On Privacy in Mobile Voice Communication Networks

by

N.J. Croft

Submitted in fulfilment of the requirements for the degree
Philosophiae Doctor in Computer Science

In the Faculty of Engineering, Built Environment & IT
University of Pretoria

2010

Contents

List of Figures

List of Tables

Fair Use

Summary

Title: On Privacy in Mobile Voice Communication Networks
Candidate: Neil John Croft
Supervisor: Professor Martin S. Olivier
Department: Faculty of Engineering, Built Environment and Information Technology
Degree: Doctor of Computer Science
Keywords: Privacy, Communications, PET, Mobile, Anonymous, NGN

Abstract

The introduction of mobile communications has undoubtedly altered our physical and social world. Like the Internet, it has changed the way we interact with each other allowing for communication using a variety of communication mediums by means of a magnitude of interactive mobile devices. The context, content, persons communicating, situation and timing all have a varying degree of influence on the sensitivity of information being shared. The individual's awareness of exposure of their private information on the Internet has filtered through into the mobile communications space.

It is commonly held in current mobile communication network literature that as privacy-sensitive information travels through a network, it may be exposed to privacy infringement at various stages along its journey. Much of the concern from the individual's perspective, though, stems from a fear of the unknown. In the presence of these threats and vulnerabilities it is justified to wonder whether current mobile communications networks (and indeed future networks) provides sufficient privacy for users with very valuable information to communicate.

In this thesis, I develop a systematic approach to identifying areas of privacy concern in a current mobile communication networks in an effort to outline mobile communication privacy principles and how applicable they are in Next Generation Networks. With a privacy stance, the objective of my work is through technical examination and sometimes theoretical undertaking to identify acceptable solutions which restrict the flow of private information and ultimately confirm, through privacy analyses, the benefits gained in doing so.

The results show that, given the current situation and technological configuration, there are commonalities which extend beyond a mere concern within a mobile communications network's requirement for privacy enhancement. In a perfect world, the idea is to articulate towards a system of privacy by design rather than as an uttered afterthought. It is no longer inconceivable to think there is an opportunity to deliver a privacy-conscious network, if careful consideration is given to all parties and aspects that govern a mobile communications network and the correct privacy-enhancing technologies are administered correctly.

Throughout my thesis, although each privacy solution is segmented and

may have a specific privacy application, the results attested contribute largely to a converged prospectus for privacy-aware future generation communication networks. The significance of this lies in the study of past privacy pitfalls in order to better manage the potential for future privacy problems. The rationalisation is if privacy principles are identified (in existing networks) and adhered and applied to (in next generation networks), then we converge towards a network infrastructure that possesses a desirable level of privacy protection.

Acknowledgements

This thesis is in fulfilment of the Doctor of Science (PhD) degree in Computer Science at the University of Pretoria, South Africa. This last assignment is a closure on the education that leads to the title Doctor of Science.

I wrote when completing my masters dissertation that the experience was like completing a marathon. A PhD on the other hand is not merely a race but a life experience, one which has lead me to new heights and new approaches in my capacity to read, learn, explore, think and apply myself. It challenges you like no other and appears to be never ending. Its constant desire for commitment and total dedication is absolute and unforgiving but as the saying goes "what doesn't kill you only makes you stronger!".

I would like to take this opportunity to thank my supervisor at the University of Pretoria, Professor Martin Olivier, for his valuable support, insight and guidance throughout the duration of my thesis. Prof. Olivier always remarks "some of your best work is done after you complete your PhD", I hope this statement holds true for me in the future.

I am appreciative of the opportunities awarded to me by my parents, Campbell and Janice, and would like to give special thanks to them. They have continually given more than I could ever have asked for and have nothing but inspired me to greater things. I will be forever grateful to them and love them dearly. Thank you so much.

Thanks to friends for all the encouragement and understanding they have given me during this time, its is really appreciated.

To those that have brought me so much joy over the years: carrots, parrot, lippy, CC, woody, sigh and coo-coo, I salute you.

Neil Croft
(Pretoria, South Africa, 2010)

Chapter 1

Introduction

The evolution of information and technology (ICT) has arguably progressed through four clearly definable phases since the invention of the personal computer (PC). The introduction of a graphical user interface (UI) was the next significant milestone providing for ease of use and visual interaction. Suddenly we found ourselves in the Internet era, connectivity and communication among PC users was now possible on a global scale. Today is the turn of the social network, where individuals rush to publish personal and sometimes private information about themselves using any medium available on the Internet. There has been a recent explosion in popularity of social networking sites such as myspace [11], facebook [161] and linkedIn [79]. Some of the issues raised regarding social networking sites concern the security and privacy of personal information and indeed the value of privacy in monetary terms [89]. This has led to a renewed interest in privacy and privacy preservation and techniques of ensuring the individual's privacy in a social and communicative context.

What the Internet did for the PC, so the introduction of the mobile phone did for telecommunications. Everyone with a mobile device became instantly connected and accessible, anywhere, anytime. However, like in the evolution of the personal computer, security and privacy has an ever increasing significance in the evolution of telecommunications. The individual's awareness of exposure of private information on the Internet has trickled over to the mobile communications space. As mobile technologies are usually maintained by an underlying controlling authority, access to, dissemination of and the capturing of network events for communicative, statistical and billing purposes increase the risk of possible privacy infringement.

This chapter focuses on defining privacy, discussing specific privacy terminology, how privacy can be enforced with the aid of technology, and finally how all these aspects relate to mobile voice communications networks. It presents a formal problem statement, the methodology used and finally the thesis structure and layout. This thesis investigates privacy and security-

related issues with respect to current mobile voice communications networks. The idea is to draw on these privacy findings to aid in the ability of Next Generation Networks (NGNs) to enhance their privacy protection mechanisms.

1.1 Privacy

Privacy is well recognised as a fundamental human right. It can best be described as the individual's desire to control the ways in which his/her personal data is collected, used, disseminated and distributed. Protecting this right requires basic privacy principles to be guaranteed when personal data is collected, stored and exchanged.

The term "privacy", in technology, is generally used to refer to the protection of data against various risks during transmission [32]. However, control of personal information is important regardless of where it is used or what type of device or medium is used. Individuals have a right to control and protect their personal information in both virtual and physical worlds [113].

Privacy is classified as a human boundary control process that allows access by others according to one's own needs and situational factors [98]. Personal or individual privacy does not always refer to total isolation from others. From an individual's perspective, too much privacy can lead to alienation and too little to an invasion of privacy [119]. Privacy cannot be seen as an absolute science when there are so many influencing factors.

Although many have tried to categorise privacy into descriptive dimensions, this is an arduous task. Privacy, in general, is a multi-faceted interest. The dimensions of privacy have been broken down into the following concepts [32] i) privacy of the person (ensuring integrity of the body, such as body searches) ii) privacy of personal behaviour (includes aspects of behaviour, such as religious practice) iii) privacy of personal communication (to communicate using any medium without being monitored) and iv) privacy of personal data (ensuring that an individual's information is not gathered, stored or processed by a third party). It is of interest that these privacy dimensions are palpable under privacy aspects relating to voice communications networks.

Privacy dimensions specifically relating to voice communications environments are summarised in [32] as i) privacy of personal communications, and; ii) privacy of personal data. These are often referred to as "information privacy" in communication environments, and can be summarised as individuals' wish to communicate among themselves using a variety of independent or integrated media without interference or monitoring of their communications activities by third parties. Additionally, individuals require that their personal information should not be automatically made available to others, even when that information is held by a third party. In essence,

the individual demands a substantial degree of control over his/her information and its use in the public domain.

We may choose to define privacy, categorise it, and measure it. Some may argue that in doing so, we quickly realise no information is truly private in nature. This stems from the fact that most private information is allocated to us by some public authority. Consider for example your government-issued identity number and the mobile number allocated to you by a network operator. This leads us to question the very existence of the concept of privacy and whether it is important at all. Nevertheless, even if it is not possible to clearly define, categorise or measure privacy, one thing is certain - there is a duty to safeguard information so as to quell all fears an individual may have regarding the anguish that the violation of this information may cause.

