SIP enables remote parties to locate each other and establish a dynamic communication path across a number of intermediaries. There is, however, little control over the communication path and a lack of trust between intermediaries. Information leakage in SIP at each inter-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

mediary on the communications path is significant. The misuse of private information and leaked personal details make it possible to profile users.

We are interested in privacy in VoIP and motivated by the technologies inherent lack of security. SIP has certain known security weaknesses. A few of these, and possibly some not yet documented vulnerabilities, pose a risk to an individual's privacy. Many have simply suggested stronger encryption [95] and IPSec [26, 68]. While these methods have proven to be secure, the solutions are unrealistic given the nature of the internet.

Users should have greater control over their personal information when transmitted across the public internet. Ensuring better control would address their concerns, and can be achieved by adding identity information at each intermediary. We contend that identity forms the critical basis and the most solution to address privacy in VoIP.

The objective of this dissertation is to make a contribution to the field of privacy in VoIP. There is already significant published work on security, yet limited research into privacy in VoIP. Concerns as VoIP is being adopted rapidly, we need to give interacting parties assurance of a trusted communication path. Our contribution is the result of exploring privacy, identifying information leakage, and presenting a mechanism on ensuring trusted communication in VoIP.

1.2 Problem Statement

We propose enhancements to SIP to provide higher levels of privacy at the intermediaries. This would reduce the risk of a user's private information being leaked. Callers would be assured of confidential information exchange using mechanisms to validate the involvement of participating intermediaries. This dissertation explores how can one be assured of a high level privacy in a decentralised VoIP environment. This brings us to the fundamental question investigated in this dissertation:

> *how does one add identity information to VoIP to ensure that a user's privacy is protected?*

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Given the premise that privacy in SIP should be enhanced, we see a fundamental need to add identity information to the protocol. The addition of security headers can be shown in a model. One must first understand *the manner in which information leakage occurs in VoIP*. Through this, we aim to determine what practical mechanism to add identity information to the SIP protocol. Given that there is little control or control in VoIP, how can the model assure that the communication path can be trusted?

We are challenged to determine how our research would realistically integrate into a real world VoIP environment. It was considered to build a prototype based on our work. A prototype, however, is outside the scope of this dissertation and left for future work.

1.3 Approach

In confronting the said problem statement, we develop a model to attach identity information at each intermediary. By drawing on identity information, the chosen approach is greatly different from existing research based on security. The model builds on the existing communications architecture and, through investigation of related technologies, extends these onto VoIP. The model is further influenced by our analysis of possible leakage of private information.

Z notation [82] is a formal specification used in software engineering. Our model is specified using Z notation. This *set theory* makes it possible to specify the states and relational functions of the model. We use the notation to formalise our model, thereby making it exact and verifiable.

The model is supported by a literature survey. The development of telecommunication systems and evolution of Next Generation Network (NGN)s and VoIP were strongly considered. In addition, a literature survey of relevant privacy papers was conducted. This background information is presented to ensure that we have a common understanding and clear notion of privacy. On this premise we later attest that information leakage and privacy threats exist in VoIP.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The technical examples in our work have been taken from real-world VoIP gateways and end-point devices, and the SIP RFC [71]. These provide a solid basis from which we propose our abstract model.

1.4 Overview

The dissertation consists of nine chapters. The first and last chapter form the required structure of introduction and conclusion, respectively.

Chapter 2 gives a brief background on the history of telephony, the transition from analog to digital and its growth and adoption.

A discussion on the relatively new concept of NGNs follows in chapter 3. NGNs are fundamental to this research as traditional telephony is moving to high speed digital networks. These NGNs will someday completely replace the current fixed line telephony infrastructure.

Chapter 4 gives comprehensive background on the emerging VoIP environment. These distributed environments can only develop on NGN. In particular, we draw attention to the underlying protocols which enable this form of communication.

The question on what defines privacy and how privacy is viewed forms the central discussion point of chapter 5.

Our main ideas and contribution are discussed in chapter 6. It deals specifically with the topic of information leakage. It illustrates the lack of control of the communication that is of great concern. We therefore extend on draft proposals by the IETF on identity headers and present our own model in chapter 7. Our model is formalised using Z notation in chapter 8.

The dissertation is concluded in chapter 9.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 2

Background of Telephony

In the modern world, communication and information dissemination play a great role in our everyday lives. Even though electronic communication has brought new ways of information exchange, many businesses and organizations still traditional heavily on the basic telephony infrastructure.

Telephony is the science of converting voices and other sounds into electrical signals which can be transmitted by wire, fibre or radio and reconverted to audible sound upon receipt. The term originates from the Greek *tele* (far away) and *phone* (voice). Its definition describes the multitude of components and technologies involved in transferring audio signals. This includes end point devices, communication infrastructure and switching technologies.

This chapter gives a background on telephony. We touch on its origins, and discuss how telephony has evolved into the modern communication tool it is today. This gives us a platform from which we can determine why telephony has achieved such huge growth and adoption. This background underpins the later chapters which reflect on this discussion. The developments of telephony have greatly influenced the design of NGNs discussed in chapter 3 to follow.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

2.1 History

The invention of the telephone is an interesting story, revealing how this innovation struggled to gain acceptance. The actual history is a subject of complex debate. The initial telephone prototype was invented by Alexander Graham Bell, whose first device was built in Boston, Massachusetts, in 1876. Unknowingly, Alexander was competing with Antonio Meucci in attempting to produce a device which would not only send musical notes but articulated speech. He achieved this with financing from Boston University and was granted a patent number (174465) in March 1876. It covered "the method of, and apparatus for, transmitting vocal or other sounds telegraphically ... by causing electrical undulations, similar in form to the vibrations of the air accompanying the said vocal or other sound" [12].

Initially, telephonic communication required physical copper wires to connect two end points. The end points had to be manually connected by operators. They did this by bridging circuits at a central switching hub to which all telephony devices were connected. This, however, inhibited the widespread deployment of telephony as the design had natural limitations. It was constrained in the number of parties it could connect and devices it could support. It further hampered telephonic communication from achieving global reach.

The early installations had limitations which arose primarily from *noise* generated by the wires. This noise increased proportionally with distance, and although various methods of reducing noise were developed over the years, it remained a noticeable problem. Other physical disturbances were passed in the transmission such as fades, multipath reception and spurious signals. These disturbances decreased the quality of the communication because they produced effects such as fadeouts, crosstalks, hisses, etc.

The design of telephony was not capable of supporting its large demand, yet the technology had proven itself. The technology was under pressure after having attracted great interest from the public which wanted to make use of this revolutionary voice communication. New methods of switching, routing and services needed to be researched, developed and implemented.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

In the early 1980s, a new approach was taken in an attempt to convert speech into digital signals. Specifically, the implementation of Time Division Multiplexing (TDM) to place multiple calls on a digital line, allowed for a greater number of calls to be made over a single wire. By using digital methods, calls could be multiplexed and carried over far greater distances than traditional analog signalling. The quality of the service of the PSTN has greatly improved since. Digital systems convert the signal into bits, and combined with other frequency transformations and digital coding, improve the quality of the transmission. The improvement of digital systems comparing to analog systems is more noticeable under difficult reception conditions than under good reception conditions.

We have given background on the origins of telephony, and are now in a position to characterise the PSTN. It has matured into a well defined network that can be described by its attributes. These attributes are the pillars that have supported its growth, and underpin our research.

2.2 Attributes

The PSTN has many attributes associated with telephony based communication. The following paragraphs will discuss the voice quality, robustness and governance of the PSTN. These have contributed to its success, and must be considered when evaluating competing technologies.

Predominantly, the parties conversing are assured of a certain level of quality. This is perceived through the clarity of the voice call, being that the remote party can interpret the sounds, free from noise and echoes.

Telephones have always been reliable and easy to use. This can be attributed to the simplistic design of telephony equipment, which depends on the intelligence of the PSTN to function correctly. The reliability of the telephone network can be ascribed to the engineering design by which the PSTN provides power to the connected devices.

The PSTN behaves predictably and consistently, ensuring that calls reach their destination. The network has become extremely robust and one of its most important functions has become to assist during emergencies. The tele-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

phone has become an important means in many countries to summon emergency help, such as an ambulance or the police or fire department. Emergency services make use of the network to request assistance, coordinate activities and notify individuals [74]. Its favourable attributes are: firstly, that citizens can dial a single number, e.g. 911 in the United States (US) or 112 in Europe (EU). Secondly, calls are routed by the PSTN to the central emergency response centers, providing a failsafe mechanism during natural catastrophes. Further, the PSTN enforces caller identification Caller Line Identity (CLI) enabling emergency services to identify the source, record the number and trace the caller. The CLI is further tied to a geographic location, allowing emergency services to locate the source of the call.

To further ensure the maintenance and upkeep of the PSTN, various goverments have appointed controlling bodies to manage its operation. The National Telecommunications and Information Administration (NTIA) was created by the US government to advise on telecommunication policies drafted to address the country's economic and technological advancement. They further regulate the industry, stimulate competition and advocate the liberalisation of telecommunications policies around the world. They participate in international negotiations to open markets for US callers. They strive to ensure that all US citizens have affordable phone and cable service. A further orgianisation in the US is the Federal Communications Commission (FCC), established by the Communications Act of 1934, which is a federal agency in charge of overseeing interstate telecommunications, as well as all the communications services originating and terminating in the US.

The following background research will describe the current state of the fixed line telephone network. It is important to understand the infrastructure supporting the PSTN, which challenges the convergence of the *legacy* analog signalling infrastructure and high speed digital networks.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

2.3 Fixed Line Infrastructure

Today's PSTN infrastructure still requires dedicated resources to establish end-to-end voice communication. Each end device connects to a physical wire and makes exclusive use of the line for the duration of the call. A person places a call by dialing the number of the remote party. The PSTN then establishes a dedicated connection through the exchange of a signalling message.

There are many advantages to highlight when discussing the properties of traditional circuit switching [44]. Once a connection is made, the communications channel remains open for the engaging parties until the call is terminated. Interacting parties can communicate in real time with minimal delay over the wire. The network is capable of providing power to end devices, thus telephony devices are able to function independent of a reliable power source. They are connected at all times and have access to a multitude of services provided by the network.

The limitation of dedicated resources implies that each end point can only communicate to one other telephony device at a time. Unlike the early days of telephony however, the core of the PSTN networks no longer depend on individual wires or dedicated channels for remote parties to converse. Calls are switched, multiplexed and forwarded along Private Virtual Channels (PVCs), allowing for a greater capacity of voice calls to occur simultaneously. The *backbone* consists of many nodes with a star-like network topology which make up this fully connected network.

The telephony network developed and matured into a comprehensive suite of technologies and protocols. It now forms the basis for our global communication infrastructure. Although the PSTN has global reach, it is constituted out of many telephone companies inter-operating with each other. Each company has a network of transmission paths or "carrier links" tying together their serving networks. Calls are switched by these carriers to remote networks, which in turn further relay a call to its destination. Through this, a carrier can support a larger number of users sharing its common communications infrastructure.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Carriers operate in a competitive industry and introduce value-added services to attract new customers. These services are qualitative in nature and have allowed them to capitalise on additional revenue sources. Carriers charge nominal fees for services such as voice mail, call forwarding, caller ID and itemised billing.

A fee for services is charged by each carrier. The fee charged for a call (or service) is calculated on the operator's infrastructure, interconnection and administrative costs. Each carrier will maintain detailed records of network events, which they in turn charge the users. Since the connection between parties is temporary, a carrier will bill the users for the call (or services) consumed. This charging model is transparent, and allows for the easy reconciliation of calls made/received and the charges incurred. It further allows carriers to charge varying fees for different services.

This section covered the fixed line infrastructure which by implementation sets the quality and reliability attributes of the PSTN. The following sections will discuss the access components of the fixed line network.

2.3.1 ISDN

Integrated Services Digital Network (ISDN) is a type of circuit switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires. This results in better quality and higher speeds than available with analog systems.

There was a worldwide standardization effort and discussions by organizations responsible for establishing the ISDN standard, who pointed out the limitation and inflexibility of the ISDN. For broadband services such as video and high-speed data, the problem is the that the fundamental rate of ISDN transmission is limited to 64 kb/s [103]. While multiple ISDN lines can be used in parallel to achieve greater throughput, the capacity of a single line can not be increased.

ISDN is affected by the compatibility of switching technology, the local loop arrangements, the availability of rate adaption, and the efficiency of bandwidth utilization. Although some basic principles of ISDN can be

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

carried to broadband, the technology is quite different. For example, the interconnection and transmission problems are different to those of analog voice.

2.3.2 Fibre Optic

Fibre optic cables have rapidly replaced copper to provide long distance carrier links. During the first half of the 1990s, the proportion of fibre rose to over 80%. Although fibre technology was first used for backbone transmission facilities, the technology is now being deployed closer to customers. Although the number of installed fibre channels nearly tripled during the first half of the 1990s, copper wire still links more than 90% of customers to the network local distribution facilities [49].

2.3.3 DSL

DSL is the most revolutionary service to enter commercial PSTN services. DSL employs new transmission technology in order to provide both greater throughput and available bandwidth. It uses passband modulation (between 25 kHz and 1.1 MHz) to more efficiently exploit the available capacity of copper wires.

Peden *et al.* [100] notes that "DSL technologies have benefited from the continuing advances in electronics. Apart from improvements in functionality, there is modest scope for DSL modems to access more of the intrinsic information capacity of the copper pairs. This relies on more sophisticated modulation and coding techniques, and making use of improvements in silicon integration to generate additional improvements by reducing cost, and reducing power consumption." DSL is therefore capable of supporting 1.5Mbps, 6Mbps, 13Mbps and 53Mbps transmissions.

2.4 Mobile Networks

The obvious factor within the PSTN is that lines are fixed to a location. This makes it difficult to communicate when not one is not physically at a tele-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

phony device. Research surrounding communication has sought for alternate means of transmitting voice and data. These considered wireless technologies with greater reach and mobility for users. We give a brief background on mobile networks, and contrast these to the above discussed fixed line infrastructure. The developments surrounding mobile communications have greatly influenced telephony and its impact is evident from the growth and adoption figures discussed in 2.5.

2.4.1 GSM

Global System for Mobile (GSM) communications is a digital cellular communications system. The idea behind GSM is a cell based mobile radio system, first prototyped by Bell Laboratories in the early 1970s. It was only introduced for commercial use in the 1980s, and implemented using analog cellular technology. The technology has experienced tremendous growth, and each country began to develop its own cellular systems. This resulted in limited coverage and incompatible hardware devices, limiting a users mobility and the mobile device marketability. In order to establish a common standard, the Conference of European Posts and Telecommunications (CEPT) formed the Groupe Special Mobile (GSM) in order to develop a pan-European mobile cellular radio system [39].

The GSM specification was drafted in great detail, and had to meet specific criteria. These included the efficient use of the radio spectrum, international roaming, low infrastructure costs and good quality voice communication. While the requirements were being drafted, GSM further had to be digital and compatible with ISDN. It needed to support the addition of new services without any major adjustments to the underlying infrastructure. GSM had to cater for all these requirements in order to ensure that the technology was future-proof.

The responsibility for the GSM specifications was passed from the CEPT to the European Telecommunications Standards Institute (ETSI) in 1989. The aim of the GSM specifications was to describe the functionality and the interface for each component of the system, and to provide guidance on

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

the design of the system. These specifications standardized the system in order to guarantee the proper interworking between the different elements of the GSM system. In 1990, Phase I of the GSM specifications was published. From the evolution of GSM, it is clear that GSM is no longer only a European standard. GSM is operational in over 220 countries around the world and used in over 800 networks [39].

GSM has adopted a multiple access scheme to allow for different simultaneous communications in the radio spectrum. A mix of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), combined with frequency hopping, is used. This allows for many handsets to roam between different mobile stations situated in different cells.

The GSM technical specification defines the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts:

- The Mobile Station (or Subscriber Identity Module)
- The Base Station Subsystem (and transceivers)
- The Network and Switching Subsystem
- The Operation and Support Subsystem

2.4.2 3GPP and IMS

The Third Generation Partnership Project (3GPP) was the first to specify a new standard for offering voice and multimedia services over a mobile network. They drafted a specification that defines a generic architecture to deliver "Internet services" over data bearing networks. Originally this was done thought using General Packet Radio Service (GPRS) but has now been extended to Third Generation (3G) mobile networks, wireless LAN and also fixed line. The specification has been termed the IP Multimedia Subsystem IP Multimedia Subsystem (IMS) standard and is now part of the vision for evolving mobile networks beyond GSM.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The 3GPP body does not want to standardize applications within the mobile environment but rather seeks to aid the communication across mediums and technology platforms. The IMS-based services should enable various modes of communication including voice, multimedia and data in a highly personalized and controlled manner.

The IMS takes care of providing Quality of Service (QoS) to mobile Internet users [15]. The standard further defines a layered architecture where services and common functions can be reused for multiple applications. This has arisen from the trends in communication where mobile network providers have to cater for the user needs and provide a richer user experience. They must make it more convenient and easy to use and accessible to the masses while ensuring that the infrastructure is secure.

The IMS standard adopted Internet Engineering Task Force (IETF) protocols and is built on SIP as the standard protocol to support the IMS architecture. Several roles of locating, signalling and administration are performed by SIP proxy servers, collectively known as CSCF (Call Session Control Functions). These process SIP signalling packets in the IMS to handle user registrations, routing, forwarding of requests and charging in the IMS network [15].

The evolution from traditional telephony to advanced, loosely coupled data networks is underway. Most of our research will focus on SIP in later chapters. It is important to understand the magnitude of devices, network operators and Internet services that will be using this advanced communications protocol. It remains to be seen if the design of 3GPP will meet consumer expectations.

The following section will summarise current statistics that show the growth and adoption of telephony. We will close this chapter with a suggestion of the significant role that telephony plays in our lives.

2.5 Growth and Adoption

The volume and duration of voice calls has grown steadily, revealing the extensive usage of the telephone network. Trends over the years have shown

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Years	1998	1999	2000	2001	2002	2003
Millions of Minutes	93,000	108,000	132,027	146,095	155,165	166,615

Table 2.1: International PSTN Traffic Summary, 1998 - 2003

this continued growth. In the US alone, over 98.5 million people have access to telephone services [20, 49]. Globally, there are over 700 million copper pairs worldwide which provide for extensive telephony connectivity [100]. This reveals how important a role telephone communication plays in our daily lives and the value society places on this facility.

Industry has closely monitored the use of telephony [66] to quantify the sustained growth in recent years. The number of minutes spent on the phone continued to grow, as shown in Table 2.1. Between 1985 and 1995, international telecommunications traffic grew from 15.6 to 60.3 billion minutes, and the US, with 22.6 billion, is by far the largest communicator. It has been calculated that about 2% of all consumer expenditure in the US is devoted to telephone services [49].

The cellular industry has grown exponentially. Mobile services based on GSM technology were first launched in Finland in 1991. This reached an estimated 10 million GSM subscribers in Europe by December 1995. The growth has however not been linear [49] and it was reported that "that it took just 12 years for the industry to reach the first billion connections". The trend has not slowed, with the GSM Association celebrating the addition of their second billionth GSM subscriber in June 2006. The success of GSM can be attributed to "an original vision of a cross border digital communications system, now used in almost every country of the world today" [39].