1.1.1 Why Privacy is Important?

Some advocates opposing privacy generally ask the question: "If you aren't doing anything wrong, what do you have to hide?" It can be argued that privacy is not about hiding the wrong but about an inherent human right. It is a fundamental requirement for maintaining our human condition with dignity and respect by not allowing others access to personal information. At the same time, privacy protects us from abuse by those in power, even if we are doing nothing wrong at the time of surveillance [139]. Privacy helps individuals maintain their autonomy and more specifically their individuality by preventing the potential exploitation by a controlling authority.

Rachels [127] suggests there is not a clear-cut or single answer to the question of privacy being important, since people have a number of interests that may be harmed by invasion of their privacy. In addition, individual privacy is exactly that - it concerns a specific individual. This is evident in certain situations where privacy is necessary to protect people's interests in competitive situations. In other cases, someone may want to keep an aspect of his/her life or behaviour private simply because it would be embarrassing for others to know about it. We recognise that privacy is an involved condition affected by situations, circumstances, timing, context and the surrounding environment, and we accept that it has a place in modern society. In many cases, privacy concerns are realised only once privacy has been infringed upon.

The significance of privacy is reflected in the fact that the fundamental documents that define human rights include reference to privacy. The Universal Declaration of Human Rights, in Article 12, states [5]:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Many national constitutions and bill of rights also contain references to privacy, data protection, associated actions and the consequences thereof.

1.1.2 Privacy, Information Spaces and Expected Flow

Privacy is not an absolute notion, but rather a highly fluid concept about controlling the dissemination and use of one's personal information. Privacy protection is measured by assessing the appropriate physical, technical and procedural safeguards that are in place to protect the security and integrity of information. We recognise that privacy protections must prevent both harm and the free-flow of information.

Jiang et al. [2002] [157] define a key set of abstractions that describe how information flows within a system of people and computers. The first abstraction is information spaces, which is a collection of data delimited by physical, social or activity-based boundaries. Personal data is stored in and used within an information space, but may flow into other information spaces. The second abstraction describes the lifecycle of personal data, namely collection, access and second use. The third abstraction is a set of themes for minimising asymmetry, namely prevention, avoidance and detection.

The constant interactivity and change in information spaces make defining explicit privacy boundaries difficult. It is, however, possible to monitor and predict the flow of information. The capability to predict expected information flows allows for the formulation of a principle stating that information that is shared is not disclosed, provided its flow is expected. Deviation from this expectation is considered a privacy violation. In general, once private information is exposed, deviation from the expected is not altogether probable, but possible. Indeed, a greater information exposure, even if the flow is expected, increases the potential of privacy violation. Once private information is known by someone else, the threat for exposure is real and, once divulged, cannot be rendered private again.

1.1.3 Privacy Techniques

There are a few common techniques for ensuring privacy - the first is to "hide" the identity of the individual and the second is to "hide" who performed a specific action. Thus, privacy is sometimes related to anonymity and is often most highly valued by people who are publicly known.

1.1.3.1 Anonymity and Pseudonymity

Anonymity typically refers to a person, and often means that the personal identity or personally identifiable information of that person is not known. More formally, anonymity is the state of not being identifiable within a set of subjects, the so-called *anonymity set* [123]. In other words, the likelihood

of identification of a particular object in a subject set is equal to zero.

Anonymity may reduce the accountability one perceives to have for actions performed, and removes the impact that these actions might otherwise have on associated reputation. However, anonymity may have a direct bearing on security.

One way of achieving anonymity is through the use of a pseudonym. A pseudonym usually refers to an artificial or fictitious name, also known as an alias, used by an individual as an alternative to his/her true identity in order to hide some part of that identity. Pseudonymity ensures that a user may use a resource or service without disclosing his/her user identity, but can still be held accountable for that use [83].

If there is an inability to hide the individual's identity, effecting privacy through the removal of association to an event may be sufficient.

1.1.3.2 Unobservability and Unlinkability

Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used [83]. In other words, unobservability is the state of items of interest being indistinguishable from any items of interest at all [123].It means that messages are not discernible from one another. Two examples in this regard are sender and receiver unobservability. Sender unobservability suggests that it is not noticeable whether any sender within the unobservability set sends. In contrast, recipient unobservability means that it is not noticeable whether any recipient within the unobservability set receives anything.

A person may wish to perform events without revealing information about his/her identity. This disassociation is often referred to as *unlinkability*. Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together [83]. Unlinkability is described as two or more items that are no more and no less related than they are related concerning a prior knowledge [123]. That is, the likelihood of linking an object in a particular subject set to an action performed is zero.

Besides having the ability to hide who is using a service, we need to preserve the privacy of the users whose information the data set contains. Differential privacy, the notion of indistinguishability, aims to provide a means to maximize the accuracy of queries from statistical databases while minimizing the chances of identifying its records.

We have argued why privacy is important, looked at information spaces and expected flow and privacy violation. We have even shown some basic techniques in ensuring privacy, but how does one go about protecting privacy?

1.2 Privacy Protection

The aim of information protection is to guarantee privacy. Privacy protection includes the protection of the personal privacy rights of individuals from the unauthorised collection, maintenance, use and disclosure of personal information about them. Privacy from the user's point of view is the protection of information, behaviour and habits from others. Furthermore, privacy protection is the process of finding appropriate balances between privacy and multiple conflicting interests. Some conflicting interests include conflict with one's own interest, with another's interest or even with a society's interest. Privacy protection can be summarised as a process of finding appropriate balances between privacy and these multiples of competing interests.

1.2.1 The Law and Privacy Protection

Existing laws and regulations in South Africa do not provide a strong framework for privacy protection, and privacy is protected under common law and Section 14 of the Constitution [34]. The constitutional right to privacy is not an absolute right, but may be limited in terms of law of general application. It has to be balanced with other rights entrenched in the Constitution.

Details of data protection legislation in South Africa appear in other South African legislation such as the Electronic Communications and Transactions Act, 2002 (No. 25 of 2002) (ECT Act) [52]. At present, Chapter 8 of the ECT Act sets out the universally accepted data protection principles describing how personal data may be collected and used. This however, only applies to information that has been obtained through electronic transactions.

The Electronic Communications Privacy Act (ECPA) (US) [53] prohibits the interception of wire, oral or electronic communications by anyone who is not the intended recipient. From a rights perspective, the ECPA only protects individuals' communications against government surveillance conducted without a court order from third parties with no legitimate access to the messages.

In 1997, the European Union (EU) directive on data protection in telecommunications was adopted [54]. Its main function was to restrict marketing activities and access to billing data and Article 6 prescribed that all data collected after each communication must be destroyed.

In many cases, technology is used to strike a balance between the protection of privacy and other competing interests. On the one hand, companies may be legally bound by government to retain data, while on the other hand they are being forced to destroy data for privacy protection. Whichever law is enforced, there are technological mechanisms and techniques available to enhance the preservation of information privacy. This is often referred to as Privacy-Enhancing Technologies (PET).

1.2.2 Privacy-Enhancing Technologies (PET)

In the clash between privacy and advancing technologies, it is sometimes possible to make a compelling argument for overriding the privacy intrusions. However, recent work on privacy is examining the ways in which respect for privacy can be balanced with justifiable uses of emerging technology [9,15]. Technological developments are considered to be the main culprit in increasing concern over the protection of privacy [94]. With the demand for new technological services set to increase, privacy protection will remain at the forefront of debate, from a practical, legal and social viewpoint. Through a privacy taxonomy, [146] endeavours to guide the law towards a more coherent understanding of privacy by identifying a wide range of privacy problems comprehensively and completely. One way of addressing privacy concerns is through the implementation and adoption of a coherent privacy policy. Several works have dealt with privacy and technology, and a collection of essays debating privacy policy can be found in [9].

Over the years much research has been done in the area of privacy in conventional IT-systems and many good solutions have been presented. The term PET is used to describe all types of technologies that provide privacy to a user [78]. Beginning with the publication of the first public key cryptographic methods in the 1970s, mathematicians have constructed a formidable array of protocols for communicating and conducting transactions while controlling access to sensitive information [9]. Typical examples of PETs that use cryptographic techniques include blind signatures [29], partial blind signatures [4] and pseudonym systems [100]. Each of these techniques has its own applications but all of them are based on the assumption that the machines where the computations are performed can be completely trusted. Over the last few years, PETs have evolved rapidly, mainly exploring new techniques in the area of network privacy. Examples include the mix network [28], onion routing [70] and the crowds system [132], [133]. Privacy in these systems is achieved by using the concept of hiding the originator of a message and sending it through a maze of unrelated connected nodes in a network.

In traditional data communications networks, various schemes to ensure anonymity have been proposed. Most have been based on Chaum's so-called mix [28]. Schemes have been proposed that enable anonymous web browsing, anonymous remailers, as well as other applications [70], [68], [66]. Often these schemes ensure anonymity (or pseudonymity) through the use of public key encryption or are based conceptually on the use of a proxy. Privacy is perhaps the most obvious application of cryptography. This is achieved by encrypting the information intended to remain private. Also, privacy can be seen as an aspect of security, one in which trade-offs between the interests of one group and another are apparent.

1.3 Security and Privacy Concerns in Wireless and Mobile Computing

Wireless and mobile computing is a pervasive medium which has defined what has become the information and communication age. Mobile devices provide for a multitude of facilities including voice calls, internet access and storage of personal information through a myriad of integrated mobile applications and wireless connectivity. Many mobile applications and new wireless technologies however also introduce concerns surrounding security and privacy. These include issues relating to anonymity, confidentiality, integrity, availability, accountability and legitimacy of use [14]. Together with other issues they are currently introducing new interests, areas of research, debate and potential solutions and will undoubtedly continue to warrant investigation regarding privacy concerns in the future.

Various security and privacy threats to wireless and mobile computing include - and are not restricted to - information extraction, monitoring, eavesdropping, violation of personal information, integrity/ identity theft, illegitimate use, fraud and unaccountability. These security and privacy threats exist due to the underlying infrastructure and fundamentals of wireless mobile computing and are exacerbated due to user mobility; the mobile device itself, and wireless connectivity and network integration.

Some measures to increase security and preserve privacy exist in traditional data communications networks. They include authentication, authorisation, confidentiality, data integrity, logging, auditing and intrusion detection [14]. However, supplying such measures in mobile communications networks may become the root of concern for privacy infringement. This is evident where in a mobile communications environment the underlying architecture is governed by a controlling authority (network provider).

1.4 Problem Statement

The ultimate goal of this thesis is to suggest ways in which to protect privacy in a mobile voice communications environment, from a technological perspective and in a proactive manner. Using the Global System for Mobile communications (GSM) as reference, we hope to identify novel techniques for privacy assurance across all areas within the network infrastructure. This study provides a basis for defining privacy principles that may apply to Next Generation Networks (NGN):

- Firstly, we present a suggested means of preserving privacy in the mobile communications environment in its entirety by dividing mobile communications environments into clearly defined areas and concentrating on privacy concerns in each.

- We investigate privacy concerns, taking each network segment in iso-

lation and apply privacy-preserving mechanisms.

- Lastly, we conduct a privacy analysis on the privacy-preserving mechanisms used.

Mobile voice communications has changed the way we interact with each other allowing for communication using a variety of communication mediums by means of a magnitude of interactive mobile devices. The context, content, persons communicating, situation and timing all have a varying degree of influence on the sensitivity of information shared during communication. Mobile communications environments facilitate communication, turning the exchange of communicative information into profits for the network operators. As privacy-sensitive information travels through a network, it may be exposed to privacy infringement at various stages along its journey. Unexpected information flow that causes a privacy violation can occur in the following areas: billing, roaming, routing, location, numbering schemes, communication channelling and forensic investigation. Finding a truly private end-to-end mobile communications network is evidently hard. However, if privacy principles are identified (in existing networks) and adhered to (in next generation networks), we converge towards a network infrastructure that possesses a desirable level of privacy protection.

1.5 Methodology

Chapter 1 is essentially a literary study that provides an introduction to privacy. Chapter 2 studies the Global System for Mobile communications (GSM) and Chapter 3 focuses on the privacy concerns in GSM. This background provides detail on the most commonly used mobile communications network in the world today in order to better understand and identify the areas of privacy concern.

Chapter 4 introduces our proposed Private Voice Communications Model, using GSM as a reference for our work. In principle, the private voice communications architecture encapsulates the various components and highlights the identified areas of privacy concern within a mobile network. Our aim is to attain a privacy-preserving mobile communications environment that can be extended to future generation networks. This is achieved primarily through technical intervention and by applying privacy-preserving principles to each identified area of privacy concern. We follow a methodology of evaluation, assessment and technical solution-building in converging towards a privacy-preserving mobile communications network.

Chapter 5 through to Chapter 11 investigates the individually identified areas of privacy concern within the private voice communications architecture. A real-world approach is adopted where possible, providing for privacy-preserving solutions. In Chapter 12, we return to our Private Mobile Voice Communications Model (Chapter 4) in order to ascertain whether

privacy principles learnt in subsequent chapters are applicable to NGN and whether any essential differences exist.

Due to the nature of widespread use and extent of mobile communications technologies, performance and scalability issues around a practical implementation of our privacy solutions, is not always possible. With this in mind, considerable effort has been placed on privacy enhancement techniques and analysis thereof rather than simulation and or actual network configuration and setup.

Lastly, conclusions and referencing are provided.

1.6 Structure and layout of this document

Chapter 1 introduces privacy, expected flow of information and privacy protection. A problem statement and methodology describe our approach towards achieving a privacy-preserving mobile communications network.

Chapter 2 introduces the Global System for Mobile Communication (GSM), provides a detailed overview of the GSM architecture and focuses in particular on security-related aspects.

Chapter 3 highlights privacy concerns in mobile communications environments, using GSM as our reference. The seven areas of privacy concern identified include sender and receiver privacy; billing privacy; location privacy; roaming privacy; legal privacy; communication channel privacy, and numbering scheme privacy.

Chapter 4 proposes a Private Voice Communications Model and takes into consideration the areas of privacy concern highlighted in Chapter 3. A mathematical approach provides a more formal description of privacy requirements.

From Chapter 4 onwards, the work presented in each chapter is that of the author's original contribution to privacy in mobile voice communication networks. Where necessary an extensive literary background on each topic is provided.

The next seven chapters describe our Private Voice Communications Model in more detail and focus specifically on each of the seven areas of privacy concern.

Chapter 5 introduces sender and receiver privacy. We cover the use of trusted third party proxies and anonymous channelling in order to achieve sender and receiver privacy.

Chapter 6 introduces various means of ensuring privacy through the number schemes used in mobile communication identification. Various techniques investigated include the receiver assigning a new identity (known only to the receiver) to the sender; identification through zero-knowledge, effectively proving knowledge of an identity without revealing any information, and secret sharing between the sender and receiver.

Chapter 7 explores public cryptography, the theory of compatible keys

and billing data anonymity models as a means to provide anonymous billing channels.

Chapter 8 investigates how privacy is preserved when a subscriber roams away from his/her home network. We introduce a Privacy-Preserving Roaming GSM Architecture to combat possible privacy violations of subscriber data from foreign network service providers.

Chapter 9 provides a privacy-preserving means of conducting a forensic investigation by balancing the competing priorities of security, privacy and forensics on data records where accountable privacy is the goal. This is achieved through the release of individual pieces of information that comprise stored information. We begin with a prior verified hypothesis (based on suspicion) and formulate a self-preserving object that releases private information without unduly compromising the suspect's privacy and security.

Chapter 10 introduces communication channel privacy techniques such as codec-hopping and non-interactive key exchange.

Chapter 11 introduces a prohibitive contract as a mechanism for ensuring location privacy. Given the possible strategies of the subscriber and the network operator, as well as the corresponding cost for each, we show that a privacy equilibrium can be found. This equilibrium is expressed in the form of a prohibitive contract which neither subscriber nor network operator may violate. Should a violation occur, the debased opponent is rewarded. An example is presented utilising the utilitarian paradigm approach for evaluating efficiency, which postulates convergence towards an overall balanced system.