The revenue derived from cellular communication in 1998 already exceed $33 billion, and shows strong growth. The cost for communicating has during the same period dropped by over 60%, making the technology more accessible to the people. The aim is to supply sub $30 low cost mobile phones to attract "a significant proportion of the world's unconnected people" [39].

Rapid advances to data bearing infrastructure have seen more than 105 networks across 50 countries launch commercial 3G services. The adoption

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

of the next generation 3G service is therefore also flourishing. GSM World reports that in Europe an estimated 95% of all new subscriptions are for 3G based services.

2.6 Conclusion

In closing of this chapter, it is evident that telephony has greatly impacted on society. Its development has influenced governments, businesses and individuals. Fixed and mobile communications have created new opportunities for people to connect. These have in effect placed pressure on the telephony services, driving further development and technology innovation.

The chapter to follow will discuss how the underlying PSTN infrastructure is converging with NGNs. The reason for the paradigm shift towards switched data networks will become clear. NGNs still have to mature to meet the aforementioned quality of service of the PSTN, but the move to digital networks is inevitable. The next chapter extends on this background as the research will be moving onto VoIP which has developed as a result of packet switched networks.

Chapter 3

Next Generation Networks

Alongside traditional PSTN infrastructure, the world has seen the emergence of distributed packet switching networks. These networks span the globe and exist in the form of a PSTN overlay. Packet switching networks have been built on top of the PSTN. They make use of the available infrastructure to create an *always on* data network. Unlike the analog PSTN, however, these networks are entirely digital.

These networks have formed the global Internet whos structure can be likened to loose coupling of independent networks. These networks are managed by independent Internet Service Provider (ISP), who decide on the infrastructure, services and prices. ISP determine where and how to supply various services, and to which of its users. The interconnections that bind the many independent networks into a connected whole is the use of a common address space and distributed traffic routing.

We will first review the Internet as it exists today, and the it role it plays in contemporary computing. We then describe its design, particularly reviewing its scalability and security, which leads to the third section detailing the facades that qualify an NGN. It will be evident from this chapter how NGNs are required to support the new emerging data and multimedia requirements. A packet network is a prerequisite to transport and exchange this type of data between two (or more) communicating parties which we detail in in chapter 4.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

3.1 Packet Networks

Packet based communication has existed for many years. Its first implementation was in "ham" radio which became a data networks. In order to communicate, a device needs to assess if the physical medium (wire or wireless) is free before transmission. The channel is always available yet shared amongst many devices. A sending device buffers data and attempts to transmit during a *quiet* interval. A listening device receives the transmission and accept the data for further processing.

The principle of packet switching is that data is fragmented into smaller packets and sent across a commonly shared infrastructure. The data can be passed between many devices until it reaches its destination. The data from various sources is sequentially interwoven, making continuous and efficient use of the underlying medium. Each data fragment carries its own instructions. It is routed to its destination based on local decision-making rules within a capable routing device. The instructions exist in the form of a headers conforming to the strict standards of the implemented communication protocol. Used protocols include TCP, UDP, ICMP etc. A header would carry source and destination information, payload size, transport flags and quality of service settings.

Devices such as a hubs, switches or routers accept packets and forward packets based on their headers. These devices act as intermediaries and collectively called *hops* . The chaining of intermediaries creates a route along which data can flow. A route can be dynamically determined while the packet is being forwarded. Therefore, a sending node is able to communicate with another without having to know how to reach the destination. The *hops* along the route maintain a *routing table* containing possible paths for the packet. This ensures the data is forwarded and passed on efficiently. Fundamentally, all devices are linked to another through some medium of physical connectivity. They employ application layer routing protocols [32] to communicate their state, and connectivity to other nodes. This will be further detailed in 3.2.2.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

This chapter summarizes the current configuration of the Internet, and discusses the approaches used in building, maintaining and expanding this global network. There are, obviously, limitations with its current implementation. The network lacks credibility, the available resources are abused and many security vulnerabilities exist, making the public Internet unsuitable for commercial use. For this very reason, the greater Internet community is evolving the infrastructure into an NGN. The features and attributes of this futuristic networking concept support the paradigm of voice and data networks convergence.

3.2 The Global Internet

Everyone knows the Internet is growing rapidly, but quantifying the exact growth with precision is difficult. Tracking the expansion of the Internet is a daunting task, as it continues to grow rapidly and expand globally [64]. Currently, this expansion occurs at a rate, which at a minimum, doubles its size each year [48].

The United Nations Development Program and Oxford University Press have published an annual report on human development since 1990. Interestingly, they found that the state of a society can be compared against *Internet hosts per capita* . They quantified society in the form of a Human Development Index. This index considers factors such as life expectancy, adult literacy, combined secondary and tertiary school enrollment, and GDP per capita. The results show a strong correlation between the index and a high number of Internet hosts within a population [67].

Internet technology advances have benefited society and increased our productivity, yet have also made us critically dependent on the reliability of Internet services [16]. Business and industry requires guarantees on service and availability, which the current Internet can not provide. The network has grown organically and, while many efforts attempt to address these shortcomings, certain remain prominent. The following sub sections will highlight a few imminent constraints which hinder the Internet in its growth.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

3.2.1 Reliability

At times, users experience the poor performance of the public Internet. Internet Service Providers can not guarantee reliable and uninterrupted access. Handley and Greenhalgh note that "...for the Internet to achieve its full potential, it has to be able to offer highly reliable service" at all times [43].

Disruptions to the network result in packet loss. This loss is considered a failure of packets to reach their destination. Newer routing devices support various redundancy mechanisms to resend data should a packet get lost. In an ideal network, no packet loss would ever occur and devices would react to physical failures immediately [61]. While network operators can reduce the frequency of physical failures, a greater number of operational errors and network faults arise.

Denial-of-Service (DoS) attacks are one of the most significant problems currently facing the Internet. Defending against DoS attacks is extremely difficult. These attacks take advantage of the limited security in IPv4, and are virtually unstoppable when initiated from widely distributed hosts. Effective solutions to prevent DoS attacks require significant changes to the Internet networking architecture. It is, however, important to weigh up the "...flexibility needed for future Internet evolution and the need to be robust to attack" [43].

3.2.2 Routing

The primary interior routing protocols in use today are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). OSPF is now the most important on large networks and ISP networks. The primary exterior routing protocol for exchanging routing information between autonomous systems is BGP (Border Gateway Protocol).

Internet routing instability and the fluctuation of network routing information is an evident problem currently facing the Internet. High levels of network instability lead to packet loss, increased network latency and time to convergence. Such errors in the Internet core can result in service interruptions at ISPs. Depending on the location within the backbone, a disruption

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

could result in a loss of connectivity between national networks.

Labovitz *et al.* [57] analyzed data collected from border routers at five ISP over a nine month period. The research shows that "...the volume of these routing updates is several orders of magnitude more than expected and that the majority of this routing information is redundant". They found that "...there are a number of anomalies in the exchange of inter-domain routing information". Observations found several unexpected trends and unpredictable behaviour in the exchange of routing information [57].

Early signs of routing anomalies are increased packet loss, additional memory/CPU overhead on routers and backbone outages. The increased network and router load results from a large number of redundant updates. While this information does not substantially impact on the network's performance, informal experiments show that high update rates could impair (or even crash) routers. The concern is, however, the volume and scalability implications of global IPv4 traffic routing.

3.2.3 Address Space

The global Internet address space currently caters for 32 bits of unique addresses with a theoretical maximum of 2^32 = 4,294,967,296 hosts. In reality, the address space has been allocated in fairly large contiguous blocks which renders strictly optimal utilization difficult. In the past this has been perceived as a worthwhile performance tradeoff, since this facilitates more efficient routing and enhances the administrative manageability of the network.

In recent years concerns have grown that the Internet may be running out of available address space. The concerns started over a decade ago about scaling of the network. The consumption of address space was considered to be an immediate and compelling threat to sustained growth of the Internet. Huston [48] measured an "...annual growth rate of a little under 7%, and at that rate of address deployment, the IPv4 address space [would] be able to support another 19 years of such growth".

The implications, however, are that ISPs are constrained by the available

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

free pool of IPv4 addresses. The limitations of Internet address space is "...largely the result of the interaction of existing router technology, address assignment, and architectural history" [47].

Industry is continuously demanding greater bandwidth and throughput, pushing the capabilities of our current data networks. Since VoIP was never provisioned for in the current Internet environment, new mechanisms to provide for reliable voice services are being sought. The primary concern when using VoIP is the quality of audio (specifically speech) after being transmitted to the remote end point. The Internet Protocol (IP) network must provide sufficient *bandwidth* to ensure that no session or audio data is lost. Considering the future requirements of network infrastructure to provide effective QoS for data, voice and video, academia and industry are looking for new means to ensuring that the growing demands are met.

Athena *et al* [58] show in a study that these interferences and interruptions result in a loss of interactivity, variable speech burst delays and sound clipping. Their research assesses the current capabilities of the existing Internet infrastructure to support VoIP communication. In an attempt to assess the perceived quality of an Internet phone call, various influential characteristics are measured. They examined 43 paths over seven different ISPs and presented insightful results. Their study reveals that "backbone networks are, in general, insufficiently provisioned" and that current networks exhibit problems in guaranteeing reliable transmissions, and confirms that the public Internet does not provide the required quality of service for VoIP. The quality and reliability of VoIP is, therefore, not guaranteed but a best-effort service.

Typical Internet applications use TCP/IP. IP itself is a connectionless best-effort communications protocol, while Transmission Control Protocol (TCP) is a reliable transport protocol. TCP/IP is, however, not suitable for real-time communications because of its acknowledgment and retransmission features. User Datagram Protocol (UDP) provides unreliable connectionless delivery service using IP to transport data between end points. In VoIP, the audio and signalling is transmitted in Real-time Protocol (RTP) packets to achieve near real-time data transmission [41]. RTP does not reserve resources

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

and does not guarantee QoS. It is purely employed to ensure that audio fragments arrive in their original sequence and can be reordered for playback at the destination.

The raised concerns about Internet services, its reliability and limited security are real, and hinder the network's growth. Various organisations and academic institutes are addressing these concerns in the design of the NGNs. We will be discussing this further, and detail the use and functioning of signalling over UDP in the chapter to follow.

3.3 Next Generation

Much hype and recent news discusses the benefits of NGN. The discussions since about 2003 has been around *what an NGN is* . The term conceptually describes the many changes and enhancements that will make available higher capacity and more reliable data networks [18]. The ITU defined an NGN (in recommendation Y.2001) as "a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies, and in which service-related functions are independent from underlying transport-related technologies". They go further on to say that "it enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users".

Our current Internet architecture has inherent limitations in design. The high demand for Internet services over the unprovisioned communications infrastructure creates contention and network congestion. The infrastructure can not supply sufficient bandwidth to all its users. Further, backbone nodes are involved in translating from one media to another, which adds latency and additional overheads. This impairs the efficient transmission since the transmitted data may undergo many optical-to-electronic *(and vice versa)* conversions [79].

Our current networks are being transformed into NGN through an evolutionary process. NGN will be the result of a major overhaul of the existing

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

infrastructure, replacing copper wiring with optical fibres, resulting in an end-to-end optical architecture [79]. Optical fibre has the capacity to transmit large volumes of data, and can be deployed in conjunction with technological innovation such as Wavelength-Division Multiplexing (WDM), to provide high throughput data networks.

The difference between an NGN and the Internet is not always understood. In effect they both use IP as a core protocol. An NGN must provide all of the services the Internet currently provides yet in an more efficient and reliable manner. In differentiating the public Internet from an NGN, an important point to note, is that an NGN does not restrict service delivery to best effort. The NGN must support various contractual services, requiring it to be a secure, trustworthy managed network [56]. The following sections will highlight these requirements to deliver these service.

3.3.1 Quality of Service

An NGN, however, is not only concerned with providing sufficient bandwidth and high data throughput. An NGN will provide many additional services, adding superior levels of Quality of Service (QoS) and reliability. It must scale to meet future demand and support the various possible usage requirements [18]. The ITU-T WG 3 is focusing on QoS and the development of end-to-end QoS related deliverables.

Greater QoS can be achieved through adaptive and network aware routing. Chen *et al.* details the relation between QoS and routing. The paper argues that traditional routing protocols used in packet switched networks do not "... meet the requirements of future integrated service networks that will carry heterogeneous data traffic". The classic constraints of meeting QoS requirements are compared to the efficiency of their practical implementation. They have classified a multitude of algorithms into three proposed categories: source, distributed and hierarchical routing. The authors acknowledge that meeting QoS requirements is a difficult task, yet note that "QoS routing is a key network function for the transmission and distribution of digitized audio/video across future high speed networks" [19].

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

One reason for creating the IMS was to provide QoS in mobile networks. Current GSM networks provide no guarantees on data throughput or transmission latency. It is therefore critical to provide a predictable and reliable multimedia session when communicating using 3G [15].

3.3.2 Redundant and Self Healing

An NGN must tolerate many network variations. A basic objective of the Internet is to tolerate various network characteristics, e.g. limited bandwidth, variable delay, packet reordering and packet loss. An Internet host must be able to interoperate robustly and effectively with any other Internet host, across diverse Internet paths. The network must be robust against failure of individual gateways and hosts.

The throughput of a packet network, however, is nondeterministic in its nature and thus the actual available bandwidth and *en route* packet delay cannot be predicted. This has been the challenge of many an academic work, and primarily led to the conceptualization of fault tolerant networks. QoS describes the prioritization and end-to-end reliability, thus embracing the concept of fault tolerant networks. In order to achieve high availability, failover configurations and network aware routing algorithms have been suggested as the most suitable recovery mechanisms [77]. A common approach is failure detection, thus allowing for the immediate rerouting of packets through an alternate route. There are both benefits and drawbacks in such a redundant architecture, since the additional resources required come at a cost and must be effectively utilised when operations are running smoothly.

3.3.3 Service Creation

Service creation is the concept of implementing a set of activities that relate to the specification, design and testing of value-added services in communication networks [18]. These generally apply to data networks where value-added services are defined and added to the existing network infrastructure. These go beyond the simple packet switching mechanisms and are targeted at specific applications such as video or voice services. Unlike the PSTN, the

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

NGN must cater for the needs of the 21st century network which is a flexible platform for service delivery. Thus service creation addresses the wide range of services, applications and mechanisms based on real-time, streaming and non-real-time services.

3.3.4 Billing and Administration

Ginzboorg [33] found that "...the telecommunications industry is undergoing three major changes". Firstly, regulators are pressuring telecommunications providers to become more competitive. Secondly, wireless services are becoming more prominent, drawing on the revenue generated by fixed line infrastructure. Lastly, the volume of Internet traffic is becoming more important than the network access charge.

To date, most commercial Internet services are charged an all inclusive flat-fee. This fee is an access charge, usually in proportion to the services, line speed and/or bandwidth requirements of the user. A problem has always been to classify and meter different types of traffic [22].

In an NGN, however, service will be differentiated and charged for on a usage basis as opposed to a single fee. Video and streaming requirements differ to those of web browsing or email, yet are charged at the same rate. One important differentiation in an NGN is that a premium can be charged for the QoS requirements of a provisioned service. This allows for the classifying, therefore fine-grained billing, of services. IMS-based services in GSM provide for differentiated service-specific billing [15].

3.3.5 Ubiquitous Access

In comparison to even a decade ago, the thought of mobile networks seemed far fetched. The concepts of the wireless spectrum carrying data had obviously been explored, but carried little weight due to its limitations in transmission range and data throughput. Reflecting upon this, the wireless networks of today are capable of transmissions comparable to the speeds of broadband. An NGN fully embraces mobility, and makes available connectivity and services across wireless networks. The convenience of location

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

independent access brings with it a various intricacies. One has to reassess the previously described attributes of QoS, reliability, redundancy and data throughput. Many papers [18,32,45] discuss ubiquitous access from a usability and reliability standpoint.

3.4 Conclusion

The basics of packet switching networks gave rise to the Internet, and we presented both its social importance, and its technical limitations. While the Internet is a tremendous achievement in creating a unified global communications system, it still has many shortcomings. These are being addressed in the concepts and design principles of NGNs. The move towards NGNs will allow for the convergence between the PSTN and Internet.

In this chapter we presented the developments behind emerging next generation networks. The remainder of the dissertation assumes that all data exchange is over a packet switched network. The above attributes confirm that the global Internet is a a large, decentralised and unmanaged network. It is the voice communication over this network which we are aiming to control, and challenge in the later chapters. We will continue this technology discussion and present the developments of the more recent voice communications in the next chapter.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 4

Voice over IP

Telephony was discussed in detail in chapter 2. This chapter continues on the trends that can be observed within academia and industry who are actively building VoIP solutions. We give background to how this communication technology is being implemented, and how it differs from the PSTN. The discussion draws on the concepts of a converged communications environment summarised in the previous chapter. The distributed architecture of VoIP leverages the bandwidth, QoS and dynamic service provisioning of an NGN. It is therefore agreed that the move of telephony onto packet switched networks in inevitable.

In these sections we discuss the developments of VoIP and related technologies. We introduce VoIP in section 4.1, and follow on to clarify the role of audio encoding and signalling play in section 4.2. It is vital for the reader to be made aware of the VoIP architecture illustrated in section 4.3. Section 4.4 explains how the distributed architecture is supported through the application layer routing of SIP. The aim of this chapter is to explain the functioning of VoIP. We specifically highlight the signalling headers in light of this dissertation and further investigation.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

4.1 Introduction

Our research begins with an introduction to VoIP. This section gives background on the developments that allowed this communications technology to take shape. The introduction will then elaborate on audio encoding methods and further clarify the underlying architecture. This holistic review gives us a platform from which the discussion delve into the technical details of the underlying protocols.

Many organisations are in pursuit of converging their communication networks, allowing for the provisioning of services over a single shared infrastructure. These services, such as voice, video and data, are being transported by packet-switched networks, extending the reach of our global communications infrastructure.

The motivating factors for convergence are the reductions in cost, the continuous innovations allowing for greater service integration and the potential for ubiquitous access and service delivery. However, with these advantages certain privacy concerns surrounding the unification of services into a single *global* network emerge [76].

In the early 1990s, technology changes supported the initial efforts of VoIP communication [76]. VoIP technology, although still in its infancy, has since experienced tremendous uptake, revealing many of the inherent benefits this distributed communication architecture has to offer.

There are many drivers behind the strong adoption of VoIP. Primarily, businesses motivate that they can achieve a reduction in cost, consolidate their infrastructure and centrally manage their telephony network [53]. Considering the radically different technology required to support VoIP, companies evaluate the capital outlay and their return on investment. An economic analysis will show that the cost per minute compared to cost of lines has a very low break-even point [36]. A business will achieve greater telephony cost savings as the network access cost is an inherent operational cost, and thus discounted when determining the cost per call. The calculated cost works out to significantly less than traditional PSTN call charges. Competition between VoIP service providers has pushed down the the rates to between 5

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

to 10 cents per minute.

Users gain ubiquitous access to their telephony services and greater mobility when using VoIP communication. They can call from any Internet-connected location, and use a softphone or VoIP device to place calls.

Service providers such as Vonage are offering voice services to consumers, allowing them to make calls to other Internet users or consumers connected to the PSTN. Cherry [20] explains how they are changing the telecommunications landscape. He writes that in North America over 400 providers are competing for residential customers. He reasons that while VoIP is not free, its low cost is the reason why these commercial providers are signing up thousands of new clients a day. The author boldly states that "all telephony will eventually be done over IP" and "the momentum is clearly in favor of VoIP".

4.2 Audio Transmission

Continuing on the developments, this section describe how audio is transmitted over a packet switched infrastructure, differentiating VoIP from traditional telephony. These innovative approaches to encoding speech and signalling give background on how VoIP functions. This section is central to our research, providing the basis to clarify the details of SIP signalling.

The transmission of audio between two communicating parties in VoIP is different to the traditional PSTN. Unlike analog signalling, the audio is digitized, and transmitted over a packet switching network. This is achieved by encoding the original sound, thereby breaking the continuous analog wave into data segments. The method of encoding and compression greatly influences the bandwidth requirements of a call. The methods of encoding audio are discussed briefly and serve to illustrate how VoIP simulates PSTN behaviour.

The speech quality of a VoIP call is influenced by various factors. Most noticeable to the user are speech interruption (dropouts), echoes and reduction in voice clarity. These interferences result from variations in network delay time and packet loss. Echos are, for example, caused by network inter-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

ruption while dropouts are a result of connection failure. Unlike data, which can be buffered and retransmitted, voice is real time. The encoded voice traffic requires end-to-end QoS.

Related papers [4,35,58] have addressed QoS and suggested viable mechanisms in provisioning network resources and guaranteeing reliable data transmissions.

4.3 Architecture

4.3.1 Signalling

VoIP communication is still in its early stages of actual implementation and developments are strongly supporting the fairly new protocol: Session Initiation Protocol (SIP). SIP was defined by the IETF in 1999 and a new version of the specification was standardised as RFC 3261 [71]. It was incorporated into the standards track in 2002 and therefore considered a relatively new protocol. SIP differs from the existing telephony signalling protocols in that it text based (ASN.1) does not reserve resources or establish dedicated connections. While competing protocols such as H.323 provide a far more robust framework, they also tend to be more complex and cumbersome to implement. SIP is considered a light weight and flexible protocol, well suited for our distributed, loosely coupled networks. It was an obvious choice for ad hoc and mobile networks and has been adopted by the 3GPP in next generation mobile networks service provisioning [15].

The signalling employed in VoIP communications is of great importance. The technical detail to follow draws upon the formal specifications to describe the protocol's functioning. This summary explains the most important attributes of SIP, particularly the information in its headers. The headers carry private and confidential information, and the transported information and attributes are pointed out. This chapter presents these in the light of the research surrounding security in VoIP. The privacy implications of possible information leaked by these headers is analysed in the chapter to follow.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The SIP is a generic session management protocol. It was drafted by the IETF and is an "application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls" [71]. The protocol itself is not a comprehensive communications mechanism, but a signalling standard for the discovery and communication of remote parties. SIP, therefore, does not define the characteristics of a session and relies on a suite of complementary protocols.

The protocol is based on HTTP-like messages, which when sent to either a proxy or device, invoke at least one response. The first line of a SIP message always contains a *Method* name and the lines to follow are optional *Headers*. The *Method* name is an instruction which is inspected by the recipient and processed accordingly. This name, comparable to requests in HTTP, assists in managing the session and either creates, modifies or terminates sessions. The *Headers* provide additional information about the session, passing attributes such as caller name, date and time or routing information. Additionally *Headers* convey signalling details such as sequence numbers, call identifiers and message expiry. Since messages are transported over UDP, a stateless protocol, SIP depends on these attributes to correlate messages to a session.

There are two influential attributes that distinguish SIP from any other technology implementation to date. Firstly, SIP messages are designed to be handled by many intermediaries. Messages are passed on until they reach their destination, incurring numerous DNS lookups and routing decisions. This leads on to the second factor. The design of SIP contravenes the guidelines set out by the ISO model through incorporating routing and network-related details in its *Headers*. It thereby abstracts the *Transport Layer* routing intelligence, giving the *Application Layer* the ability to decide on the next hop. Messages can be passed to any chosen proxy (or device) for handling. The implications of *Application Layer* routing are discussed in [32, 75]. The agility of SIP is therefore also its weakness.

A caller would initiate a session by specifying a SIP URI e.g. sip:alice@atlanta.com. The calling device does not know of the destination, and thus the domain name portion of the URI is used to locate an authorative

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

proxy. The URI is passed on to this proxy, and the specified username used to communicate with the intended recipient.

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
   ;branch=z9hG4bK77ef4c2312983.1;received=196.35.68.101
Via: SIP/2.0/UDP pc33.atlanta.com
   ;branch=z9hG4bK776asdhds;received=196.35.68.99
Record-Route: cdr-svr.atlanta.com
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
User-Agent: <Motorola VT1000 mac: 000F9F466CD0>
Contact: <sip:bob@192.168.1.110>
Contact: <tel:+27837890107>
Max-Forwards: 70
CSeq: 314159 INVITE
Content-Type: application/sdp
Content-Length: 131
```

Figure 4.1: SIP Message detailing Headers

Once contacted, the recipient responds and messages are sent back to the originator indicating a resulting state. Communicating over a public network further implies that SIP messages will traverse multiple proxies and service provider networks. Thus, in almost all scenarios the messages will be handled by two or more proxy intermediaries.

The Request For Comment (RFC) outlines the many aspects of negotiating and establishing a communications session, in particular the sequencing, timing and response codes used when exchanging SIP messages. These will not be discussed here as they are detailed in the RFC, and the focus of our research is on securing the communication across intermediaries. The protocol is explored in detail above as chapter 7 refers back to this background when we developing the model for securing SIP communication.

4.3.2 End Points

An end point is often a device identified by a SIP Uniform Resource Locator (URI). This URI is an address comparable to an email address, specifying either source or destination of a message. The URI is the concatenation of a user identifier, the @ sign and a Fully Qualified Domain Name (FQDN). Illustrated in Fig. 4.2, a SIP URI would be *sip:bob@biloxi.com*, where *biloxi.com* is the FQDN and the user registered as *bob*. These URIs are used in **To** and **From** headers respectively, depending on the direction of the messages.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

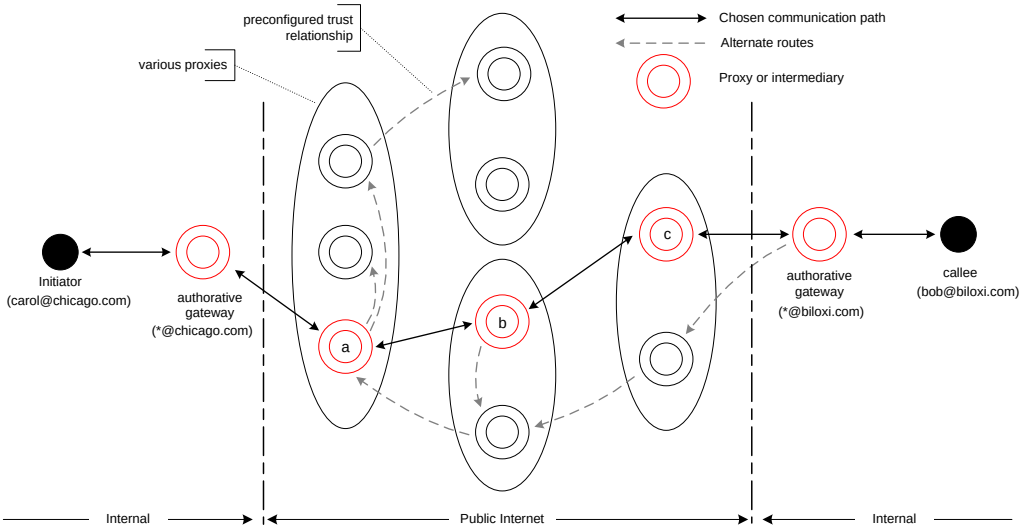

Figure 4.2: Typical VoIP Configuration

4.3.3 Intermediaries

In order for VoIP communication to take place, end point devices communicate via VoIP intermediaries. A VoIP intermediaries could be a gateway or proxy. These assist in establishing, maintaining and terminating telephone calls across an IP network. They manage the many sessions between local devices and remote networks. The term session is used more generally to describe all the handshaking and signalling during a VoIP call.

A gateway is often a software implementation and referred to as a call controller or session manager. Goode [35] gives comprehensive background on the gateway and the role they play. He describes the primary function of this device as being to manage a central dialing plan and follow programmed logic to route calls to their destination. A gateway is essentially an application layer routing engine. It analyzes an incoming invitation and makes a decision, after accounting for various factors, on how to best route SIP messages. This device assists in coordinating calls by initiating, updating or tearing down sessions. It often provides others services over and above session management such as authentication, location and network information. Interestingly, VoIP gateways exist in H.323 (H.323), MEGACO and SIP voice networks.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The gateway further provides translation of transmission formats and signalling procedures. It will accept calls using a specific protocol and recode the data for the destined end points. While this has performance implications, translation allows dissimilar devices to communicate using their respective signalling, codecs or protocols.

A gateway will often enforce some form of authentication. Authentication is not mandatory but wise to implement to ensure that services are not abused. It is common for devices to prompt the user for credentials before making any requests. A VoIP device can make a call or query the the gateway for information. If a service requires authentication, the gateway will challenge the end point and ask a for a set of credentials before servicing the request. The gateway will receive additional headers with subsequent requests, providing credentials and confirming the device's capabilities, location and user preferences.

A wide variety of services are made available to local devices or remote endpoints by the gateway. Depending on the complexity of the system it is not uncommon to distribute the services. They can be hosted on dedicated servers, reducing the load off a single intermediary. Common services provided to end points include *voice mail*, *unified messaging* , *call parking* and *conference calling* [35, 53].

Numerous gateways exchange call control messages during a communications session and are thus constituted as intermediaries. These make up the loosely coupled and distributed architecture in which each intermediary is an autonomous gateway [52]. This intercommunication between these autonomous intermediaries allows for sessions to dynamically locate and establish calls between remote end points.

This clarification of gateways is pivotal to our research as SIP gives no assurance of the identity of the intermediary. It will have become clear that the entire communications is at risk if even a single intermediary is misconfigured or maliciously used. The next section further extends on this risk by giving background to the application layer routing that threatens the communication path.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

4.4 Message Routing

4.4.1 Route

The Route header field is used to force the routing of a request through a predefined list of intermediaries. This strict routing ensures that messages are passed through certain proxies before reaching the destined party. The purpose of the Route instruction is to allow the sender to specify intermediaries that might assist in the routing, forwarding or control of a SIP session.

Routing is achieved by modifying the *Method* of the SIP message, allowing the intermediaries to process a message as normal. The proxy would thus proceed as if it received this modified request, and forward it through the standard forwarding mechanisms employed by the intermediary.

The Route header could, for example, be used to force messages through a Call Data Record (CDR) server or forward messages using the *tel* addressing scheme to a PSTN breakout.

4.4.2 Record-Route

The Record-Route header is added by proxies that wish to remain involved in future communication. A proxy wishing to remain on the path must insert a Record-Route instruction above any existing Record-Route headers. This header is preserved throughout the SIP session and ensures that an intermediary is included in the passing of subsequent messages. An intermediary can therefore override the actions of any remote party by adjusting or terminating a SIP session after it was successfully established.

Similar to the trick employed when processing Route instructions, the Record-Route headers are copied into the response as Route headers. Therefore, messages are sent to all intermediaries that requested to remain on the communication path through these implied strict routing headers. Responses are processed as normal, and returned to the source by adjusting the URI specified in the *Method*.

The Record-Route header can be practically used, for example, to ensure that messages pass through an intermediary for billing purposes. Similarly,

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

a prepaid billing system could terminate sessions once the initiating party has run out of credit.

The involvement of numerous parties in the communication bring with it various risks on privacy and trust. The SIP messages pass between proxies outside the control of the caller [62]. This arises from SIP having the ability to route messages independent of the governing networking topology. The resulting path which SIP messages take is initially undetermined. Unknown to the caller, the messages could be sent over unreliable or untrusted networks. Related work [35] points out that rogue proxy servers could "modify the signalling [by] adding *Via* headers". The destined device would respond to the initiator, and the messages are sent back over the dynamic path created during session initiation. Alternately, an "attacker could falsify the Via header in a request" and launch various denial of service attacks on devices or proxy servers [35].

The application layer routing logic could choose these paths based on various criteria. Very feasible are rules arising from least cost routing agreements, fault tolerant routes and government or corporation interconnect policies. This criteria influences the created path, yet other scenarios should be considered. Rules could be injected by compromised proxies or manipulated by malicious devices. The consequence of the aforementioned is that SIP messages would be directed through proxies and networks not previously anticipated. This naturally gives rise to certain privacy concerns [26]. Details such as source and destination of call can be logged, and various attributes about the session recorded. Calls, and potentially individuals, can be monitored by intermediaries.

In contrast to the proxies, it can be presumed that the user might want to modify specific *Via* or *Route* instructions. If a user consciously wants to avoid being monitored, the caller or recipient could manipulate the additional routing headers. Thus, a user could remove these headers to by-pass proxies or media controllers. This results in that a user could avoid billing or logging systems. Since the session would then no longer be communicated to all participants, it would not be possible to restore accurate records about the events.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

4.4.3 Response Codes

SIP responses are "... consistent with, and extend, HTTP/1.1 response codes" [71]. They are prefixed by a three-digit code followed by a descriptive phrase. Response codes allow for both machine and human interpretation, and are defined for all communication during session initiation. Response messages are sent, along the same path that they were sent, back to the caller.

Responses codes are categorized into provisional and final responses. They are further indicative of positive acknowledgements or unsuccessful attempts in establishing a communication session. Provisional responses indicate that an intermediary has processes the SIP request, and will pass back subsequent messages received from the destined party. Final responses indicate a conclusive state, upon which no further action is required. Section 21 of RFC 3261 [71] details the defined responses and respective codes.

The above mentioned parameters have been highlighted as they have bearing on our approach to cross-domain distributed security and trust.

4.5 Communication

The developments and enhancements to network infrastructure, paralleled with the rapid advancements in desktop and mobile computing, have brought about great change in information technology. Today's pervasive systems collect and communicate information about their configuration, the applications and the users. There is a need for security in VoIP as part of its design. Unfortunately, the standards were implemented without sufficient consideration for privacy yet we will review the efforts to secure the communication.

4.5.1 Security

Arkin et al. [6] correctly points out that most VoIP "related protocols were not designed with security in mind...". Some efforts have been made to add security mechanisms to the protocols, yet Arkin dismisses these for being inappropriate and impractical.

Section 22 of the RFC [71] details the SIP authentication process. SIP employs a stateless challenge-response mechanism for authentication. When a proxy or device receives a request, the proxy may challenge to verify the identity of the sender. The challenged device responds with the user credentials which are added to the message headers. The digest authentication mechanism employed provides message authentication and replay protection. It does not, however, ensure message integrity or confidentiality. An authentication credential set is showing here for reference.