Chapter 12 revisits our Private Voice Communications Model from Chapter 4 and determines if privacy principles learned from GSM are applicable and provide a degree of privacy assurance in Next Generation Networks (NGN). Chapter 12 reflects on current and future work and concludes the thesis.

It is important to note that this dissertation contains a large number of abbreviations and acronyms due to the fact that specific technical terms are used within mobile communications networks. Hence, a complete list of abbreviations and acronyms has been provided for the reader in the Appendix.

The details of all referenced material are provided in the Bibliography.

1.7 Conclusion

This Chapter has dealt with definitions of privacy, reasons for its importance, and suggestions of how it may be ensured with the aid of technology. A formal problem statement and methodology was provided, outlining our goal of achieving a privacy-preserving mobile voice communications network.

Chapter 2

Global System for Mobile Communications

2.1 Introduction

The Global System for Mobile Communications (GSM) is a common telecommunications standard originally issued by the European Telecommunications Standards Institute (ETSI) [55]. GSM is an open standard which is currently developed by the 3rd Generation Partnership Project (3GPP) [1]. GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but does not address the hardware specifically. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers.

The name GSM first comes from a group called Group Special Mobile (GSM), which was formed in 1982 by the European Conference of Post and Telecommunications Administrations (CEPT) to develop a pan-European cellular system that would replace the many existing incompatible cellular systems already in place in Europe. However, when GSM service started in 1991, the abbreviation "GSM" was renamed to Global System for Mobile Communications from Group Special Mobile.

GSM has become an international cooperation and collaboration between people, companies and governments, creating a truly global wireless communication network. At the time of writing, GSM service had surpassed the 3 billion people mark and is currently available across more than 214 countries and territories worldwide [72].

GSM differs from first generation wireless systems in that it uses digital technology and time division multiple access transmission methods. GSM is a circuit-switched system that divides each 200kHz channel into eight 25kHz time-slots.

The decision to position our work in the GSM context is based on the popularity of GSM. All previous work from the author forms part of an

ongoing interest in mobile privacy and security projects [36,37,39–41,43,102] set in the GSM and next generation communication context. It is important to note that although concepts presented in this thesis apply directly to GSM, we later focus on what GSM may teach us for creating a private Next Generation Network (NGN).

2.2 GSM Architecture

The GSM network architecture [36,128] can be divided into four parts. The Mobile Station, the Base Station Subsystem, the Network Switching Subsystem and the Operation Subsystem. The Mobile Station and the Base Station Subsystem communicate across the air interface or radio link while the Base Station Subsystem and the Network Subsystem communicate across a fixed network.

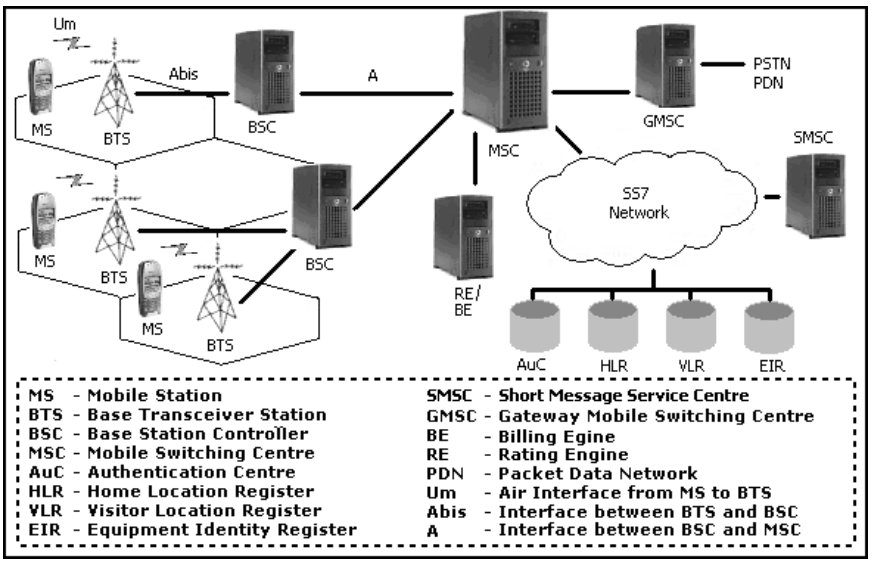

Figure 2.1: GSM Network Architecture

2.2.1 Mobile station

The Mobile Station (MS) provides access to the GSM network. The MS consists of Mobile Equipment (ME) and a Subscriber Identity Module (SIM) [58]. The mobile equipment is uniquely identified by what is referred to as the International Mobile Equipment Identity (IMEI). The SIM card stores the sensitive information such as a unique identifier called the International Mobile Subscriber Identity (IMSI) and a secret key for authentication called K_i. The IMSI consists of three parts, namely [63]:

1. Mobile County Code (MCC) - 3 decimal digits

2. Mobile Network Code (MNC) - 2 decimal digits

3. Mobile Subscriber Identification Number (MSIN) - 10 decimal digits

where MSIN is unique for a MCC/MNC combination. All this information may be protected on the MS by personal identity number (PIN). In 3GPP terminology, MSISDN (Mobile Subscriber ISDN Number) refers to the telephone number of a mobile subscriber and has a direct relationship with the IMSI number on the serving GSM network.

2.2.2 Base Station Subsystem

The Base Station Subsystem (BSS) is responsible for handling traffic and signalling between a MS and the Network Switching Subsystem. The BSS carries out the coding of speech channels, allocation of radio channels to MS, paging, quality management of transmission and reception Over The Air (OTA) interface among other tasks related to the radio network.

The Base Station Subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The Base Station Controller manages the radio resources for one or more BTS. It handles channel setup and handover when the MS travels to another BTS. The BSC is the connection between the MS and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network (PSTN).

2.2.3 Network Switching Subsystem

The Network Switching Subsystem (NSS) is the main component of the GSM mobile network. Its main responsibilities include: GSM switching, mobility management, interconnection to other networks and system control.

The central component of the Network Subsystem is the Mobile Switching Center (MSC). The MSC provides the connection to the public fixed network (PSTN), and signalling between functional entities using the ITU-T Signalling System Number 7. This is more commonly known as the SS7 network [97]. The MSC thus has an interface to one or more BSCs and to external networks.

Several databases are available for control and network management. It is important that these databases are scalable, have high capacity and low delay. The following databases are usually considered to be part of the MSC [36]:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Centre (AuC)

- Equipment Identity Register (EIR)

The Home Location Register (HLR) is a central master database containing permanent and semi-permanent data for all registered users with a network operator. Permanent data would include the user's profile while semi-permanent data could include the current location of a subscriber. One network provider may have several HLRs, but it may be implemented as a distributed database.

The Visitor Location Register (VLR) is a local database for a subset of subscriber data, including data about all subscribers currently in the geographical area controlled by the VLR. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time. Although each functional entity can be implemented as an independent unit, most manufacturers of switching equipment almost always integrate the VLR together with one MSC.

The Authentication Centre (AUC) is a protected database that authenticates each SIM card that attempts to connect to the GSM. The AUC does not engage directly in the authentication process, but instead generates data known as **triplets** for the MSC to verify a subscriber. The security of the process depends upon a shared secret between the AUC and the MS (stored on the SIM) called K_i. The K_i is securely burned into the SIM during the manufacturing process and is also securely replicated at the AUC. This K_i is never transmitted between the AUC and MS, but is combined with the IMSI to produce a challenge/response for identification purposes. An session key called, known as K_c, is used in over the air communications.

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its unique International Mobile Equipment Identity (IMEI). Stolen or malfunctioning mobile stations can be locked and sometimes even localised by the network operator according to the IMEI.

2.2.4 Operation Subsystem

The Operation Subsystem (OSS) enables centralised operation, management, and maintenance of all GSM subsystems. The purpose of OSS is to offer the customer cost-effective support for centralised, regional, and local operational and maintenance activities. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organisations.

2.3 GSM Security Model

The key function of GSM security elements is: privacy, integrity and confidentiality. However, the use of radio communications for transmission to the mobile subscribers makes GSM particularly sensitive to misuse with regards to resources. Unauthorised Mobile Stations, who impersonate authorised subscribers and eavesdroppers are just some threats to mobile information, which is exchanged on the radio path. The main security features in GSM is to protect: i) The access to the mobile services and ii) any relevant item from being disclosed on the radio path, mainly in order to ensure the privacy of user-related information.

2.3.1 GSM Security Algorithms

Three algorithms are used in the GSM Security Model and each has a different purpose. These are: A3 — Mobile Station Authentication Algorithm, A5 — Over The Air (OTA) Voice-Privacy Algorithm, A8 — Voice-Privacy Key Generation Algorithm. The GSM consortium followed a policy of security byobscurity with these algorithms; which means that all of the algorithms used are not available to the public.

2.3.1.1 The Mobile Station (MS) Authentication Algorithm (A3)

The A3 algorithm is the authentication algorithm in the GSM Security Model. Its function is to generate a $SRES$ response to the RAND, which the MSC received from the HLR. The A3 algorithm takes the 128-bit RAND it receives via the MSC and the 128-bit K_i that resides on the SIM card as inputs and generates a 32-bit output.

$$(RAND, K_i) \bullet \mathbf{A3} \rightarrow SRES \tag{2.1}$$

2.3.1.2 The Voice-Privacy Key Generation Algorithm (A8)

The A8 algorithm is the key generation algorithm in the GSM Security Model. Its function is to generate a Session key (K_c). The A8 algorithm takes the 128-bit $RAND$ and 128-bit K_i as inputs and generates a 64-bit output. This output is the 64-bit Session key (Kc), see [23] for "C" code implementation. The Session key (Kc) is used until the MSC decides that the Mobile Station (MS) needs to be re-authenticated.

Nearly every GSM operator in the world uses an algorithm known as "COMP128" for both A3 and A8 algorithms [121]. The COMP128 algorithm takes the 128-bit $RAND$ and 128-bit K_i as inputs and produces a 128-bit output. The first 32 bits of the 128 bits form the $SRES$ response [23]. The last 54 bits of the COMP128 output form the session key. Note that the key length is 54 bits and not 64 bits, ten zero bits are appended

to the K_c generated by the COMP128 algorithm. This effectively increases the key space to the required 64 bit Session K_c.

$$(RAND, K_i) \bullet \mathbf{A}8 \rightarrow K_c \tag{2.2}$$

2.3.1.3 The Over The Air (OTA) Voice Privacy Algorithm (A5)

Only Over The Air (OTA) traffic is encrypted in the GSM network. The A5 algorithm, which is a stream cipher, is responsible for this. The stream cipher is initialised for every frame (or voice packet) that is sent Over The Air. The A5 algorithm takes as input the Session key (K_c) and a 22-bit frame number. The same K_c is used throughout GSM communication, however the frame number changes, which results in the generation of a unique key stream for every frame [10]. The A5 algorithm consists of three LSFRs of different lengths [138]. The LSFRs are 19, 22 and 23 bits long with sparse feedback polynomials with a combined length of 64 bits [121]. 228 bits of key stream are generated as output from the A5 algorithm. The first 114 bits are used for MS to BTS encryption, while the next 114 bits are used for BTS to MS encryption. The A5 algorithm is re-initialised with the same K_c and the number of the next frame [10]. Once the frames have been received by the Base Transceiver Station (BTS), the frames are decrypted and sent in plaintext to the operator's backbone network [36].

$$(K_c, FrameNumber) \bullet \mathbf{A}5 \rightarrow keystream \tag{2.3}$$

2.3.2 GSM Authentication Protocol

The authentication process in GSM is based on algorithms A3, A5 and A8, in such a way that A5 is responsible for communication encryption between MS and BS using a session key K_c, once MS has been authenticated. This authentication requires MS to compute a response $SRES_m$ to the challenge RAND received from BS, using A3 and the secret key K_i, that is,

$$SRES_m = A3(K_i, RAND) \tag{2.4}$$

The same challenge $RAND$ is then used to compute the session key

$$K_c = A8(K_i, RAND) \tag{2.5}$$

When a GSM subscriber turns on his phone for the first time, its IMSI is transmitted to the AuC on the network. After which, a Temporary Mobile Subscriber Identity (TMSI) is assigned to the subscriber. The IMSI is rarely transmitted OTA after this point. This prevents a potential eavesdropper from identifying a GSM subscriber by their IMSI. The subscriber continues to use the same TMSI, until such time as a location update occurs. When this happens, the network assigns a new TMSI to the mobile phone. The

TMSI is stored along with the IMSI in the network. The mobile station uses the TMSI to report to the network or during call initiation. Similarly, the network uses the TMSI, to communicate with the MS. The Visitor Location Register (VLR) performs the assignment, the administration and the update of the TMSI. When the MS is switched off, it stores the TMSI on the SIM card to make sure it is available when it is switched on again.

The authentication process (refer to Figure 2.2 begins when a user MS changes his location. At this time, MS sends to VLR an authentication request containing his temporal identification TMSI and the Location Area Identity (LAI). A GSM network is divided into cells. A group of cells is considered a Location Area (LA). A mobile phone in motion keeps the network informed about changes in the location area. If the mobile moves from a cell in one location area to a cell in another location area, the MS performs a location area update to inform the network about the exact location of the mobile phone. The new VLR obtains the real MS identity IMSI from the old VLR using TMSI. Then the VLR tells the HLR the identity of the user who is requesting the authentication. The Authentication Centre (AuC) is responsible for generating the following set of three values, known as triplets: i) Random number ($RAND_i$) ii) Signed response ($SRES$) and iii) Session key (K_c). When HLR receives the request, it generates n triplets ($RAND_i$, $SRES_i$, K_{c_i}) and sends them to the new VLR.

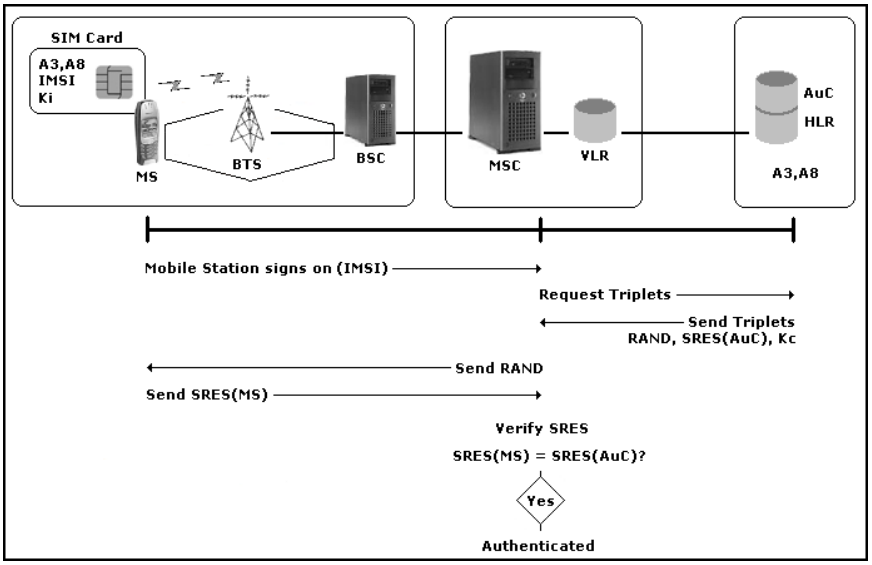

Figure 2.2: GSM Subscriber Authentication Process

The VLR receives the triplets and stores then in the database. Next, the VLR selects a triplet to authenticate the MS, and sends $RAND_i$ to MS. When MS receives $RAND_i$, the response $SRES_m$ is computed and returned to VLR. MS also computes the session key K_c. Finally, the VLR compares

$SRES_i$ with $SRES_m$. If this matches, then the MS is authenticated.