```
Proxy-Authorization: Digest username="14169079479",realm="216.115.25.174",nonce="136885787",
                     uri="sip:01127117931486@atlas-east.vonage.net",
                     response="e260e929dc7d869a733d0bb462d97434",
                     algorithm="MD5"
```

In a managed VoIP network, a proxy (or collection of proxy servers) would manage the authentication within the network. The network would limit communication to external destinations ensuring that all calls are managed, monitored and controlled. Such a configuration would restrict devices from communication directly with remote parties, and thus direct all traffic through the gateway. An organisation with a managed VoIP configuration will be able to identify each internal device and broker all outbound communications. This allows for a tightly controlled communications platform in which authorization is integrated with internal authentication services (Databases, Kerberos, RADIUS). Goode [35] terms this the "administrative domain" which should employ secure routing policies, including the blocking of source-routed traffic. Authentication should be controlled within the administrative domain against which presented credentials can be verified. It must be noted that messages leaving the network no longer carry any credentials or identity descriptors.

Various approaches to securing SIP have been suggested through Transport Layer Security (TLS) [71] (26.4.3) and S/MIME encryption [71]. (23.1). TLS however "... offers strictly hop-by-hop security", which we will be investigating. We compare currently available security mechanisms in the paragraphs to follow and present how various attempts have been made to secure the underlying communication.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The intricacies and complexities of SIP are the reason for continuous debate about its suitability for voice communication. It is a highly discussed protocol with research attempting to address all its applications and implementation requirements. It was elected as the Session Initiation Protocol (SIP) in the core of 3GPP mobile networks because of its flexibility. The protocol meets the mobility requirements of 3GPP to support a large number of devices communicating over a cellular based data network. There is consensus on its robustness and scalability to support the emerging communication requirements. We agree that this protocol is suitably designed for a large, loosely coupled and distributed communications infrastructure.

4.6 Conclusion

This chapter introduced Voice over IP (VoIP) as the central topic of this dissertation. Whilst the previous chapters gave background on telecommunication and data networks, we detailed VoIP and SIP to introduce this new online communications paradigm. Our aim was to clarify its functioning to lead onto our own research. In particular, it would have become evident that control and session messages traverse various networks, the public Internet and are handled by many intermediaries. This has privacy implications which we will reveal in the chapter to follow. The motivation to investigate the privacy in VoIP is that we believe there are trust issues.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 5

Privacy in Communication

This chapter focuses on privacy in general and on the Internet. Our research examines what is meant by *privacy* and how it affects the individual exchanging information online. It is important to understand what users consider as personal information, and how their ability to control this information affects their level of privacy.

A general definition of privacy is "the ability of an individual to control the terms under which their personal information is acquired and used" [24].

In 1967, Westin [99] already defined privacy in terms of control. He noted that "the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others" is what defines privacy. A privacy advocate from that era was Charles Fried [31]. He was interested in the foundation of the right to privacy, particularly in electronic eavesdropping. Fried noted that "privacy is not simply air absence of information about us in the minds of others, rather it is the control we have over information about ourselves" [31].

This chapter plays a pivotal role in this dissertation. We start our research here by giving an account of the theories of privacy. This draws on the research in chapter 6 which justifies the need to protect privacy in VoIP, and we follow on in chapter 7 to propose a mechanism to assure privacy. Each chapter is independent, yet we will clearly show how these continue to build on our research.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

We first introduce the social context in section 5.1 before clarifying the legal standing of an individual's privacy protection in section 5.2. This leads us to contrast available public information with private details transported in VoIP in section 5.3 and 5.4, respectively. We briefly review existing privacy enhancing technologies in section 5.5, and conclude with section 5.6.

5.1 Social Context

This section gives background to the views society has of privacy. It is not easily possible to quantify privacy and thus we draw on related literature to support our critical review. Privacy is a complex topic yet it has "become the object of considerable concern" to society [31]. We will not however discuss VoIP here as the section to follow will contrast these social issues in light of the emerging digital, online communication medium.

Individuals do not view privacy uniformly and often have different types and different degrees of concern over their personal information. Their primary concern is the unauthorised use of their data, either within a managed network or illegally intercepted. Secondly, they have different degrees of concern, dependent largely on privacy preference and attitude. Culnan et al. [23] confirm through research that some individuals might feel strongly over a particular personal detail while others might be indifferent.

As more and more users utilise Internet services as part of their daily routine, a growing amount of information is exposed about them. The risk exists that remote systems and 3rd parties are able to identify and profile individual users. Technologies collecting private information have raised disputes as individuals want to protect their privacy from those who want to profit from the gathered information [102].

It was no wonder that a study such as the one undertaken by the Federal Trade Commission in 1998 found that the majority of e-commerce businesses "had failed to adopt even the most fundamental elements of fair information practices" [23]. A Business Week/Harris Poll [83] found that over 40% of online shoppers were very concerned about the use of personal information, and 57% wanted some sort of laws regulating how personal information is

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

collected and used. Fisher [29] reported that individuals did not feel that their information was being used wisely. He found that over 40% of web buyers surveyed said they had contacted a site to be taken off their database. Their concern was the misuse of their private information.

The right to privacy is for citizens and consumers to be "free from unauthorized intrusion". To assure a user that his personal details are not misused, "privacy involves the policies that determine what information is gathered, how it is used, and how customers are informed and involved in this process".

Westin [99] defined three separate groups: the marginally concerned, the privacy fundamentalists, and the pragmatic majority. These groups differ significantly in their privacy preferences and attitudes. The marginally concerned group is mostly indifferent to privacy concerns; privacy fundamentalists, on the other hand, are quite uncompromising about their privacy. They are concerned about their privacy, but are willing to trade personal data for some benefit (e.g. customer service). In Ackerman et al. [3], these groups were 27% marginally concerned, 17% privacy fundamentalists and 56% pragmatic majority. Indeed, in Ackerman et al., the concerns of pragmatists were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on Web sites [3]. His work confirms that recent studies show that concerns for privacy are "as prevalent in the online environment as [in the] physical-world interactions". Spiekermann et al. [81] noted a larger group of privacy fundamentalists and fewer marginally concerned in Germany. It should be noted that, despite these groupings, consumers still want adequate measures to protect their information from inappropriate sale, accidental leakage or loss and deliberate attack.

It is known that the largest extent of monitoring occurs within the private business sector, although governments have a vested interest in monitoring the activities of their citizens. Tuerkheimer details the "underpinnings of privacy protection" [90] in a paper that details the motivations and reasons for such monitoring activities, considering the legislative background of developed nations. It is clear that the issue of privacy, specifically within the digital realm, remains a controversial issue.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The academic ways of analysing privacy have merit and draw on fundamental beliefs to protect an individual's privacy. To achieve this often requires government support and legal protection, striving to protect the individual at all times. At this point privacy becomes a highly discussed topic with debates often turning heated. This is, however, not within the scope of our research and should be left for the philosophers to debate. For completeness we will briefly touch on the legal protection that exists.

5.2 Legal Protection

In addition to privacy, which is a social issue, individuals also require legal protection.

Originally set out in the American Constitution, the Fourth Amendment stipulated that the "right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated" [90]. This fundamental right became more difficult to manage in the emerging digital age where information flows freely. Tuerkheimer [90] applauds the many countries that over the last two decades have adopted a variety of strategies to achieve meaningful protection. The Organization for Economic Cooperation and Development (OECD), for example, defined a set of privacy principles more than 20 years ago. The aim was to strike a balance between the need for the free flow of information and the fundamental human right to privacy. Commonly known as the *OECD Guidelines*, they were recognized by all OECD member nations, including the Europan Union (EU) and America. They are, however, not legally binding and interpreted differently by the various member nations.

The greatest progress was made by the EU. They drafted the EU-Directives 95/46/EC on personal data protection and 2002/58/EC on privacy in the electronic communication sector [60]. The EU created comprehensive guidelines to address location information, the presentation of call identification, data traffic and specifically unsolicited communications. The EU focuses on the rights of individuals, often citing that attempts of communicating are only allowed once "subscribers have given their consent" [60].

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Even though the EU had drafted these new policies, they still had to be adopted and implemented. As with most aspects of ensuring privacy, the EU places enforcement in the hands of governmental authorities. These, however, have limited resources "to seriously impact the vast volume of fraud that occurs in cyberspace, let alone pursue misuses of personally identifiable information" [10]. This makes it difficult to take action against any privacy breaches.

Brandeis [96] noted that the fundamentals of communication privacy are discussed in light of the invasion thereof, thus breaching an individual's "right to be left alone". Monitoring telephone communication implied that "the privacy of persons at both ends of the line is invaded" [96]. The implications of tapping a phone line would not only compromise the privacy of the individual being monitored, but further that of every person whom he may call or who may call him. Brandeis motivated that an individual's right to be left alone was "the most comprehensive of rights and the right most valued by civilized men" [96]. It was through this that in the early 20th century legislation was introduced specifying the need for a court order before being allowed to tap a phone line.

Arkin et al. [6] are of the opinion that "privacy and security are not being correctly balanced with what is technically feasible". This poses great challenges as large amounts of information are already in the public domain, and cannot be easily controlled. We will examine this in more detail in the section to follow.

5.3 Public Information

The above social and legal discussion on personal information raises the question: what do individuals consider as personal? Further, when do individuals consider personal information as private, and at what point deem a breach of their privacy?

We answer these questions through comparative research on related communications technologies. The motivation for this investigation arises from the following discussion on *public information*, specifically presence and avail-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

ability. For this investigation we draw on user behaviour, rhythms and presence which manifests itself in Instant Messaging (IM). Our research found that a fine distinction exists between deducing presence information that aids individuals in finding opportune times to interact, versus giving away too much detail about the user.

Context-aware services can share real-time cues about individuals and opportune times to starting, maintaining, and ending communication sessions. Monitoring systems can be developed into more advanced mechanisms that go beyond simply indicating a user's presence. They attempt to predict a user availability and status based on a user's historic behaviour. Such monitoring systems gather data to model a user's behaviour and indicate an assumed availability. Prototypes [11] have been developed to demonstrate how these would effectively integrate into the workplace, and develop a kind of awareness of subscribing users.

Presence is a unique and compelling feature of IM systems today, but it currently indicates only whether a person is reachable. It perfectly compliments an IM service, allowing others to be informed when a user comes online or their status changes [15]. Presence does not consider the time vector and only indicates the current status of a user. Effective communication however requires far richer presences information of current and future reachability, context, and availability.

In looking at current IM systems, Tang et al. [86] looked at how the information in a system can help coordinate to future contact when one person is trying to reach another. The team of researchers performed a detailed analysis of over 21,000 IM conversations involving 437 users, attempting to model their behaviour and interactions. They continued their research in an attempt to find more effective ways of exchanging information, particularly on a individual availability for discussions. They found that it would be helpful to know "whether the user has a currently scheduled appointment in their online calendar or is engaged in a phone call", indicating more opportune times to make contact.

It is important to differentiate suitable times at which to disclose presence, location and availability information. These factors by themselves do

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

not necessarily compromise a user's level of privacy, yet simply enhance the communication with temporal information.

However, the information analysed and processed through inference algorithms could allow for the creation of rhythmic patterns. Systems are being designed to "establish patterns of presence" to model user behaviour [91]. Begole et al. [11] analyzed awareness histories of distributed groups and found it possible to model an individual's behaviour. He motivates that "awareness information over time could be used to infer rhythmic patterns that would be useful in coordinating distributed group work". An inference attack could draw on a user's historic presence and predict possible future events from recurring, for example work absenteeism or departure times.

Awareness systems, however, must assist users in understanding "the tension between their desires for privacy and [disclosing their] availability to others". These advanced systems "should allow users to control the extent to which they wish to present full details about their context versus an abstract inference of their availability" [86]. Tang notes that attributes are examples of the growing requirement for "the sharing of awareness information that infrastructures for future communication tools need to be capable of supporting".

Our concern is that IM, presences and availability will play a greater role in ubiquitous and pervasive computing. Users need to understand and trust the control they have over their information.

5.4 Privacy in VoIP

At the start of this chapter we cited theories advocating that users should have greater control over their private information. We then illustrated how instant messaging systems draw heavily on intrinsic evidence of the communication to model user behaviour. The stark contrast between theorists jousting for stricter controls and the flexibility of technology to breach privacy became clear. This section extends this research to VoIP, and discusses privacy aspects considering that this is a new and emerging technology.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

In conventional telephony, tapping into a line to eavesdrop requires physical access to a wire. More sophisticated attacks involve penetrating a switch, yet this greatly increases the malicious user's risk of discovery. It makes the attack "complicated because [the attacker] needs to install and operate the wiretapping software on the exchanges without being detected". However, intruders in the past have successfully exploited the network on a significant scale. [65].

In VoIP the opportunities to intercept a call are far greater. The technology is often implemented without sufficient understanding of the security and privacy implications. The communication is shared over a common medium and often carried over the same logical portion of the network. Using existing network sniffers it is notably easier to intercept both control and voice traffic. Well known tools such as **Wireshark** or **tcpdump** make it possible to capture and extract this information from a SIP session, Session Description Protocol (SDP) or RTP stream.

Communicating over public or shared infrastructure can unknowingly expose private information. By engaging in a communications session with a remote party, the possibility exists that private details are revealed or sensitive information exposed.

Arkin [6] confirms our views that a "malicious party can take advantage of multiple attack venues". The network "elements and network components pose a greater risk of misuse" than traditional telephony. These risks can be attributed to the infrastructure and underlying signalling technology employed. A few of the risks are inherent to the traditional telephone network. Examples of this are wire tapping or line abuse. A far larger number of vulnerabilities and security weaknesses exist in IP networks. These are a result of the distributed nature of the network and the limited control any single party has over the infrastructure. Numerous risks trouble the network ranging from software exploits such as viruses and trojans, through to network layer exploits involving traffic redirection and denial of service. Third and lastly, there are many yet undetermined risks exist which are specific to VoIP.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The aforementioned risks in VoIP stems from the fact that information about users and their actions is communicated to various parties during information exchange. Some critics [6, 87] have raised concerns that private information is transmitted (insecurely) and is attainable without much difficulty. Users can no longer assume that they are anonymous when using online services.

Not all data transmitted can be treated as the same. It is important to differentiate the type of information transferred, which can be split into the two types: content rich data and the signalling required for communication. An example is Skype which draws on a video feed for content, yet uses underlying signalling to transmit the data stream. A user can choose his preferred application, yet not control the underlying communications [25].

Signalling information is required for two parties to communicate. In contrast to what could be debated as private information, devices must share configuration or exchange predefined settings. Systems and devices often depend on additional information about the user to enhance the user's experience. An example of this is alternate contact details, location, pseudonyms, preferences. It is therefore extremely difficult to evaluate what is considered private and conceal this information without hindering the communication mechanisms.

Signalling is almost always based on a common standard. It is usually not a proprietary implementation by any vendor, but a protocol created by a standards body (IETF, Institute of Electrical and Electronics Engineers (IEEE), GSM). The nature of such standards is that weaknesses in the protocol will be present in all implementations. We note this as this is the risk that exists in the signalling.

A further point to stress is that most protocols are extensible. SIP for example (similar to HTTP) will freely transmit any additional information placed in its headers. The protocols are thus capable of transmitting information over and above the minimum required instructions. This extensibility has been provided in an attempt to future-proof the protocols at the risk of the unknown.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

When using information and communication infrastructures and applications, the users personal data is exposed at various intermediaries. This can easily be accumulated to complete profiles of the users communication, habits, preferences or movements. Such privacy risks are significant, especially for users of location-based or context-aware services [25].

Culnan [23] argued that privacy concerns are a critical reason why people do not go online and why they provide false information. Users feel that these risks are inherent to online communication, and more fundamental in that they do not have sufficient control over the medium. These concerns can be mitigated through technology solutions that enforce stricter control.

PET have been developed in an attempt to protect a user's privacy. These technologies vary in their effectiveness to provide the user with an acceptable level of privacy. Some are privacy mechanisms such as P3P, while other use encryption, information hiding or anonymity. These will be discussed next.

5.5 Privacy Enhancing Technologies

Ackerman presents four broad categories into which privacy has been tackled through technical enhancements. These categories are encryption and security mechanisms, anonymizing mechanisms, infrastructures, and labelling protocols [2]. The discussion focuses on privacy in pervasive environments, paving the way for a next generation solution to controlling privacy. In related work, his research confirms that users greatly welcome such enhancements [2]. Drawing on these categories we investigate these PET.

An early understanding for Privacy Enhancing Technology (PET) according to Burkert [14] was that these are "technical and organizational concepts that aim at protecting personal identity". PETs could be described as guidelines for privacy protection, either through technical or organisational functions.

Various mechanisms exist that attempt to protect an individual's privacy. Some approaches include using pseudo-identities [63], encrypting sensitive data [71] and information hiding [62]. PETs attempt to provide individuals with an acceptable level of privacy.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

In technical terms, PETs can be viewed as technologies that aid individuals in controlling the amount of personal information they disclose when exchanging information online. On this basis the next paragraph briefly discusses mechanisms to protect a user's privacy when using VoIP.

Our aim is to show that such PETs for VoIP can assist in protecting a users privacy. However, the practical implications of using PETs and the limited benefit make them ill-suited for practical use.

5.5.1 Anonymising Proxies

The primary feature of an anonymising proxy is to offer connection anonymity. Although frequently used in web browsing, a comparable solution could facilitate privacy in VoIP. The proxy would act as the first-line hop, authenticating the user and acting on his behalf. This would achieve caller anonymity, allowing an individual to subscribe to such a service. This anonymising gateway could further conceal sensitive private details of the called party, similarly to JANUS providing sender anonymity [70], through the removal of identity information from the SIP headers. An anonymising proxy would provide plausible deniability to create sufficient doubt that the proxy was not the source of the original request. This is achieved when using a PET such as *Polar* to ensure that the communication ensures *forward-secrecy* even if the path is compromised [89].

There are, however, plausible hindrances to such an implementation in VoIP. The proxy would have to implement TLS between itself and the authenticating user agent, an implementation often not supported by a hardware telephony device. Secondly, an organization would have to allow the SIP messages to traverse its boundaries, passing messages through a firewall and possibly circumventing mandatory proxies; something unthinkable from within a managed network. A further issue is that once the engaging parties have established an end-to-end communications path, there is no guarantee that the data passing between them (for example audio) is transferred either directly or securely to the anonymising proxy. This limits the possible value such a PET would add to an individual.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

5.5.2 Identity Concealing Gateway

An option is to masquerade the details of the source through official methods of translating user details. This is similar to network address transaction (NAT) in firewalls where the source addresses are never exposed to the outside world. An Identity Concealing Gateway would therefore implement logic to perform this masquerading.

The suggestions by Peterson et al. [63] on identity management appeared in a draft RFC in 2005. They presented their thoughts on how a users privacy could be hidden behind anonymous values sent to the destination. Essentially, they envision an intermediary facilitating the communication and masquerading the users details.

The primary concern is that a PET such as an Identity Concealing Gateway would actually hinder efficient communication. Certain information is removed from the messages which might be important to the call. The destination cannot correctly validate the presented information as it was altered en-route. We therefore do not believe that the methods presented by Peterson et al. [63] would provide a suitable privacy solution. The issue remains around control and thus our research shall continue to address privacy through message validation at each intermediary.

Users assume that using (or subscribing) to a PET gives them direct control over revealing their personal information. This is because PETs offer new options on what information to disclose during an online transaction. It gives the user an alternative which the user might not otherwise have. In part, this emerges from the fact that the user has a choice about what to present and how to use the PET.

Herman et al. [87] argue that "providing privacy-enhancing technologies (PETs) that seem to promote individual control may actually blur the need for stronger privacy protection, not provide it." They question whether privacy is increased and stand by their claim that "PETs, though important tools, are not adequate to fully protect personal privacy".

Considering the views of Herman et al., one has to challenge Burkert on his motivation that PETs give users direct control over their personal

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

information. Even if a user is given more control, it does not mean that these tools provide adequate privacy protection. Users are often not entirely aware of the implications of the information they are disclosing.

5.6 Conclusion

This critical review of privacy arose from inherent lack of security in existing protocols, and the methods of protecting sensitive information. This obviously now raises the question of "how private is a user's communication" and "what control do does the user have over his privacy"? The research in this chapter extends on our background of VoIP of chapter 4. The aim was to review privacy and describe why privacy in VoIP is a concern. We continue this investigation in chapter 6 to follow, specifically to classify the information leaked during communications.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 6

Information Leakage in VoIP

The growing dependence on technology by society brings with it various privacy issues. More and more people make use of intelligent communication services when performing their day-to-day activities [97]. They knowingly (and unknowingly) transmit large amounts of personal information, putting themselves at risk of being monitored.

Consider an incident reported in July 2007 in Greece which ended in tragedy. Vodafone found that software had been illegally implanted in a total of four of their voice call switches. The "bugging began sometime during the fevered run-up to the August 2004 Olympic Games in Athens" and remained undetected until 24 January 2005. The rouge code had been installed to create two parallel streams of the digitized voice. It was put in place to record one stream, and create another, being an exact copy, which was directed to an unauthorised destination. It was confirmed that the "software also routed location and other information about those phone calls to these shadow [destinations] via automated text messages." [65]

One technology that has the potential to considerably raise privacy concerns is VoIP, an emergent voice communications technology over the Internet. VoIP will eventually replace our current Public Switched Telephone Network (PSTN). VoIP is however still in its infancy. The implementation of services has not yet matured sufficiently to address the multitude of possible privacy issues.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

In VoIP, details of a session such as the participating individuals are visible to various intermediaries, proxies and end-devices. Profiling can be done through the analysis of information visible at any of the mentioned intermediaries. Individuals could be monitored and profiled. Records can be used to describe the behaviour of an individual, and mined for private information. This would make it possible to determine an individual's activities, habits and whereabouts. Any unauthorised use of such intercepted records is an infringement on an individual's right to privacy.

The risk to individuals is that their information could collected by targeted research, marketing or similar companies. The collection of information for customer relationship management (CRM) and business intelligence (BI) has developed into valuable practises [51]. Extracting personal information from VoIP sessions support marketing initiatives in directing and focusing their efforts on particular user segments or individuals. Further, they could aggregate the available information to summarise the collective activities for specific business purposes.

One has to ask if privacy is really an issue within VoIP. This is posed in trying to identify the particulars that are exposed when two communicating parties establish a SIP session. Is the information part of the session, or superfluous for VoIP communication? How can this be determined? These can be answered by analyzing VoIP, particularly SIP and its functioning in a real world environment.

This chapter highlights the privacy implications when communicating using SIP. We question the need for privacy in section 6.1. More specifically, section 6.2 takes into consideration the private details which are visible when messages are exchanged. We use the Freiburg Privacy Diamond [107] in section 6.3 to analyse the protocol and show that the exchanged details reduce an individual's anonymity. A communicating party can possibly be linked to an action, device, location and identity. There exists an obvious invasion of privacy which we present in section 6.4. We conclude with section 6.5, in which we motivate why adding identities to control the communication path will enhance user privacy.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

6.1 Concerns about Profiling

Privacy in VoIP services has received limited attention, largely due to more pressing technical challenges such voice quality [93], seamless mobility [93] and session management such as SIP [73]. Many privacy concerns trace back to the underlying session management protocol which is central to VoIP communication, and more specifically SIP. It will become evident in this section that SIP headers carry various private details. We present examples of SIP sessions, and highlight the headers revealing privacy related information.

VoIP commonly distinguishes between two types of a communication: a control channel and a data channel. The data channel is used to transfer the encoded audio stream between two remote parties. The channel is datagram-oriented by design and hence often uses UDP over TCP. The data channel is set up according to instructions received from the control channel during session initiation.

The control channel ensures that the data channel is established, maintained for the duration of the session and terminated at the end. It is used to exchange messages with the destined remote party, containing details about the source and destination, capabilities of the communicating devices and session information [73]. The control channel is used for what in traditional telephony is described as signalling. A protocol commonly used for the control channel is SIP [73]. SIP is the successor to H.323 [76] and has been adopted by the IEEE as the new signalling standard. A more detailed discussion of SIP is therefore appropriate.

An individual wishing to communicate using a SIP-enabled device would instruct the device to *call* a remote party, specified by either a number or an alias. Gartner predicts with great certainty that users will continue to use traditional numbering schemes in VoIP [30]. This numbering will allow for the use of the ITU-T's international public telecommunications numbering plan (E.164) [27] in VoIP. This will allow for the smooth transition from traditional PSTN to VoIP and ensure that every device is contactable. Since devices are no longer bound to physical locations, it would be impossible to *locate* the remote device without assistance from intermediaries.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

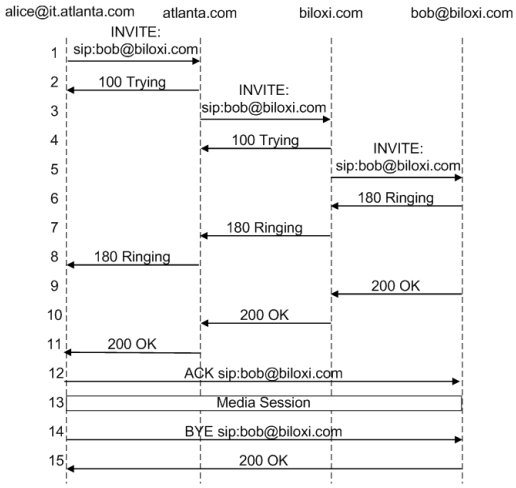

Figure 6.1: SIP Message Exchange

We refer to Fig. 6.1 to illustrate the steps involved in setting up a SIP session between caller Alice and remote party Bob. SIP initiates a session by sending an INVITE request (step 3). This invite is forwarded by a number of proxies (steps 3,5) until the final proxy is reached. Every proxy is only responsible for its authoritative domain, and messages not destined for it are passed on. In this example *atlanta.com* and *biloxi.com* are intermediaries responsible for their respective domains. This effectively allows for a hierarchical structure – for example: calls destined for Bob working in the human resources (HR) department at a company called *Biloxi* can be directed to proxy biloxy.com which subsequently forwards the call to proxy hr.biloxi.com. Therefore, proxies dynamically map out a route, from one proxy to another, before the INVITE finally reaches the destination.

This "loose routing" established a path which is used for the exchange of subsequent messages. Responses are sent along this path but in the reverse direction. Every proxy, only knows the previous and next proxy. Optimal routes are created, which allow for efficient passing of messages and fail-over mechanisms to ensure sessions are maintained. Call status messages, such as ringing (steps 6–8) and answered (steps 9–11), are routed back to the calling proxy.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Once the call has been acknowledged (step 11), a data channel is established between the calling and final proxy (step 12). Each proxy will interface with the end-devices; which in our example are operated by Alice and Bob.

Various attributes are exchanged during a *call* and stored in SIP headers. These attributes are useful to proxies, devices and users. Required headers are *To*, *From*, *Contact*, *Call-ID* and *Timestamp* values. The *To* and *From* headers are URIs identifying a device or user reachable domain (e.g. bob@hr.biloxi.com). Additional headers can be used to convey location, alternate contact numbers, device capabilities, codecs and firmware versions.

The VoIP communication paradigm bear little relation to existing PSTN networks. Telephony operators control the PSTN network, its interconnects and call routing. Whilst many individuals assume that their VoIP calls are private, few understand the implications which the signalling protocol has on their privacy.

6.2 Information Leakage

In this section we discuss possible sources of information leakage and details visible to intermediaries. We present the headers through which deductions about a user and his actions can be made. This argument is supported by the RFC 3261 [71] which states that "SIP messages frequently contain sensitive information about their senders". The RFC elaborates on the privacy of users and that it is possible to know with whom, when, how long and from where a user communicates.

We first discuss the explicit and implicit attributes which are exchanged during a SIP session. Our research then examine how this can be used to compromise a user's privacy in section 6.4.

While known security threats exist, this section highlights the privacy issues in SIP.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
INVITE sip:01127117931486@atlas-east.vonage.net SIP/2.0
Via: SIP/2.0/UDP pc33.intdev.co.za;branch=z9hG4bK776asdhds;received=192.0.2.1
Record-Route: <sip:p1.vonage.net;lr>
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>;tag=28491840-EE2
Call-ID: a84b4c76e66710@192.168.0.120
CSeq: 314159 INVITE
Contact: <sip:tozzi@intdev.co.za:5060>
User-Agent: <Motorola VT1000 mac: 000F9F466CD0 sw:VT20_1.1.16e ln:0 cfg:1097174/100282>
Content-Type: application/sdp
Content-Length: 142

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP logging.vonage.net
     ;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP pc33.intdev.co.za
     ;branch=z9hG4bK776asdhds;received=192.0.2.1
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>;tag=28491840-EE2
Call-ID: a84b4c76e66710@192.0.2.1
CSeq: 2 INVITE
Content-Type: application/sdp
Content-Length: 160
```

Figure 6.2: SIP Message with Headers

6.2.1 Explicit Attributes

SIP exchanges many messages during a session, thus ensuring that engaging parties can communicate. We define explicit attributes which are fact and which are defined by the protocol. These are connection-related properties, exchanged among communicating parties across various networks. These details are stipulated in SIP headers as shown in Fig. 6.2.

Each device requires an IP address to communicate giving some indication of its location on the Internet. IP address information revealed in the SIP header does not tie to a particular location, but does bear on a user's locality. It can be determined if a user is at work, communicating from a corporate domain, on a mobile or home network. It can be argued that this information carries little weight on its own, yet when tied to a user's pseudo-identity has greater implications.

A user must assume a pseudo-identity and use it when engaging in VoIP communication. This pseudo-identity is an address in the form of a SIP URI and comparable to an email address denoted by *alias@domain.ext*. Devices and intermediaries assisting in the session require this address to *resolve* the destination and communicate with the proxy responsible for the *domain*.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds;received=192.0.2.2
Route: <sip:bigbox3.site3.atlanta.com;lr>
Route: <sip:cdr-svr.atlanta.com;lr>
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

Figure 6.3: SIP Message with Route Instructions

The communication within a realm is often controlled by an authoritative proxy. A user has little control over what is communicated by the proxy, as this intermediary governs over the routes and session particulars. The SIP message can contain auxiliary headers that enhance the communication. A user might be reachable at more than one location and provide multiple contact points. These could be *sip*, *mailto* and *tel* addresses. While the latter are not mandatory, a device must convey how it can be contacted[71]. Individuals might, however, want to conceal their name, pseudo-identity or contact points. This is increasingly important when SIP messages are sent outside of the realm of the domain.

Depending on vendor implementations, devices might want to inform intermediaries of additional device-specific functionality. Since SIP is a generic implementation for session management, it caters for remote parties to determine a device's capabilities. A device might want to communication additional functionality such as support for video, presence information or mobility options. In our research we found that Vonage devices disclose the device model, its MAC address, software version and latest configuration.

Protocol and Services

The SIP RFC states there are six fundamental header fields for communication. They "jointly provide for most of the critical message routing services including the addressing of messages, the routing of responses, limiting message propagation, ordering of messages, and the unique identification of transactions." [71]

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.10.202:5061;branch=z9hG4bK-31f-c3d55-4b44
Record-Route: <sip:18003569377@216.115.25.54:5061>
```

Figure 6.4: SIP Message with Record-Route Instructions

The *Route* and *Record-Route* header specify paths over which a message should be passed. The *Route* only specifies a route for a single message, while the *Record-Route* instruction forces future requests to be sent along the specified path. These headers can be set during session initiation, or dynamically added once the *call* has been established. Our great concern is that these instructions can be set by any intermediary, and have no visible impact on the data channel.

The strong motivation for these headers is that these are required for call routing and decision logic purposes. The privacy aspects are, however, mostly ignored. The entire SIP message is passed between various, potentially untrusted, remote hosts. While these hosts are instructed to forward the request, they can record these headers and even alter the message path. In either scenario, the particulars of the user and originating network are vulnerable [95].

Networks

SIP places machine names, host names and device addresses in the header. Devices are specified by IP addresses or Domain Name Service (DNS) records, and could potentially reveal the network configuration.

The IP addresses of managed or corporate networks are often hidden from the outside world. They are masked by Network Address Translation (NAT) or connections relayed by proxies. However, SIP could expose details about the network and non-public servers. While these servers might not be accessible from outside the managed network, they reveal the network architecture and participating intermediaries.

This is illustrated in 6.4 where a participating proxy is exposed, and the internal IP address of this intermediary communicated to third parties.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Devices

A proliferation of hardware devices and VoIP telephones have emerged on the market. While there are governing standards, manufacturers can add additional information into SIP headers.

Devices communicate additional information about their capabilities. This makes it possible to negotiate on mutually supported functionality. An example of this is video capabilities, presents or directory integration. It further makes it easier identify and troubleshoot supported functionality.

The concern is that devices could reveal various details about the manufacturer, the hardware and embedded operating system. These devices could be fingerprinted [95] and potentially vulnerabilities easily identified.

A far greater concern surrounds audio codecs. In order for two (or more) devices to communicate, they will share information about their available codecs. This will be used to negotiate a commonly supported audio encoding algorithm. The open nature of the protocol would allow third parties to lists the available codecs and report on the employed algorithms. Certain codes such as G.729a are, however, registered as intellectual property and must be licensed. Querying a device for its supported codecs could be used in scanning the network, and reporting on legitimacy of implemented encoding algorithms. This clearly highlights it would be fairly simple to audit VoIP network without requiring physical access, or authorisation over the devices.

Location and Presence

The communication protocols implemented in VoIP are ideally suited to convey locations specific information, tied to a users presence or status. This presence can be described in terms of availability at a given location at a particular time.

Data mining techniques can be applied to the available information in order to determine a user's current presence. This can be used to establish patterns of presence through various learning approaches [91]. Inadvertently, the network could model a user's future presence as we discussed in chapter 5.

Within a managed environment, SIP devices would log on and off from an

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
INVITE sip:01127117931486@atlas-east.vonage.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.3:5060
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>
Contact: <sip:192.168.1.3>
Call-ID:3D2FC501-ECA1-4526-8257-C1FB36B56771@192.168.1.3
CSeq: 2 INVITE
User-Agent: <Motorola VT1000 mac: 000F9F466CD0 sw:VT20_1.1.16e ln:0 cfg:1097332074174/1002226282>
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 112
Proxy-Authorization: Digest username="14169079479",realm="216.115.25.174",nonce="136885787",
                     uri="sip:01127117931486@atlas-east.vonage.net",response="e260e929dc7d869a733",
                     algorithm="MD5"

v=0
o=- 3315231798 3315231798 IN IP4 192.168.1.3
s=-
c=IN IP4 192.168.1.3
t=0 0
m=audio 16386 RTP/AVP 8 0

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.3:5060
From: "Thorsten Neumann"<sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>
Call-ID: 3D2FC501-ECA1-4526-8257-C1FB36B56771@192.168.1.3
CSeq: 2 INVITE
Max-Forwards: 15
Content-Length: 0

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.1.3:5060
Record-Route: <sip:27117931486@216.115.25.174:5060>
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>;tag=28491840-EE2
Call-ID: 3D2FC501-ECA1-4526-8257-C1FB36B56771@192.168.1.3
CSeq: 2 INVITE
Contact: <sip:27117931486@216.115.23.17:5060>;rtpupdated=-
Max-Forwards: 15
Content-Type: application/sdp
Content-Length: 160

v=0
o=CiscoSystemsSIP-GW-UserAgent 9397 7747 IN IP4 216.115.23.40
s=SIP Call
c=IN IP4 216.115.23.40
t=0 0
m=audio 12712 RTP/AVP 0
c=IN IP4 216.115.23.40
```

Figure 6.5: SIP Header Revealing Device and Software Version

```
Protocol Info
RTP      Payload type=ITU-T G.711 PCMU
```

Figure 6.6: Ethereal SIP with SDP Packet Declaring G.711 Encoding

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

authorative proxy, indicating a users availability. Once further augmented with user-specified availability information (such as *busy* or *do not disturb*), one could detail a user's behaviour.

The intent of the communications infrastructure is to foster better collaboration and optimal user interaction. This has obvious privacy implications. While this is beneficial within a collaborative environment, such an analysis could reveal confidential information about any user's activities. In our analysis using the Freiburg Privacy Diamond (Freiburg Privacy Diamond) it will become clear how location-related information in particular compromises a user's anonymity.

Call Data Records

The sample headers presented in this chapter reveal various details about the communicating parties. Our great concern is that this information is passed between various parties by means of the application layer routing performed in SIP. Not only do these particulars pass between designated proxies, they also transgress various network boundaries.

Each session will result in *call data records*, a summary of the call details to record the event. These will be stored as reference and proof that the communication took place. However, these will not be collected in a single, central repository unlike PSTN networks.

Various intermediaries, proxies or devices can keep a record of these calls. Call data records therefore have a notable implication for an individual's privacy.

6.2.2 Implicit Attributes

Other more subtle deductions can be made by watching the transaction within a session. Next we identify how particulars about a user can be inferred from these attributes.

The presented list of attributes are fact, while further conclusions could be drawn through observing a progressing session. Implicit properties are tacit yet could be deduced from the SIP headers. Numerous messages are

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

exchanged during a session, as illustrated in Fig. 6.1, and can reveal subtle behavioural attributes. We agree with RFC 3261 which notes that there are also less direct ways in which private information can be divulged. Two important factors are those of time and the duration of a session.

Observing SIP messages exchanged at a particular time has a bearing on the user's location. A user could have left the office, yet still be communicating thus implying that he or she is possibly at home.

Secondly, the progression of a session and its cumulative duration indicate the nature of the call. Many longer calls after work could be assumed to be personal, while those with a duration of less than a minute are more likely work-related. This is comparable to the usage patterns found in fixed and mobile phone usage [45, 59] and instant messaging [50].

The final state of a call plays an important role. This state can be drawn out of responses returned by the destined device. SIP response codes are consistent with, and extend to HTTP/1.1 response codes [71] and allow for both machine and human interpretation. These give insight as to how a session was redirected or terminated. States such as *Redirected*, *Moved*, *Busy Here*, *Do Not Disturb* or *Rejected* are communicated in system-generated responses. These will indicate a conscious action of a user when being contacted.

Section 13.3 of the now deprecated RFC 2543 talks specifically about privacy in SIP. The document notes that "location and SIP-initiated calls can violate a callee's privacy". This includes revealing alternative contact numbers which could infringe on privacy and be of concern to the organisation.

The aforementioned attributes have been tabulated in 6.1. These either visibly reveal details about the user (or device) and allow for the analysis of implicit attributes.

In the section to follow, we assess the implications of the attributes, and how they breach an individual's privacy. The Freiburg Privacy Diamond is used as a model to show that an attacker can launch an inference attack on a user. This will confirm that users can indeed be profiled and their behaviour modelled.

We pay specific attention to the SIP headers and analyse the information that could be acquired and subsequently retrieved from the headers. Fur-

thermore, the inadequacies of the SIP protocol allows intermediate proxies to monitor and alter a SIP session. This raises the question about the method in which SIP operates and the amount of personal information that is *leaked*.

We investigate the SIP message exchange, in particular SIP headers, in light of the mentioned privacy concerns. We explore what sensitive data is exchanged and how callers can be linked to a device or location. A proxy might have no knowledge about the source or destination, but consider the impact of aggregating messages from multiple proxies and different sources, which could lead to identifying and profiling users.

6.3 Freiburg Privacy Diamond

We apply the the Freiburg Privacy Diamond [106] to VoIP. This model captures the essence of anonymity with regard to device and user mobility. We can then model and analyze the anonymity of a user.

The Freiburg Privacy Diamond considers four entities which impact on the user's level of privacy. They are: the action itself, the device, the location of the device, and the user, visually (see Fig. 6.7(a)). These different entities are related. The user performs an action, using a device at a particular location. In order to achieve anonymity, an attacker should not be able to link these entities when observing a single message, or complete session.

(a) *Related entities* **(b) *Multiple relations***

Figure 6.7: The Freiburg Privacy Diamond

The model has been extended to describe the additional challenges faced in achieving anonymity in pervasive computing [107]. It shows how communicating devices must protect privacy through working together in achieving

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

anonymity. It is well suited to analyse information leakage in SIP communication.

Assessing these entities, an attacker would have to reveal the relations between a user and his action to deduce the identity of a user. Depending on the information captured, the attacker could correlate a user to a device or location. Any such relationship would breach the user's privacy by revealing the action performed on a device and at a specific location. The flexibility of SIP would allow a user to utilise any device from any location.

A user would be reachable within close proximity of a device. He would further perform actions using a capable device. The user also could make use of more than one device. A device could be mobile (cellphone or softphone) or bound to a location (as is the case with traditional telephones). It is assumed that the user is in close proximity to the device. While this creates an immediate relation between the user and his location, it does not imply that the user can be identified. The semantics of the Freiburg Privacy Diamond require an attacker to determine which user or which device performed the action. Here we apply the Freiburg Privacy Diamond to VoIP communication.

In order for a user to be *contacted*, it must be possible to locate the device being called. Considering that the utlised device will authenticate on the user's behalf, an implicit relation between the user and a device is created, contravening the Privacy Diamond entities. The exchanged information could also reveal the user's location.

Referring to the Freiburg Privacy Diamond, we can confirm the following: there exists a physical connection between the user and the device. The device however is in most cases not independent of its location. There is further a clearly *visible* sequence of events in which the model classifies these as actions. The user initiates the action, and the supporting systems will honour this. These could respond with acknowledgements or further instructions for the session to establish. The behaviour of the devices and intermediaries could result in multiple relationships as illustrated in 6.7(b). It complicates that matter yet does not lessen the implied relation between the four entities.