2.4 Problems with GSM Security

Much research has been conducted on the security aspects of GSM. Agarwal et al. [6] recently extended GSM security by using identity-based cryptography, however, the problems with GSM security stem largely from design limitations rather than defects in the security features themselves. Design limitations within GSM can be summarised as follows:

- Access security, communications and signalling in the fixed portion of the network are not protected.
- Does not address active attacks, where networks elements may be impersonated.
- Designed with integration in mind to existing networks and thus are only as secure as their fixed line counterparts.
- Lawful intercept only considered as an after thought.
- Inadequate flexibility to upgrade and improve security mechanisms over time.
- Lack of visibility that security is being applied, no indication that encryption is on, and more importantly, no explicit confirmation to the home network.
- Unilateral identification, subscriber authenticated to network, network not authenticated to the subscriber.
- No data integrity algorithm provided for.
- Unsecured terminal, IMEI is an unsecured identity.
- Potential use of false BTSs.

Problems specific to GSM's security model are summarised as follows:

- Security by obscurity. Most security analysts believe any system that is not subject to the scrutiny of the world's best minds can't be as secure.
- Only provides access security. All communication between the Mobile Station and the Base Transceiver Station are encrypted. But all communications and signalling is generally transmitted in plaintext in the fixed network.
- Difficult to upgrade the cryptographic mechanisms.

- Cryptographically weak algorithms.
- Lack of confidence in cryptographic algorithms, lack of openness and design and publication of A5/1 , key length too short (K_c uses only 54 bits of the 64 bits making the cipher key purposefully weaker).
- Clear transmission of cipher keys and authentication values in and between networks.

Having identified the immediate threats to GSM security, how can these be exploited and in turn possibly infringe on a subscribers privacy? Possible interception attacks include [121]:

- Brute-force attack against the A5 algorithm.
- Divide-and-Conquer attack against the A5 algorithm.
- Retrieving the K_i from the SIM and or AuC.
- Retrieving the K_i from the SIM Over The Air (OTA).
- Cracking the A8 algorithm.

GSM SIM cards have also been cloned through partitioning attacks [129]. It has been shown how to break the COMP128 authentication algorithm; an instantiation of A3/A8 widely used by providers [67]. The attack is a chosen-challenge attack. A number of specially chosen challenges are formed and the SIM is queried for each one; the SIM applies COMP128 to its secret key and the chosen challenge, returning a response. By analyzing the responses, it is possible to determine the value of the secret key K_i. Mounting this attack requires physical access to the target SIM, an off-the-shelf smartcard reader, and a computer to direct the operation. The attack requires one to query the smartcard about 150,000 times [67]. Very little extra computation is required to analyze the responses.

Such inception and cloning attacks have a privacy impact on not only the subscriber's communication but also on personal identifying information. From a networks perspective, its capacity in providing a privacy protective environment may be severely affected.

2.5 Conclusion

This chapter provided background literature on the GSM architecture and GSM security model. It is clear that the problems associated with GSM security have a direct impact on possible privacy threats in GSM. There is a real and definite likelihood that currently before, during, or after the GSM network activity, a subscriber's personal or communication privacy-sensitive information may be revealed. A combination of one-way identification, weak cryptographic algorithms, difficulty in upgrading cryptographic algorithms,

data integrity concerns and various possible design flaws aggregate a subscribers privacy concern.

The next chapter focuses entirely on these concerns and aims to categorise the areas where privacy may be infringed upon.

Chapter 3

GSM Privacy

3.1 Introduction

Mobile communications have grown tremendously over the last decade; however little attention has been directed to addressing privacy concerns around mobile interactions. Few mobile subscribers are aware that their serving GSM Network holds sensitive information regarding every aspect of the mobile users communications which is monitored, logged and could potentially be compromised. Such information includes personal information such as banking details, place of residence, and associated communication information such as location, movement and - in particular - with whom the user communicates on a daily basis.

The Global System for Mobile communications (GSM) [128] provides a degree of privacy to its subscribers: GSM caters for privacy by encrypting voice communication and allowing its users to control whether a called party gets the caller's phone number (known as Call Line Identity or CLI). However, GSM requires that a subscriber trusts their service provider with details such as calls made and received, billing information, roaming information and location information. It has become apparent that the extent to which GSM addresses privacy is not comprehensive enough. From the design and security limitations of GSM, highlighted in Chapter 2, it is evident that there are specific areas of concern which hold a direct relationship and bearing on privacy.

This chapter highlights current privacy concerns in mobile communication using GSM as a reference. It lends itself to the formalisation of the proposed Private Voice Communications Model in Chapter 4. It focuses on real and potential threats and subdivides these into distinct areas of privacy concern. Each of these privacy threats are individually addressed in chapters 5, 6, 7, 8, 9, 10 and 11. Our aim is to identify each specific privacy threat and investigate possible technical solutions that thwart these concerns by enhancing privacy.

3.2 Mobile Communication Privacy Concerns

Any communications environment where information pertaining to the parties involved, what medium was used, where the communicating parties are located and when communication took place, and how this is billed for constitutes information that is private in nature. Mobile communication environments are no different and encompass these and other privacy-sensitive network components in facilitating basic mobile voice communication. Mobile communication contains varying degrees of privacy-sensitive information held at different stages in the communication process, which is controlled and maintained by the network operator. For example, all information regarding who performed the network transaction is classified as sender information. The recipient of this communication, constitutes receiver information. Identification of the sender and receiver is provided for using a designated number, which forms numbering scheme information. Likewise, where the sender and receiver communication transpired, is dually classified as location information. All information is classified and categorised, in this case, according to basic mobile voice communication requirements needed in aiding real-time interactive communication. It is apparent that trying to solve privacy as a broad based view across the entire mobile communications environment is unrealistic, given the parties involved, network components and information surrounding mobile communication. Thus, before privacy concerns can be addressed holistically, we choose to firstly identify and categorise each area facilitating mobile communication. By doing this, privacy concerns are specifically addressed more concisely at each phase in the communication process. The areas identified, using GSM as a reference, includes the existence of a sender, a receiver, a communication medium, the sender's and receivers location, the time of communication and finally the network operator charge. In addition, government regulation might require access to network communication information for legal purposes in the event that a forensic investigator needs to conduct a digital investigation.

We briefly address each of these areas in terms of privacy concern in the remainder of this section:

- Sender and Receiver Privacy
- Numbering Scheme Privacy
- Billing Privacy
- Roaming Privacy
- Legal Privacy
- Communication Channel Privacy
- Location Privacy

3.2.1 Sender and Receiver Privacy Concerns

In any context, when two parties communicate, certain personal information is susceptible to a privacy violation during or even after the communication. An underlying controlling authority is a prerequisite in managing, relaying and providing infrastructure needed to support mobile communication. The fact that all communication is controlled by the network, without immediate transparency, confirms suspicion from subscribers that private information may be abused. The sender and receiver must retain a degree of control over their privacy-sensitive information and have confidence in the fact that personal information is not misused or disseminated to a third party. The sender and receiver may wish to keep their identity private, thus remaining anonymous to each other and the underlying network. Furthermore it may be required that communication is unlinkable to the sender or receiver. However, in the context of a mobile network, providing anonymity poses potential problems in areas such as billing, roaming and forensic ability.

3.2.2 Numbering Scheme Privacy Concerns

Each subscriber is identifiable on a network by an assigned mobile number (MSISDN). A numbering scheme is assigned to each subscriber by the network provider and is based on internationally governed country and network calling codes. An MSISDN is unique to each subscriber. Therefore, in order to initiate communication, the sender must know the receiver's mobile number. Likewise, the network provider must use this assigned identity in finding subscribers and routing communication appropriately. The privacy concern is highlighted by the fact that once known, a mobile number can be distributed in a public domain. Once the mobile number is known by an untrusted third party, the client can be targeted to receive unsolicited communication.

3.2.3 Billing Privacy Concerns

Billing is an integral part of a network operator's infrastructure. Its core functions include storage of communication detail, rating systems and managing of charges for all subscriber activity on the network. The network is required to perform accurate billing while not revealing the users privacy-sensitive information.

In the current mobile communication networks, a subscriber thus requires an undeniable means of ensuring billing information integrity should a dispute arise with the serving network operator.

Distributed billing systems or billing for mobile content (e.g. ringtones, wallpapers) by a third party, results in subscribers receiving itemised bills from different service or content providers. This provides an additional privacy concern, having external parties contribute to privacy-sensitive billing

information.