Two situations arise when a user is *contacted*. In the first scenario the user

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Privacy Concerns			
Type	Attribute	Information Leakage	Privacy Implication
Explicit	Protocol	Medium	Low
	Services	Medium	Low
	Networks	Medium	Medium
	Devices	High	Medium
	Location	Medium	High
	Presence	Medium	High
	User	High	High
Implicit	Duration	Low	Medium
	Time of day	Medium	Medium
	Frequency	Low	Medium
	Status	Low	High

Table 6.1: Sensitive Details Revealed in a SIP Session

is contacted and accepts the incoming call. The SIP session is initiated in which particulars about the session, therefore the user, are exchanged. This includes the user's name, direct contact details and device used. Further, particulars about the user's current location, presence and availability could be deduced. Redirection instructions such (181 Call Is Being Forwarded, 300 Multiple Choices, 301 Moved Permanently, 302 Moved Temporarily or 380 Alternative Service) communicate this information as part of the response.

An alternate scenario is when the user can not be located or does not accept the incoming call, thereby communicating back a state of a device or a conscious action of a user. If the user is not present at the time (480 Temporarily Unavailable) the resulting SIP headers would reveal alternate contact numbers or locations at which the user could be reached. In contrast, a conscious action would indicate that the user was contacted but unreachable (486 Busy here, 600 Busy everywhere) or declined the call (603 Decline).

Reverting to the Freiburg Privacy Diamond, the user can therefore be tied to the action, and can be associated with a device and possibly a location. Further assumptions can be made through observing the session, and the extracting the implicit attributes.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

6.4 Profiling

We consider profiling of a VoIP user and the possible privacy implications thereof. The Freiburg Privacy Diamond provides a model through we we have shown that a user's privacy is at risk. The Voice over IP Security Alliance [5] remarks that VoIP "faces different threats than other Internet applications, triggering unique security and privacy concerns." Profiling in VoIP is the process of analysing personal information found in call data. We have introduced explicit and implicit attributes as two sources of personal information found in call data.

During the establishment of session, a proxy could unbeknown to the caller, insert a *Record-Route* header. This instructs the participating devices to relay subsequent SIP messages through the proxy for the duration of the SIP session. The host specified in the *Record-Route* header need not be the proxy handling the SIP message. An simple example to illustrate the risk of information leakage is where *eve.com* would forward the SIP INVITE with this additional *Record-Route* header. While *eve.com* should no longer play a role in the session, the proxy will receive all messages and event updates exchanged between the communicating parties. As indicated in Fig. 6.1, neither Alice nor Bob are aware of this intermediary.

SIP devices and proxies additionally rely on the *Route* directive to pass messages to specific hosts for processing and routing. A misconfigured or compromised proxy can manipulate messages without consent from the user, such as injecting additional headers. The SIP header will force the message to be forwarded to a specific intermediary before reaching the intended destination.

The possibility exists where *eve.com* inserts a *Route* instruction to have the current SIP message forwarded to *profiling.com* . This allows the next en route proxy to collect the Explicit Attributes described in Section 6.2.1. Further, one could consider this in combination with the aforementioned *Record-Route* header. This gives *profiling.com* the ability to monitor and profile the user, correlating the actions and ability to deduce the implicit attributes described in Section 6.2.2.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The users of a SIP session are not in control of the communication environment, often restricted to the interface of the device (or softphone). The communicating parties might not be aware of intermediaries logging and recording call control messages. While the mentioned records are specific to call control events, they expose a great amount of detail about a user.

With the growing adoption of VoIP, profiling becomes an increasingly dangerous threat. Analysing a collection of calls performed or received by an individual could expose a substantial amount of information about a user's behaviour, habits or preferences. Whilst these threats are currently minor, one should consider a case where VoIP becomes a truly ubiquitous communications technology.

One could consider the case whereby many household, workplace and public devices are networked and support IP communications. Not every device needs to be a communications device. It could be used to inform an individual if his phone is ringing or if messages are available. If this were the case, more personal information would be available.

Further research is required to study the implication that a widespread acceptance of VoIP has on personal privacy. An interesting case is a probable future scenario whereby communication is possible from anywhere and by anybody using his own unique pseudo-identity or telephone number. We have only briefly touched on the implications hoping to stimulate ongoing discussions.

6.5 Conclusion

Our research aimed to show that information is leakaged in VoIP and specifically SIP which affects users' privacy. Personal details are exposed and thus compromise user anonymity. A user is therefore not assured of a sufficient level of privacy when communicating over the Internet. We then went on to show that a user's action, the device used, location and identity can be correlated.

In this chapter we identified the information revealed when communicating with a remote device. We used The Freiburg Privacy Diamond [106] to

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

substantiate this argument.

The main arguments of this chapter were presented at TrustBus 2006 in support of the body of this research. The chapter drew from the paper discussing *Information Leakage in Ubiquitous Networks* by Neumann et al [84]. We have now built on this work to qualify the type and magnitude of the risks of user profiling.

The trends indicate that the VoIP will increasingly dominate cable telephony and start replacing traditional telephone lines [76]. This raises concerns about a user's privacy as this pervasive technology starts replacing our existing communications infrastructure.

Chapter 7

Enhancements to SIP

In order to address the proprietary vendor implementations, the Internet Engineering Task Force (IETF) drafted a comprehensive communication protocol in 1998. They defined protocols that assist in the establishing of VoIP communication, yet clearly separate the signalling from the data. They created the SIP protocol and underlying signalling mechanism. It was designed to work in a distributed fashion, and simply coordinates the data exchange between communicating parties.

The greater research community recently convened to propose enhancements to SIP for a new mechanism to certify the identity of a caller [63]. They wanted to create a means to provide a level of certainty amongst communicating parties of each other's identities. The identity of a remote device would therefore be assured, and changes to an individual's details could be validated. This noteworthy addition to SIP did not, however, guarantee that all intermediaries assisting in the SIP session are trustworthy.

The previous chapters built on the caveat of privacy which is our primary concern. We highlighted the risks and strongly motivated for greater transparency on identity information of intermediaries.

The contribution in this chapter is to present a mechanism to certify the intermediaries. Our approach is to assert the identity of intermediaries which assist in establishing a SIP session. Thus, the intent is to create an acceptable level of trust over the chosen path during the initiation of a SIP session. This

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

is achieved through certifying the intermediaries and any changes which are made to the messages *(*en route).

Originally in chapter 4, we explained the headers used in SIP messages and their purpose. The research thus far has shown that there is concern for the content and transfer mechanisms used in SIP communication.

We now follow on from the various discussions that have arisen about the integrity of SIP headers, and give background to our proposed enhancements. Firstly, we present the enhancements in section 7.1. Section 7.2 elaborates on these concepts and details our implementation of securing SIP messages. The adjusted state of messages in transit and methods of certifying the participating intermediaries are explained in Section 7.3. We highlight the gained trust and how our contribution assists in securing SIP in Section 7.4

7.1 Proposed Enhancement

In order to ensure that the SIP messages remain unchanged, a new method of securing specific message headers [63] has been proposed. The motivation for securing the headers is to ensure that the content of the SIP message itself has not been modified in transit. This section will explain the proposed enhancements, which leads us to our research of certifying the intermediaries involved in a SIP session.

A device initiating a call creates a SIP message and passes it to a proxy server. Depending on the destination, the proxy will in turn pass the message on. However, of concern is the integrity of the message once it has been forwarded. The next-hop proxy determined through resolution and routing mechanisms cannot be assured that the content has not been changed. Thus, it and any consecutive proxy (or devices) cannot ascertain whether any of the presented attributes are true. This raises concern about the possible manipulation of SIP messages resulting in deception, abuse or denial of service. The implication is that plausible scenarios such as the construction of deceitful messages would arise. This would not only interfere with a caller's credibility, but also raise doubt as to the trustworthiness of the originating network. The problem is that this could materialise as the abuse of VoIP services compa-

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

rable to the previously unexpected creation of SPAM in email [21]. Industry has hypothesized about SPAM in VoIP and accordingly termed this abuse of VoIP services as SPIT [17]. This issue would have to be addressed before the technology is too widespread to be secured.

Two new headers, namely *Identity* and *Identity-Info* have been proposed in [63]. These enhancements to SIP do not require changes to any existing implementations, but allow for proxies (or devices) honouring these extensions, to establish a common level of trust. It is assumed that a device is authenticated to an authoritative proxy server. Thus, the proxy server represents the device within the domain it is communicating in. The device will communicate through this proxy, leveraging off the routing, rules and defined policies.

The *Identity* header is a digest string computed from specific values within a SIP message. This string is a hash over important attributes, and signed using a X.509 certificate. The digest string is written into the SIP message before being sent on.

$$Identity = sha1\,WithRSAEncryption(attributes)$$

The calling device will provide the necessary attributes to initiate a session. It therefore presents the source SIP URI, the destination SIP URI, the *Sequence Number*, specified *Caller ID* and the *Method* headers. These details are sufficient for the proxy to process the SIP message, and attempt to establish a session.

$$attributes = source : destination : callid : method : timestamp : contact : message\ body$$

The proxy must be configured to hold a certificate valid for its authoritative domain, and use this in signing outbound messages. The certificate must be valid for the represented domain, and match the host name of the proxy handling the message. The hash and signature is computed using the sha1WithRSAEncryption algorithm over the canonical string.

A remote party might not know of the caller, and would want to verify the presented identity and integrity of the message. In order compute a

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

comparable hash, the remote party must retrieve the authoritative proxy's public keys. The proposed enhancements draw upon the *Identity-Info* header to assist in describing the location (URI) of the certificate.

This new mechanism of certifying a caller's identity allows for the true source of this message to be determined, and the integrity of the presented attributes verified. It ensures that all headers remain intact without hindering the end devices in communicating. It further shifts responsibility away from end devices, and makes it impractical to modify these headers once a digest has been computed.

There are many benefits to confirming a user's identity. Systems can trust the caller and can be built to securely allow to access confidential or private information. The caller no longer has to audibly confirm his identity, nor confirm secrets using DTMF inputs. Misuse of telephony services would be reduced as users are aware that their session identity is managed by an intermediary. Although this has bearing on a user's privacy when communicating, he is assured that his details are not maliciously intercepted. It must be noted though, that this mechanism only focuses on the caller.

In this section, we described the enhancements to SIP in order to certify a user's identity. In the section to follow, we apply these principles and extend these to intermediaries. The aim is to provide a way of certifying the intermediaries' handling of SIP messages in transit.

7.2 Identify Assertion

We detail how we propose certifying changes made to a SIP message in this section. The attributes deemed necessary to ensure integrity are described, and the implementation of our proposed mechanisms explained. It requires that proxies correctly sign the traversing messages and simultaneously underwrite the changes made during transit.

The obvious concern with SIP messages is that they dynamically establish a route to the destination, thus directed over a previously undetermined path. The routing headers are inserted into the message, as shown in Fig 4.1. To avoid a rogue proxy modify the signaling as Goode [35] points out, one has to

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

establish trust in the SIP network. Yet since the route cannot be predicted, we propose that each proxy identify itself en route. This is achieved by appending a digital signature to the SIP message before it is forwarded. The *Application Layer* routing headers should not be modified when handled by the next proxy, and the signature will ensure this.

A intermediary handling the SIP messages is required to insert a *Via* header in order for the message exchange to continue. SIP prescribes that the version, protocol and host name of the proxy are recorded. Our mechanism allows us to ascertain whether a proxy claiming to have handled the message, is indeed the true intermediary. This is achieved through the addition of a digest string linked to this intermediary.

The proxy must confirm that it adjusted the request, inserting its particulars in a *Via* header. Policy might have the proxy inserting logging or routing headers, and these must additionally be certified. Proxies process these headers top-to-bottom — thus any new details are inserted at the top of the request. If each proxy signs its inserted *Via*, a trace of modified *Via*, *Route* and *Record-Route* headers can be produced.

Considering that the original headers produced by the caller and particulars about the session have been signed into the *Identity* header, it is not required for the hashing to consider all SIP attributes. This is a fair performance improvement since only the *Identity* header must be included, when signing the concatenation of newly inserted headers. The signature would similarly be formed through a digest computation.

$$Signature = sha1WithRSAEncryption(attributes)$$

$$attributes = adjusted\ Method : inserted\ Via : inserted\ Routes : \\ inserted\ RecordRoutes : Identities$$

The *Via* header must include this signature, as well as the path to its public X.509 certificate. The header structure of SIP messages allows for this through semi-colon separation of attributes, and thereby inherently caters for these extensions.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
Via: SIP/2.0/UDP cdr-svr.atlanta.com
   ;branch=z9hG4bK776asdhds;received=196.35.68.101
   ;identity=A5oh1tSWpbmXTyXJDhaCiHjT2xR2PAwBroi5Y8tdJ+CL3
       ziY72N3Y+lP8eoiXlrZOuwb0DicF9GGxA5vw2mCTUxc0XG0KJOh
       pBnzoXnuPNAZdcZEWsVOQAKj/ERsYR9BfxNPazWmJZjGmDoFDbU
       NamJRjiEPOKn13uAZIcuf9zM+
   ;identity-info=https://sip.atlanta.com/cert
```

Implementing this mechanism at every proxy along the route creates layers of identities. Each proxy performs this computation and asserts its changes together with those made before it. This layering produces a chain of auditable modifications. By verifying a digest, it can now determined where in the chain certain routing instructions were modified. This allows for the interrogation of changes made to the dynamic route, as well as modifications to instructions already inserted by hosts having previously handled the SIP message. It further ensures that SIP messages cannot be redirect nor intermediaries be removed from the path already traversed. This is visually illustrated in Fig 7.1.

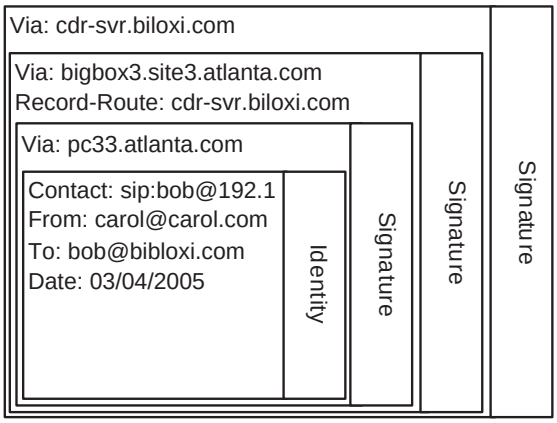

Figure 7.1: Layers of Identities

In light of what has been presented, we will proceed with a discussion on integrity of the headers. We depict the state of a SIP message while in transit, accumulating layers of identities. This state model is used to describe the criteria under which the intermediaries are considered as verified. It allows for a chosen path be regarded as acceptable and trustworthy.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

7.3 Asserting Changes

To ascertain whether or not a chosen route is acceptable, the newly placed identities must be checked. Although the actual implementation is fairly straightforward, we believe that a policy-based evaluation of the intermediaries would be best suited to verify the validity of any particular path. This will be further explored in chapter 8.

Ideally, the SIP message would arrive entirely certified. This requires all proxies to sign for handling the message. This might be a prerequisite when communicating with partners or affiliates with whom confidential information is exchanged. An organisation might wish to choose service providers who guarantee their routes and third-party interconnections. The parties relying on such secure communication would be assured that the caller and remote party are indeed who they claim to be, and managed from within their organisation. It further confirms that they have been identified, and that their session is not handled by any unknown intermediary. Fig 7.2 depicts the state of the SIP message during transit, and the resulting integrity based on the headers being entirely or partially certified.

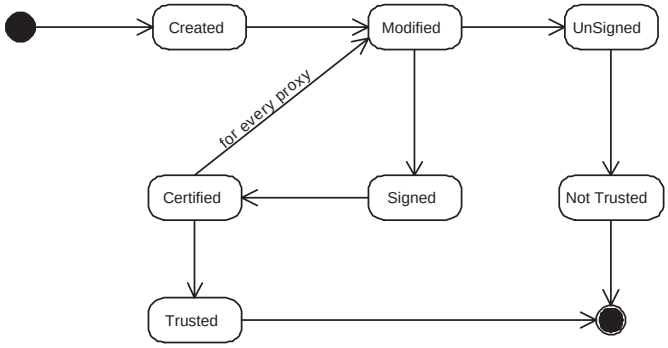

Figure 7.2: States of Certified SIP Headers

Callers communicating over the public Internet, or utilising services from a VoIP provider (such as Vonage) could be partially certified. Existing security issues surrounding access to Public Switched Telephone Network (PSTN) and predefined access lists have been discussed in related work [8,53]. PSTN break-in or break-out gateway and authoritative proxies should certify their

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

identity. This confirms their involvement for accepting a call, while subsequent proxies might not certify their changes.

Should a SIP message not contain a signature over changes made to the headers by a proxy, certain deductions can be made. Not all imply misuse, and would be dependent on the wider acceptance of this mechanism. However, when receiving an unsigned message, it could be assumed that either:

1. A proxy was not configured to sign traversing messages yet is operating correctly.

2. An unexpected intermediary assisted in routing the messages to reach their destination.

3. A malicious proxy was inserted and rerouted the message.

The prior two possibilities could arise under normal operation, yet these scenarios would be more to likely to exist when messages are forwarded by misconfigured or compromised proxies. Thus, the header will reveal the routing messages through unknown and untrusted intermediaries.

A policy can be defined to highlight these situations, and limit untrusted communication. Such policies would be defined by an organisation, and implemented on the authoritative proxy server. It would thus be possible to avoid untrusted requests from being accepted. A policy requiring certification by intermediaries ensures that users cannot by-pass the billing and call control systems fronting the organisation. The design of such a policy is discussed in chapter 8.

In section 7.4 following this paragraph, we will show how the above presented mechanism assists in trusted communication. We conclude that the the discussed application of identity assertion can compliment the proposed enhancements to further securing SIP.

7.4 Trusted Communication

The aim of the chapter was to show that many parties assist in establishing a SIP session. The technology supports VoIP communication as it facilitates

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

the signalling between remote parties. It was shown that the information exchanged is potentially at risk since the messages could be handled by untrusted intermediaries.

We acknowledge that these intermediaries are required, yet raise concerns about the possible implications of call-related data being communicated to untrusted intermediaries. Changes made to the routing headers by either a misconfigured proxy or malicious device, would be able to redirect SIP messages. Third parties and previously unexpected proxies would participate in a session without the user's knowledge.

This chapter has shown how recent discussions of certifying a user's identity can be extended to intermediaries. Participating proxies would underwrite their host names and certify their changes. These could be audited, and modifications attributed to a responsible intermediary.

We believe that security plays an important role in the adoption of VoIP. The underlying technologies must be adequately secured to ensure trustworthy communication. Our research will thus continue to address the facades of security in SIP to achieve this.

The following chapter will evaluate the policies required to govern of such security enhancements. These will consider the emerging enhancements, and motivate through the learnings of previous technologies, how to effectively limit the abuse of VoIP services.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Chapter 8

Formalising using Z Notation

The previous chapter built on the underlying communication technology and proposed a conceptual solution. We alluded to privacy concerns in VoIP and described a mechanism to protect an individual's privacy. Our premise was that if each intermediary attaches a valid signature, the communication path was established between valid and trustworthy proxies. This mechanism of applying signatures at each intermediary seems credible yet must be expressed more formally. We aim to accurately represent our methods for which we have chosen a formal specification language.

This final chapter formalises our previous research on privacy in VoIP. We describe our mechanism using Z notation [101]. The Z specification is mature, structured and well suited to describe the states of our model. Z further requires us to be precise in our notation to ensure the model is consistent and unambiguous.

The advantage of a formal specification is that it forces us to conform to a predefined syntax. This makes it possible to type-check the notation. Type-checking a formalised specification gives assurance that the methods are consistent. By evaluating both the syntax and data types, it can be confirmed that our model conforms to the specification language. This is the desired outcome of this chapter. All schemas in the below Z specification have been validated with **ZTC**, a type-checker for the Z notation [104]. The detailed output of the type report is provided in Appendix A.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

We start this chapter by introducing Z in 8.1, and identify and describe the primary types in section 8.2. In section 8.3 the methods for signing messages are formalised in Z notation. The validation of signatures is specified in section 8.4. The chapter concludes with section 8.5.

8.1 Z Notation

Z notation assists in defining methods based on set theory and first order predicate logic [82]. In general, it is described as a non-executable specification language. It is not a programming language but defines a schema calculus. Z notation is a set of conventions for a model based notation. It is merely a notation, not a method, for representing states through an abstract formal specification.

A specification in Z notation is a collection of schemas. Each schema contains entities and shows relationships between these entities. The specification is constructed by class and object diagrams to consistently specify a model. Relations can be expressed as functions that affect the state of the model. Schemas can further be combined to create new specifications which inherit the properties of the included schemas. It is, therefore, a natural and iterative specification created by a hierarchy of referenced entities.

The rendered version of a Z specification has a unique appearance. A schema is wrapped with a border as in Fig. 8.1. The border of each schema contains the schema name and within its boundaries the specification. The first section above the dividing horizontal line is the *signature* which introduces the the names and types of the entity. The predicate below the separating line contains the *logic* expressing the relationships between the types in the *signature* which must always hold.

8.2 Attributes Types

In order to describe VoIP communication when using SIP, we must first define the participants and the session. We therefore introduce the *user*

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

as a participant of a SIP session and the *session* type which encompass all communication events. In employing Z as an abstract notation, the definition of these two types will be kept constant throughout the model for clarity of the specification.

8.2.1 User

The user type represents an individual participating in the session. In the bi-directional message flow of the SIP session, this individual can be either the initiator or recipient of a SIP message. A required attribute to identify this participant is the *domain* specified by a FQDN. We describe a participant as a *user* followed by a FQDN. The model differentiates between a local and remote user. A proxy, also referred to as an intermediary in this dissertation, is described by only the FQDN.

$$[USER, DOMAIN]$$

$$LOCALE ::= Local \mid Remote$$

$$PARTICIPANT == (USER \leftrightarrow DOMAIN) \nrightarrow LOCALE$$

$$PROXY == DOMAIN$$

This dissertation and supporting work [63] propose adding the identity of the sender over the *from* header. As motivated in chapter 6, SIP messages should further carry a signature for each intermediary. We therefore introduce two signature types for the *identity* and the *via signatures*, respectively.

$$[IDSIGNATURE, VIASIGNATURE]$$

The signatures are checksums as proposed in the previous chapter. These are computed to certify that the contained headers are valid at the time of signing. This mechanism was described in section 7.2 which evaluates the information available in the message to produce a unique checksum. These types are referenced in the specification to follow to validate signatures.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

8.2.2 Session

The second defined type is the SIP session. It represents the communication, all participants and intermediaries. A SIP session is defined in the predicate by the constraints listed in the schema of Fig. 8.1. A SIP session must have a participant initiating the session and one or more intermediary facilitating the communication.

The schema only references primary SIP headers which we determined as mandatory in our model. The required headers including *to*, *from*, *date*, *sequence number* and related, were identified in chapter 7. Optional headers were not included in the *Session* schema as they are not required.

Unique to our model is the power set of *trustedproxies*. This abstract set in Z notation represents a collection of intermediaries who can be trusted. Initially, *trustedproxies*is an empty set. Each intermediary prepares and appends its unique signature over the headers of SIP message. Each proxy is added to this power set as the session progresses.

SipSession

$$
\begin{array}{l}
trustedproxies : \mathbb{P}\, PROXY \\
via : PROXY \pfun VIASIGNATURE \\
from : PARTICIPANT \pfun IDSIGNATURE \\
\hline
\#from = 1 \\
\#via \geq 0 \\
trustedproxies = \mathrm{dom}\, via
\end{array}
$$

Figure 8.1: SipSession Schema

The initial state of the model is set through an initialisation schema. The predicate section of the schema sets the initial constraints upon the sets as they must equal the empty set. This is specified in Fig. 8.2.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

SessionInit

$\Delta SipSession$

$from' = \emptyset$
$via' = \emptyset$
$trustedproxies' = \emptyset$

Figure 8.2: SessionInit Schema

8.3 Signing Messages

The value of our model lies it the ability to determine the trustworthiness of a message. This concept is formalised in Z using two attributes to describe the session state. A constant is defined to represent the result of a checksum computation to confirm that a single message was correctly signed. A second type determines wether the session as a whole can be trusted.

The formal specification must be consistent with our model and thereby caters for these two possible outcomes. A message will either be signed or unsigned. We define two new types to indicate the state of the message and session. It is important to note that these two types affect each other as modelled in section 7.3. The outcome bears on the trustworthiness of the session.

$$SIGNED ::= Signed \mid Unsigned$$

$$TRUST ::= Trusted \mid NotTrusted$$

In order to confirm the identity of the initiator, a schema is required to apply an identity signature to the *from* header. Drawing on headers described in section 7.1, a computed identity checksum is append to the original *from* header in the *SignIdentity* schema in Fig. 8.3.

During the progression of a SIP session, messages will pass through various intermediaries. We mentioned in previous chapters that it is not possible to determine the final set of intermediaries at the start of the session. The unknown intermediaries confirm their identity by appending a valid signature.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

SignIdentity

$\Delta SipSession$
$f? : PARTICIPANT$
$idsig? : IDSIGNATURE$
$s! : SIGNED$

$from = \emptyset$
$via = \emptyset$
$Local \in \operatorname{ran} f?$

$from' = \{f? \mapsto idsig?\}$

$s! = Signed$

Figure 8.3: SignIdentity Schema

In adding their signature, they become part of the set of trusted intermediaries of the session. They must not previously exist in the *trustedproxies* set nor in the *via* set else a loop would have occurred.

SignViaMessage

$\Delta SipSession$
$proxy? : PROXY$
$viasig? : VIASIGNATURE$
$s! : SIGNED$

$(from \mapsto IDSIGNATURE) \notin \emptyset$
$proxy? \notin (trustedproxies)$
$(proxy? \mapsto viasig?) \notin via$
$Remote \in \operatorname{dom} second\,(from)$

$via' = via \cup \{proxy? \mapsto viasig?\}$
$trustedproxies' = trustedproxies \cup \{proxy?\}$

$s! = Signed$

Figure 8.4: SignViaMessage Schema

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Once the message has been verified and all headers are confirmed valid, the *via* signature is appended. This new intermediary is subsequently added to the *trustedproxies* set (as it is now a participant in the SIP session). This mechanism is visually illustrated in Fig. 7.1 and specified in the *SignEachVia* schema in Fig. 8.5.

The formal specification is only correct in representing the model if all intermediaries were added to the *trustedproxies* set. This can be proven by applying the above method at every intermediary. We apply the propositional logic of the domain function to can show that the power set of *trustedproxies* is the union of all proxies with signatures.

$$
\begin{aligned}
trustedproxies' &= \mathrm{dom}\ via' \\
&= \mathrm{dom}(via \cup \{proxy? \mapsto viasig?\} && \text{[by SignViaMessage]} \\
&= \mathrm{dom}\ via \cup \mathrm{dom}\{proxy? \mapsto viasig?\} \\
&= \mathrm{dom}\ via \cup \{proxy?\} \\
&= trustedproxies \cup \{proxy?\}
\end{aligned}
$$

This iterative process of computing and appending signatures must be expressed in Z. We can verify if each intermediary appended a valid signature by the *SignEachVia* schema. This formalisation is consistent with the method described in section 7.3.

The *proxy* and *viasig* variables are input parameters computed for the given intermediary being evaluated, and is compared to the values of the *forall* loop.

It could be argued that the return variable of the *SignEachVia* schema never explicitly returns *Unsigned*. Our riposte is that the logic of a later schema will identify a malicious intermediary when validating the signatures. This validation can occur either en-route or latest at the final recipient. The Z schema *SipMessage* in the next section to follow illustrates the critical outcome of this signature evaluation.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

$$
\begin{array}{|l}
\textit{SignEachVia} \\
\Delta \textit{SipSession} \\
\textit{proxy}? : \textit{PROXY} \\
\textit{viasig}? : \textit{VIASIGNATURE} \\
s! : \textit{SIGNED} \\
\hline
\forall\, v : \textit{via} \bullet \\
\quad (\textit{proxy}? = \textit{first}\,(v) \land \\
\quad \textit{viasig}? = \textit{second}\,(v)) \\
\qquad \Rightarrow \textit{SignViaMessage} \\
s! = \textit{Signed} \\
\hline
\end{array}
$$

Figure 8.5: SignEachVia Schema

8.4 Assertion Framework

Our attempt at specifying the model is not complete without a mechanism to validate the identities of each intermediary. The above schemas precisely describe the method of applying signatures. We now attempt to formalise the validation of SIP message to determine the trustworthiness at any give intermediary and the participants.

Each signature can be validated in accordance to the sequence of signing, as illustrated in Fig. 7.1. A single schema can be used to verify the received message shown in Fig. 8.6.

Two further schemas are required to complete the model. These are used to logically conjugate the positive results with a negative outcome. The negative assignments can now used together with propositional operators to determine the trustworthiness of a session.

We now combine all of the above schemas to indicate the final state of signing and validating SIP messages. The *SipMessage* schema definition appends the signatures, while *PolicyAssertion* validates them as discussed in chapter 7. The outcome of this evaluation determines whether or not the chosen communication path can be trusted.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

ValidateMessage

$\Xi SipSession$
$idsig : IDSIGNATURE$
$viasig : \mathbb{P}\ VIASIGNATURE$
$t! : TRUST$

$\exists_1 f : from \bullet second\,(f) = idsig$
$\forall v : via \bullet first\,(v) \in (trustedproxies) \land$
$\quad second\,(v) \in (viasig)$

$t! = Trusted$

Figure 8.6: ValidateMessage Schema

UntrustedMessage

$t! : TRUST$

$t! = NotTrusted$

Figure 8.7: UntrustedMessage Schema

NotSigned

$s! : SIGNED$

$s! = Unsigned$

Figure 8.8: NotSigned Schema

$SipMessage \mathrel{\widehat=} (SignIdentity \land SignEachVia) \land NotSigned$

$PolicyAssertion \mathrel{\widehat=} (ValidateMessage \land UntrustedMessage)$

Figure 8.9: Final Validation Schema

The desired outcome of the predicate logic should return *Trusted* and allow the session to establish. A failure during validation resulting in *Not*

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Trusted should deny the call to establish.

In this section we managed to completely specify our model in Z notation. The schemas are consistent and unambiguous in precisely representing our previously proposed solution. We defined types and schemas to describe the states of our model. Using ZTC [104] to validate our model, it was confirmed that our Z notation conforms to the specification language.

In the real world, the interactions between individuals are, however, not as black-and-white as the result of this evaluation. Policies often govern over communication preferences, and will be mentioned briefly in the final section.

8.5 Conclusion

This chapter formalised our privacy model using Z notation. The aim of this chapter was to describe our model using a precise and unambiguous formal specification language. The final chapter will follow concludes this dissertation. It will briefly summarise the background, own published research and findings.

Chapter 9

Conclusion and Future Work

9.1 Introduction

All research has been presented and it is now possible to conclude on the findings of information leakage and privacy in VoIP. We believe that through this research, we presented answers to the questions of the problem statement. Universally solving privacy issues is difficult; however, the contribution made by this dissertation seeks to provide additional surety to users. We conclude this dissertation with a brief summary.

9.2 Summary

The problem considered in this dissertation was privacy in VoIP. The aim was to show significant risk to an individual's privacy when communicating using SIP. This allowed us to introduce a privacy enhancement to assure users of a greater level of privacy, and develop a model to support our work.

In addressing the problem statement, our work introduced the underlying protocol, SIP, and gave background on the transparently exchanged headers. These were further investigated to highlight the possible risks to an individual's privacy. Privacy, as commonly expressed in related research, is a controversial topic of research, subjective in nature and a matter of social interpretation. We did not research privacy exclusively yet discussed the legal

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

protection and classification of private information.

We tackled the problem by identifying the private particulars of a user visible at each intermediary. These were classified and differentiated by their implicit and explicit properties, allowing us to determine the implications when SIP messages are unknowingly leaked. It was established that a significant risk exists at the intermediaries where SIP sessions are managed and manipulated. Without sufficient controls to verify the changes made by these intermediaries, messages can be be routed through unexpected or unauthorised proxies. The lack of control over SIP messages was a result of limited identity information about the intermediaries.

Our aim was to build a model to add identity information to SIP messages. We presented a solution of adding *Identity Headers* to the message at each intermediary en-route to their destination. These new headers were a signature over the original headers and routing instructions, certifying the state of the message at the time of handling. Any irregular changes could now be traced to the unexpected or malicious intermediary.

We presented a model as a mechanism to solved the central problem. It was specified in Z notation to formalise the addition of our new *Identity Headers*. The notation provided a consistent framework allowing the intermediaries to evaluate these new headers.

9.3 Publications

This research work was conducted in collaboration and support by the ICSA (Information and Computer Security Architecture) Research Group at the University of Pretoria. Tillwick, a fellow student of ICSA, assisted in the peer review of research into PETs. This stimulated interest in privacy and ways to mitigate the risks of information leakage. The findings lead onto further research forming the basis of various chapters in this dissertation. The product of published papers, ongoing research and gained knowledge is this dissertation. The following works were published as part of our research into information privacy and security:

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

- H. Tillwick, T. Neumann, M.S. Olivier, H.S. Venter, and J.H.P. Eloff. Polar: Proxies collaborating to achieve anonymous Web browsing. *Proceedings of the Fifth International Network Conference (INC2005)*, pages 317–324, Samos, Greece, July 2005. SM Furnell, PS Dowland and G Kormentzas (edt).

- T. Neumann, H. Tillwick, and M.S. Olivier. Information Leakage in Ubiquitous Voice-over-IP Communications. *Trust and Privacy in Digital Business* , pages 233–242, Krakow, Poland, September 2006. S Furnell and C Lambrinoudakis (eds).

- T. Neumann and M.S. Olivier. Enhancements to SIP to prevent abuse of Voice-over-IP services. *Southern African Telecommunication Networks and Applications Conference (SATNAC) Proceedings*, pages 359–364, Champagne Castle, South Africa. D Browne (ed).

The joint paper [89] presented at INC2005 on information privacy gave general introduction to privacy in chapter 5. A second published work [84] presented at TrustBus06 contributed towards chapter 6. This investigation stimulated debate on how the possible risks of privacy in VoIP could be addressed. Chapter 7 resulted from a paper [85] presented at SATNAC on a possible way to secure SIP messages.

9.4 Future work

There is room for further research in this field. There are possible extensions to the privacy framework, which were however, beyond the scope of this dissertation. For example, the extent of the privacy implications should be measurable. A good start would be a survey of how individuals respond to pertinent privacy issues in VoIP. Studies should also evaluate device and user interfaces. It has become clear that these should be enhanced to give the participants more information about a call indicating security weaknesses.

Privacy enhancing technologies have their place and role to play within the realm of protecting user's privacy in online communication. These have

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

however not sufficiently matured in VoIP to provide any notable benefits. The nature of the SIP communications architecture does not allow for the effective placement of PETs to hide or conceal the identity of the source. They therefore have limited protection on the privacy of the individual. We greatly encourage more work into this aspect of protecting privacy.

The investigation into drafting comprehensive privacy policies for VoIP must continue. There is room to address each of the headers of SIP and postulate how these affect the communicating parties. Of broader interest would be if existing privacy control mechanisms such as Privacy for Preference Project (P3P) or content rating could be suitably extended into VoIP.

The criminal and forensic aspect to privacy in VoIP opens an entirely new field of research. Slay and Simon [78] are looking into the implications of using protocol headers for forensic investigations. Their research expands on our topic of protecting an individuals privacy into the legal realm and electronic evidence preservation. This unexplored area of privacy is complex to research bridging technology, privacy and law enforcement.

It would be naive to think that there is a ultimate solution to privacy in VoIP, let alone privacy on the Internet. It will require a combination of technologies, PETs, organisational and legislative policies to protect an individual's privacy. Research must continue on all levels to improve these facets in equal measure. This approach will not guarantee privacy, but will set a high level of privacy protection. In the end, the fact that sensitive information is transmitted becomes less of a contentious issue when users have the ability to control their communication. We believe this dissertation has brought us one step closer to achieving this goal.

In closing, the dissertation has, through a narrative discussion, taken us from the basics of fixed line through to the truly ubiquitous and mobile nature of telephony. All forms of communication will convey private information about an individual and, in light of this, it has become clear that privacy will remain a challenge.

Appendix A

ZTC Output

```
given sets
    USER
    DOMAIN
    LOCALE
    IDSIGNATURE
    VIASIGNATURE
    SIGNED
    TRUST
end given sets

global names
    Local :     LOCALE
    Remote :    LOCALE
    PARTICIPANT :   (P ((P (USER x DOMAIN)) +-> LOCALE))
    PROXY :     (P DOMAIN)
    Signed :    SIGNED
    Unsigned :  SIGNED
    Trusted :   TRUST
    NotTrusted :    TRUST
end global names

schema SipSession
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
end schema

schema SessionInit
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
end schema
```

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


```
schema SignIdentity
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    f? :    ((P (USER x DOMAIN)) +-> LOCALE)    ([P ([P (USER x DOMAIN)] x LOCALE)])
    idsig? :    IDSIGNATURE (IDSIGNATURE)
    s! :    SIGNED  (SIGNED)
end schema

schema SignViaMessage
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    proxy? :    DOMAIN  (DOMAIN)
    viasig? :   VIASIGNATURE    (VIASIGNATURE)
    s! :    SIGNED  (SIGNED)
end schema

schema SignEachVia
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    proxy? :    DOMAIN  (DOMAIN)
    viasig? :   VIASIGNATURE    (VIASIGNATURE)
    s! :    SIGNED  (SIGNED)
end schema

schema ValidateMessage
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    idsig :     IDSIGNATURE (IDSIGNATURE)
    viasig :    (P VIASIGNATURE)    ([P VIASIGNATURE])
    t! :    TRUST   (TRUST)
end schema

schema UntrustedMessage
    t! :    TRUST   (TRUST)
```

```
end schema

schema NotSigned
    s! :    SIGNED  (SIGNED)
end schema

schema SipMessage
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    f? :    ((P (USER x DOMAIN)) +-> LOCALE)    ([P ([P (USER x DOMAIN)] x LOCALE)])
    idsig? :    IDSIGNATURE (IDSIGNATURE)
    s! :    SIGNED  (SIGNED)
    proxy? :    DOMAIN  (DOMAIN)
    viasig? :   VIASIGNATURE    (VIASIGNATURE)
end schema

schema PolicyAssertion
    trustedproxies :    (P DOMAIN)  ([P DOMAIN])
    via :   (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from :  (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    trustedproxies' :   (P DOMAIN)  ([P DOMAIN])
    via' :  (DOMAIN +-> VIASIGNATURE)   ([P (DOMAIN x VIASIGNATURE)])
    from' :     (((P (USER x DOMAIN)) +-> LOCALE) +-> IDSIGNATURE)  ([P ([P ([P (USER x DOMAIN)] x LOCALE)]
                x IDSIGNATURE)])
    idsig :     IDSIGNATURE (IDSIGNATURE)
    viasig :    (P VIASIGNATURE)    ([P VIASIGNATURE])
    t! :    TRUST   (TRUST)
end schema
```

Output from