3.2.4 Roaming Privacy Concerns

Mobility complicates the process of identifying subscribers. A typical scenario arises when a mobile user registered in one domain appears in a different foreign domain. In order to obtain services in the visited domain, the user must be authenticated and his solvency must be confirmed to the visiting domain by his home authority [150]. To receive service from the visited domain, the subscriber provides an unambiguous identity to the visited domain to be confirmed by the home domain. This is primarily for cross domain billing to occur at a later stage.

A central repository of foreign billing records, contains large amounts of privacy-sensitive network event data of roaming subscribers. The home network and roaming subscriber has no control as to the extent to which these billing records are analyzed, stored and transferred. Furthermore, all communication conducted by the visiting subscriber is susceptible to abuse in the foreign domain.

3.2.5 Legal Privacy Concerns

People store private information on their phones, thus making the mobile itself a rich source of potential evidence for law enforcement officials. Likewise, stored network information for the purpose of billing a subscriber contains sensitive information which may be used in conducting a forensic investigation.

Once a decision is made to proceed with a forensic investigation, current techniques do not allow for the accused to return to the original privacy-preserving state prior to the investigation. Furthermore, a subscriber is unaware of what information is made available to a forensic investigator, and has no direct control over this information.

The problem exists in presenting a privacy-preserving means to conducting a forensic investigation on stored information where accountable privacy is the goal, while providing a balance between the competing priorities of security, privacy and forensics.

3.2.6 Communication Channel Privacy Concerns

During mobile communication, sensitive information travels over the air waves and through the underlying network infrastructure. This information is susceptible to interception from an eavesdropper or manipulation from a third party.

Traditional voice compression techniques do not fulfil security and privacy requirements. Encryption techniques, may be one form of ensuring security and privacy on a communication channel medium. However, in

mobile voice communication environments available bandwidth may restrict the use of strong encryption algorithms resulting in insufficient protection of this privacy-sensitive information. As voice communication is a real-time medium, encryption may significantly slow the voice rate resulting in unrecognisable speech. The trade off exists, to provide audible voice communication while maintaining a level of security and privacy which is acceptable to the subscriber.

The controlling authority has a direct influence on communication traffic passing over its network. Furthermore, communication information may exist in the "clear" within the network at a stage where conversion between different voice compression algorithms is needed.

3.2.7 Location Privacy Concerns

Location information is sensitive information and is considered of high importance to individuals as it places a person at a particular place and time. Individuals should be able and free to explicitly identify what location information is divulged, under what circumstances this can take place, and how this information is communicated across a network. This information is leaked and can be collected as a side effect of most wireless communication and can be valuable [47]. Knowledge of client location is a privacy concern and can be calculated using methods such as proximity and triangulation [8].

Mobile phones communicate with a BTS in order to connect to a network. Subscribers communicate with various BTSs as they move and roam around on the mobile network. Therefore, the mobile network must know the location of subscribers in order to route calls between subscribers. The problem is evident. How can location privacy be retained when this information is necessary in connecting communicating parties? The risks associated with the unauthorised disclosure, collection, retention and usage of location data are highlighted in [108].

3.3 Conclusion

This chapter highlighted the identified areas of concern in a mobile communications environment making specific reference to GSM. GSM, a popular mobile communications network, provides an ideal platform to build on privacy related issues as both security and privacy have not been comprehensively addressed.

In the next chapter we assemble these privacy concerns and compose a generic private mobile voice communications architecture. This lends itself to our proposed Private Mobile Communications Model and formal mobile communication privacy requirements. The architecture is accompanied by an adversarial / threat model.

Chapter 4

Private Mobile Voice Communications Modelling

4.1 Introduction

With billions of privacy-sensitive communications transactions taking place each day, the potential abuse of private communication information is extensive. Few mobile subscribers realise that their serving network holds sensitive information regarding every aspect of mobile users' communications, and that such information is monitored, logged and potentially open to privacy violation.

Some formal language notations have been proposed to standardise telecommunications systems. These include the Comité Consultatif International Téléphonique et Télégraphique (CCITT) which began work in 1976 on standardising SDL [142] (Specification and Description Language, Z.100). Similarly, ISO began work in 1980 on standardising Estelle [82] (Extended Finite State Machine Language, ISO 9074) and LOTOS [99] (Language Of Temporal Ordering Specification, ISO 8807) for formal specification of open systems standards [149]. All three languages have reached a stable state and are widely applied in specifying communications standards. However, no language extends itself to private mobile voice communications.

We chose not to focus our attention on any formal languages presented for telecommunications thus far. Instead, we describe a generic Voice Communications Architecture that forms the premise for our Voice Communications Model by identifying various components where privacy concerns arise (refer to Figure 4.1). This lays the foundation for the remainder of the work presented in this thesis.

As can be recalled from Chapter 3, the areas of concern include sender and receiver privacy; numbering scheme privacy; billing privacy; roaming privacy; legal privacy; communications channel privacy, and location privacy. Each of the following seven chapters suggests technical and theoretical solutions in combating these privacy concerns in mobile voice communica-

tions networks. We investigate privacy concerns in detail, apply privacy-preserving solutions and conduct a privacy analysis in order to confirm findings in each of the seven identified areas.

Our philosophy applies privacy properties from ISO 15408 to our Private Mobile Communications Model. For preciseness, we choose to formally adopt the privacy properties in ISO 15408 [83] namely anonymity, pseudonymity, unlinkability and unobservability within the mobile communications environment context. Formal privacy requirements provide for a theoretical dispensation of private mobile communications and ensure privacy in adhering to these privacy properties (refer to Chapter 1).

The model used will constitute a basis for our evaluation of and recommendations for privacy principles in Next Generation Networks (NGNs).

4.2 Private Mobile Voice Communications Architecture

In Figure 4.1, numbers one through seven highlight the possible threats for a privacy infringement in a mobile voice communications network.

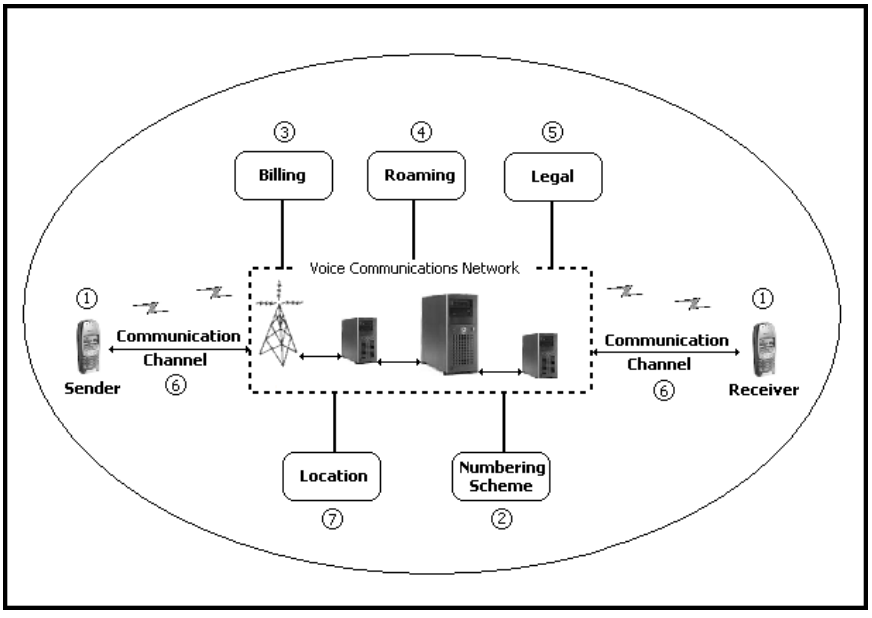

Figure 4.1: Private Voice Communications Architecture

In any voice communications network, the subsystem encompasses the following elements that each has specific privacy concerns:

1. Subscribers participating in communication
2. A numbering scheme, used for identification of subscribers
3. Billing information storage

4. Integration with legacy systems and other networks
5. Legal and forensic ability
6. Underlying communications network, core network acting as network facilitator combined with media transfer gateways
7. Location of subscribers in the network

Informally, for mobile voice communication to take place, there exists a need for inter-operation between these subsystem components. Each component may have a direct bearing on security, privacy and operation of other components.