```
C:\Masters\ztcwin>ztc "C:\Masters\dissertation\zed.tex" -V0 -T
This is ZTC (version 2.03)
Copyright (c) Xiaoping Jia, 1993-1998.
... Initializing.
... Loading Z mathematical tools library: math0.zed
Parsing main file: C:\Masters\dissertation\zed.tex
End of main file: C:\Masters\dissertation\zed.tex
Type report written in "C:\Masters\dissertation\zed.typ"

Log written in "C:\Masters\dissertation\zed.log"
```

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Appendix B

Acronyms

3G Third Generation

3GPP Third Generation Partnership Project

CDR Call Data Record

CLI Caller Line Identity

DNS Domain Name Service

DoS Denial-of-Service

FCC Federal Communications Commission

Freiburg Privacy Diamond Freiburg Privacy Diamond

FQDN Fully Qualified Domain Name

GPRS General Packet Radio Service

GSM Global System for Mobile

H.323 H.323

HTTP Hyper Text Transfer Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IM Instant Messaging

IMS IP Multimedia Subsystem

IP Internet Protocol

ISP Internet Service Provider

ISDN Integrated Services Digital Network

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

NAT Network Address Translation

NTIA National Telecommunications and Information Administration

NGN Next Generation Network

OECD Organization for Economic Cooperation and Development

P3P Privacy for Preference Project

PET Privacy Enhancing Technology

PSTN Public Switched Telephone Network

PVC Private Virtual Channel

QoS Quality of Service

RFC Request For Comment

RTP Real-time Protocol

SIP Session Initiation Protocol

SDP Session Description Protocol

TCP Transmission Control Protocol

TDM Time Division Multiplexing

TLS Transport Layer Security

UDP User Datagram Protocol

URI Uniform Resource Locator

VoIP Voice over IP

WDM Wavelength-Division Multiplexing

Bibliography

[1] Karl Aberer and Zoran Despotovic. Managing Trust in a Peer-2-Peer Information System. In *Conference on Information and Knowledge Management*, pages 310–317. ACM, 2001.

[2] Mark S. Ackerman. Privacy in pervasive environments: next generation labeling protocols. *Personal Ubiquitous Computing*, 8(6):430–439, 2004.

[3] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *EC '99: Proceedings of the 1st ACM conference on Electronic commerce*, pages 1–8, New York, NY, USA, 1999. ACM Press.

[4] Yali Zhu Adrian E. Conway. A simulation-based methodology and tool for automating the modeling and analysis of voice-over-IP perceptual quality. *Performance Evaluation*, 54:129–147, 2003.

[5] Benjamin Alfonsi. Alliance addresses VoIP security. *IEEE Security & Privacy*, 3(4):8, July/August 2005.

[6] Ofir Arkin. E.T. Can't Phone Home. In *Security Issues with VoIP*, http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt, 2002. Black Hat USA 2002.

[7] R. Atkinson and S. Kent. *IPSec: Security architecture for Internet Protocol, RFC 2401.* IETF, 1998.

[8] James Aweya. Trunking of TDM and narrowband services over IP Networks. *Int. J. Netw. Manag.*, 13(1):33–60, 2003.

[9] James Aweya. Trunking of TDM and narrowband services over IP networks. *International Journal of Network Management*, 13:33–60, 2003.

[10] David L. Baumer, Julia B. Earp, and J.C. Poindexter. Internet privacy law: a comparison between the United States and the European Union. *Computers & Security*, 23:400–412, 2004.

[11] James Begole, John C. Tang, Randall B. Smith, and Nicole Yankelovich. Work rhythms: analyzing visualizations of awareness histories of distributed groups. In *Proceedings Conference on Computer-Supported Collaborative Work (CSCW)*, pages 334–343, 2002.

[12] Alexander Graham Bell. Improvement In Telegraphy, May 1876.

[13] Mark Buchanan. *Small World.* Weidenfeld Nicolson, 1st edition, 2002.

[14] Herbert Burkert. Privacy-Enhancing Technologies: Typology, Critique, Vision. *Technology and Privacy: The New Landscape*, pages 125–142, 1997.

[15] Gonzalo Camarillo and Miguel-Angel Garcia-Martin. *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds, Second Edition.* John Wiley & Sons, 2006.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

[16] Jean Camp and Y. T. Chien. The internet as public space: concepts, issues, and implications in public policy. *SIGCAS Comput. Soc.*, 30(3):13–19, 2000.

[17] Vinton G. Cerf. Spam, spim, and spit. *Communication of the ACM*, 48(4):39–43, 2005.

[18] Lee Chae-Sub and D. Knight. Realization of the next-generation network. *IEEE Communications Magazine*, 43(10):34–41, October 2005.

[19] Shigang Chen and Klara Nahrstedt. An overview of quality of service routing for next-generation high speed networks: Problems and solutions. *IEEE Networking*, pages 64–79, November/December 1998.

[20] Steven Cherry. Seven Myths about Voice Over IP. *IEEE Spectrum*, 42:52– 57, March 2005.

[21] Lorrie Faith Cranor and Brian A. LaMacchia. Spam! *Communication of the ACM*, 41(8):74–83, 1998.

[22] Jon Crowcroft, Vicky Hardman, and Dave Lewis. Pricing internet services. *xyz*, 2000.

[23] Mary J. Culnan. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing*, 19(1):20–26, 2000.

[24] Mary J. Culnan and Pamela K. Armstrong. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1):104–115, January 1999.

[25] Daniel Cvrceka and Ahmed Patel Vaclav Matyas Jr. Evidence processing and privacy issues in evidence-based reputation systems. *Computer Standards & Interfaces 02345*, 2005.

[26] Douglas C. Sicker and Tom Lookabaugh. VoIP Security: Not an Afterthought. *Queue*, 2(6):56–64, 2004.

[27] P. Faltstrom. E.164 number and DNS. RFC 2916, IETF, 1998.

[28] Claude S. Fischer. *America Calling: A Social History of the Telephone to 1940.* University of California Press, Berkeley, CA, 1992.

[29] S Fisher. Privacy by design. *Info World*, pages 20–22, 2002.

[30] David L. Fraley. Voice Over IP Communications Must Be Secured. *Gartner, Inc.*, 1(G00124016):5, 15 November 2004.

[31] Charles Fried. Privacy. *The Yale Law Journal*, 77(3):475–493, 1 1968.

[32] Atanu Ghosh, Michael Fry, and Jon Crowcroft. An Architecture for Application Layer Routing. *Lecture Notes in Computer Science*, 1942:71, 2000.

[33] Philip Ginzboorg. Seven comments on charging and billing. *Communication of the ACM*, 43(11):89–92, 2000.

[34] David Goldschlag, Michael Reed, and Paul Syverson. Onion Routing. *COMMUNICATIONS OF THE ACM*, 42:39–41, 1999.

[35] Bur Goode. Voice over internet protocol (voip). In *18th IFIP/ACM International Conference on Distributed Systems Platforms*, volume 90, pages 1496–1517, September 2002.

[36] Larry Greenstein. Transporting Voice Traffic Over Packet Networks. *International Journal of Network Management*, 8(4):227–234, 1998.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

[37] W3C Working Group. Web Services Architecture. Technical report, W3C, http://www.w3.org/TR/ws-arch/, 2004.

[38] XML Protocol Working Group. Milestones and Deliverables. Technical report, W3C, http://www.w3c.org/2000/xp/Group/, 2000.

[39] GSM World. GSM Coverage Maps and Roaming Information. Technical report, GSM Association, http://www.gsmworld.com/roaming/gsminfo/index.shtml, December 2005.

[40] Martin Gudgin. Secure, reliable, transacted: innovation in Web Services architecture. In *SIGMOD '04: Proceedings of the 2004 ACM SIGMOD international conference on Management of Data*, pages 879–880, New York, NY, USA, 2004. ACM Press.

[41] H. Schulzrinne and S. Casner and R. Frederick and V. Jacobson. RTP: A transport protocol for real-time applications, RFC 1889. Technical report, Network Working Group, 1996.

[42] M. Handley and V. Jacobson. *SDP: Session Description Protocol, RFC 3261.* IETF, 1998.

[43] Mark Handley and Adam Greenhalgh. Steps towards a dos-resistant internet architecture. In *FDNA '04: Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, pages 49–56, New York, NY, USA, 2004. ACM Press.

[44] Edmund A Harrington. Voice/data integration using circuit switched networks. *IEEE Transactions on Communications*, 28(6):781–793, 1980.

[45] Debby Hindus and Chris Schmandt. Ubiquitous audio: capturing spontaneous collaboration. In *CSCW '92: Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 210–217, New York, NY, USA, 1992. ACM Press.

[46] Jiann-Min Ho, Jia-Cheng Hu, and Peter Steenkiste. A Conference Gateway Supporting Interoperability Between SIP and H.323. *MM*, pages 421–430, 2001.

[47] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, and J. Postel. Internet registry ip allocation guidelines. Technical report, Network Working Group, United States, 1996.

[48] G Huston. Analyzing the Internet's BGP Routing Table. *The Internet Protocol Journal*, 2001.

[49] Industry Analysis Division, Common Carrier Bureau. Trends in Telephone Service. Technical report, Federal Communications Commission, http://www.fcc.gov/ccb/stats, May 1999.

[50] Ellen Isaacs, Alan Walendowski, Steve Whittaker, Diane J. Schiano, and Candace Kamm. The character, functions, and styles of instant messaging in the workplace. In *CSCW '02: Proceedings of the 2002 ACM conference on Computer supported cooperative work*, pages 11–20, NY, USA, 2002. ACM Press.

[51] Subhash C Jain. Crm shifts the paradigm. *Journal of Strategic Marketing*, 13(4):275 – 291, 2005.

[52] Matthew L James. The Internet telephone: Voice over Internet Protocol (VoIP). *Parliamentary Library*, 29, February 2005.

[53] Wenyu Jiang, Jonathan Lennox, Henning Schulzrinne, and Kundan Singh. Towards junking the PBX: deploying IP telephony. In *NOSSDAV '01: Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video*, pages 177–185, New York, NY, USA, 2001. ACM Press.

[54] Radu Jurca and Boi Faltings. An Incentive Compatible Reputation Mechanism. *Autonomous Agents and Multi-Agent Systems*, pages 1026–1027, 2003.

[55] KaZaA. Supernodes. Technical report, Sharman Networks, http://www.kazaa.com/us/help/faq/supernodes.htm, 2002.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

[56] Keith Knightson, Naotaka Morita, and Thomas Towle. Ngn architecture: Generic principles, functional architecture, and implementation. *IEEE Communications Magazine*, pages 49–56, October 2005.

[57] Craig Labovitz, G. Robert Malan, and Farnam Jahanian. Internet routing instability. In *SIGCOMM '97: Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 115–126, New York, NY, USA, 1997. ACM Press.

[58] Athina P. Markopoulou, Fouad A. Tobagi, and Mansour J. Karam. Assessing the quality of voice communications over internet backbones. *IEEE/ACM Transactions on Networking*, 11(5), October 2003.

[59] Leysia Palen, Marilyn Salzman, and Ed Youngs. Going wireless: behavior & practice of new mobile phone users. In *CSCW '00: Proceedings of the 2000 ACM conference on Computer supported cooperative work*, pages 201–210, USA, 2000. ACM Press.

[60] The European Parliament and the council of the European Union. Directive 2002/58/ec of the european parliament and of the council. *Official Journal of the European Communities*, 37(201):1–11, 7 2002.

[61] Dan Pei, Lixia Zhang, and Dan Massey. A Framework for Resilient Internet Routing Protocols. *IEEE Networking*, March/April 2004.

[62] J. Peterson. *A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323.* IETF, November 2002.

[63] J. Peterson and C. Jennings. *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), draft-ietf-sip-identity-03.* IETF, February 2005.

[64] Larry Press. Tracking the global diffusion on the internet. *Communication of the ACM*, 40(11):11–17, 1997.

[65] Vassilis Prevelakis and Diomidis Spinellis. The Athens Affair. *IEEE Spectrum*, 5280, July 2007.

[66] PriMetrica. Telegeography. Technical report, TeleGeography, Inc., 2004.

[67] United Nations Development Programme. *Human Development Report 2005: International cooperation at a crossroads. Aid, trade and security in an unequal world.* Oxford University Press and United Nations Development Programme, December 2005.

[68] M.K. Ranganathan and L. Kilmartin. Performance analysis of secure session initiation protocol based VoIP networks. *Computer Communications*, 26:552–565, 2003.

[69] W3C Recommendation. SOAP Version 1.2. Technical report, W3C, http://www.w3.org/TR/soap12/, 2003.

[70] Andreas Rieke and Thomas Demuth. JANUS: Server Anonymity in the World Wide Web. In *Conference Proceedings EICAR International Conference*, pages 195–208. U. E. Gattiker, 2001.

[71] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, RFC 3261, June 2002.

[72] Antony Rowstron and Peter Druschel. Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems. In *18th IFIP/ACM International Conference on Distributed Systems Platforms*, November 2001.

[73] H Schulzrinne and J Rosenberg. The Session Initiation Protocol: Internet-centric signaling. In *Communications Magazine*, volume 38, pages 134–141. IEEE, October 2000.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

[74] Henning Schulzrinne and Knarig Arabshian. Providing emergency services in internet telephony. *IEEE Internet Computing*, 6(3):39–47, 2002.

[75] Henning Schulzrinne and Elin Wedlund. Application-layer mobility using sip. *SIGMOBILE Mobile Compututer Communication Rev.*, 4(3):47–57, 2000.

[76] Phil Sherburne and Cary Fitzgerald. You don't know jack about voip. *Queue*, 2(6):30–38, 2004.

[77] Kang G. Shin and Seungjae Han. Fast Low-Cost Failure Recovery for Reliable Real-Time Multimedia Communication. In *IEEE Network*. IEEE, November/December 1998.

[78] Jill Slay and Matthew Simon. Voice over ip forensics. In *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, pages 1–6, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[79] Arun K. Somani and Byrav Ramamurthy. *Optical Communication Networks for Next-Generation Internet*. IEEE Network, November/December 2000.

[80] R. Sparks. *SIP call control*. IETF, July 2000.

[81] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In *ACM Conference on Electronic Commerce*, pages 38–47. ACM, 2001.

[82] J. M. Spivey. *The Z Notation: A Reference Manual*. Prentice Hall International Series in Computer Science, 2nd edition, 1992. Free online.

[83] Harris Interactive Survey. Online privacy: a growing threat. Technical Report 96, Business Week, Rochester, New York, March 2000.

[84] H. Tillwick T. Neumann and M.S. Olivier. Information leakage in ubiquitous voice-over-ip communications. In Springer-Verlag, editor, *Trust and Privacy in Digital Business*, volume 4083/2006 of *Lecture Notes in Computer Science*, pages 233–242. Springer Berlin / Heidelberg, 2006.

[85] T. Neumann and M.S. Olivier. Enhancements to SIP to prevent abuse of Voice-over-IP services. In D Browne, editor, *Southern African Telecommunication Networks and Applications Conference (SATNAC) Proceedings*, volume 1, pages 359–364, September 2005.

[86] John C. Tang and James Begole. Beyond instant messaging. *Queue*, 3:28–37, 11 2003.

[87] Herman T. Tavani and James H. Moor. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *Computers and Society*, pages 6–11, March 2001.

[88] G.A. Thom. *H.323: the multimedia communications standard for local area networks*. IEEE Communications, December 1996.

[89] H. Tillwick, T. Neumann, M.S. Olivier, H.S. Venter, and J.H.P. Eloff. Polar: Proxies collaborating to achieve anonymous Web browsing. In *Proceedings of the Fifth International Network Conference (INC2005)*, pages 317–324, 2005.

[90] Frank M. Tuerkheimer. The underpinnings of privacy protection. *Communication of the ACM*, 36(8):69–73, 1993.

[91] Joe Tullio, James "Bo" Begole, Eric Horvitz, and Elizabeth D. Mynatt. Forecasting presence and availability. In *CHI '04: Extended abstracts of the 2004 conference on Human factors and computing systems*, pages 1713–1714. ACM Press, 2004.

[92] Upkar Varshney, Andy Snow, Matt McGivern, and Christi Howard. Voice Over IP. *Communications of the ACM*, 45(1):89–96, 2002.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

[93] Upkar Varshney, Andy Snow, Matt McGivern, and Christi Howard. Voice over IP. *Communication of the ACM*, 45(1):89–96, 2002.

[94] Son Vuong and Yan Bai. A survey of voip intrusions and intrusion detection systems. *The 6th International Conference on Advanced Communication Technology*, 1:317–322, 2004.

[95] Thomas J. Walsh and D. Richard Kuhn. Challenges in Securing Voice over IP. *IEEE Security and Privacy*, 3(3):44–49, 2005.

[96] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4:193–220, 12 1890.

[97] Mark Weiser. The Computer for the 21st Century. *Scientific American Ubicomp*, 3:94–104, September 1991.

[98] Aaron Weiss. Trends for 2005. *netWorker*, 8(4):20–27, 2004.

[99] A Westin, L Harris, and Associates. Harris-equifax consumer privacy survey. Technical report, Equifax Inc, Atlanta, Georgia, 1991. 1,255 adults of the U.S. public.

[100] "J Wiley". "from voice-band modems to dsl technologies". *International Journal Network Management*, 11(5):265–276, 2001.

[101] Jim Woodcock and Jim Davies. *Using Z: specification, refinement, and proof*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1996.

[102] Marie A. Wright and John S. Kakalik. The erosion of privacy. *SIGCAS Comput. Soc.*, 27(4):22–25, 1997.

[103] W.W. Wu and A. Livne. ISDN: a snapshot. In *Proceedings of the IEEE*, pages 103–111. IEEE, 1991.

[104] Xiaoping Jia. *ZTC: A Type Checker for Z – User's Guide*. Chicago, IL 60604, USA, 1994.

[105] Bin Yu and Munindar P. Singh. An Evidential Model of Distributed Reputation Management. *Autonomous Agents and Multi-Agent Systems*, pages 294–301, 2002.

[106] Alf Zugenmaier. The Freiburg Privacy Diamond - A Conceptual Model for Mobility in Anonymity Systems. In *Proceedings of Globecom*, 2003.

[107] Alf Zugenmaier, Michael Kreuzer, and Günter Müller. The freiburg privacy diamond: An attacker model for a mobile computing environment. In *KiVS Kurzbeiträge*, pages 131–141, 2003.