One cannot hope to to defend against all types of security and privacy threats, however we articulate a threat model which examines the data flow between network components. For each component we illustrate (refer to Figure 4.2): i) Trust and machine boundaries (shown as dotted half and full circles respectively) ii) Flow of data (shown as arrows) and iii) External interactors (shown as rectangles). A trust boundary occurs when one component doesn't trust the component on the other side of the boundary while a machine boundary occurs when data moves from one machine to another. An external interactor is an element that is outside the networks control. The aim is to review privacy threats an identify mitigation techniques and technologies in each instance.

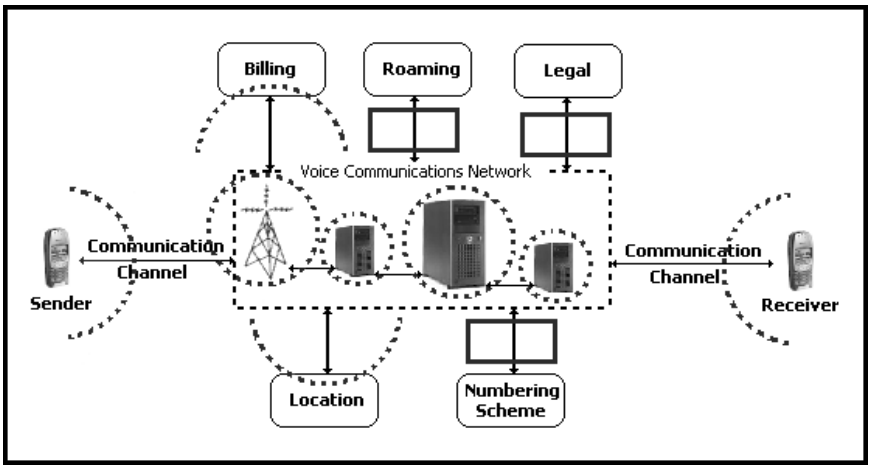

Figure 4.2: Private Voice Communications Threat Model

There may exist several other privacy concerns similar in nature to micro-data disclosure [49], anonymity via clustering [7, 25] and statistical inference [136], however this work concentrates its efforts on privacy from a user anonymity point of view.

4.3 Formal High-Level Private Mobile Voice Communications Modelling

The Unified Modelling Language (UML) is a standardised specification language for object and system component modelling. UML includes a graphical notation set used to create an abstract model of a system, often referred to as a UML model.

In UML 2 [117] there are 13 types of diagrams. Structure diagrams emphasise the elements that are required in the system being modelled, namely Class diagrams, Component diagrams, Composite structure diagrams, Deployment diagrams, Object diagrams and Package diagrams. Behaviour diagrams emphasise what must happen in the system being modelled, for instance Activity diagrams, State Machine diagrams, Use case diagrams and Interaction diagrams. A subset of behaviour diagrams emphasises the flow of control and data among the elements in the system being modelled. These include Communication diagrams, Interaction overview diagrams, Sequence diagrams and Timing diagrams.

We focus our attention on the component diagram whose main purpose is to show the structural relationships and interaction between the components of a system. This is ideal for the representation of a mobile voice communications network where components disseminate across the network architecture and yet are tightly coupled. UML 2 officially changes the essential meaning of the component concept. In UML 2, components are considered as autonomous, encapsulated units within a system or subsystem that provides one or more interfaces.

In component diagrams, components are represented as rectangular classifiers. Connectors illustrate communication links between parts to fulfil the structure's purpose. Each connector end is distinct, controlling the communication pertaining to its connecting element. The assembly connector (represented by a ball and half circle) bridges a component's required interface (from Component 1) with the provided interface of another component (to Component 2); this allows one component to provide the services that another component requires.

In the next section we choose to represent our Private Mobile Communications Model using a composite UML structure in the form of a component diagram. The diagram shows the relationships among components involved in mobile voice communications.

4.4 Mobile Communications Network Components

In order for a sender and receiver to communicate, a form of identifying the subscribers is essential. Currently, numbering plans (like those present in GSM) allow for the identification and discovery (location) of subscribers in the network. Likewise, a communications channel carries messages between

subscribers using the underlying infrastructure. In any communications environment, these components constitute the basic requirements for voice communication. Billing forms an immediate encompassing layer required to charge subscribers for communicating. At this stage, a network service provider manages, controls and facilitates communication in conjunction with billing services. Figure 4.3 illustrates a composite UML structure in the form of a component diagram for a mobile voice communications network.

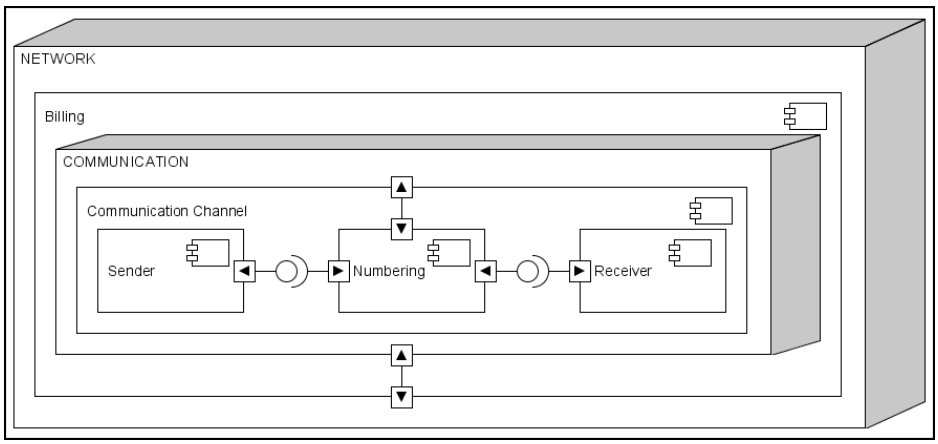

Figure 4.3: Mobile Communications Network Domain - UML component diagram

Communicating subscribers may not necessarily reside in the same domain; one or both may be roaming in a foreign domain managed by a foreign network service provider. Roaming is permissible and communication across domains valid only if a subscriber is billable in a foreign domain. In such cases, this is made possible via a roaming agreement that stipulates interconnection charges between network service providers. Furthermore, for forensic purposes, any legal authority may require access to any information in the communication system. However, in such a case a degree of trust in the legal entity is imminent from both the subscriber and network service provider's standpoint. Seeing that there is inter-operation between subsystem components, enforcing privacy at each level is a pre-requisite for communication to take place. Thus, in achieving a private mobile communications network, privacy is administered across all components and domains. Refer to Figure 4.4 for an illustration of our Mobile Communications Network Architecture, which provides the basis for privacy analysis.

In order to better understand privacy preservation, we provide a formal privacy component classification that helps to define privacy requirements influenced by component interaction.

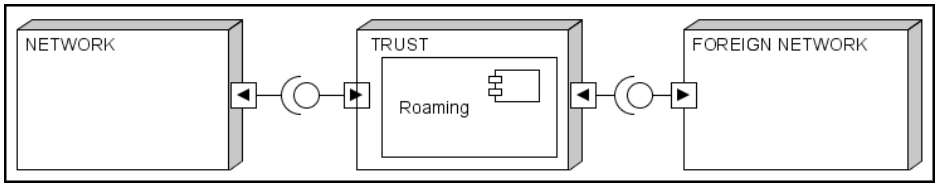

Figure 4.4: Mobile Voice Communications Network Architecture - UML component diagram

4.5 Formal Mobile Communication Requirements

As is clear from Figure 4.3, the following components are necessary for mobile voice communication (denoted by $MComm$) to take place: a sender (S), a receiver (R), a numbering scheme (NS), the location (Loc) of the sender and receiver, a communications channel (C) and a charging method ($Bill$) is required. This is facilitated by an underlying $Network$ (e.g. GSM) that provides the communications environment. Mobile communication ($MComm$) can thus be represented by the following:

$$\begin{aligned} MComm \quad = \quad & \langle NS_{SR}; Loc_{SR}; Comm_{SR}, Bill_{SR} \rangle_{Network}; \\ & \forall \{S, R, NS_{SR}, Loc_{SR}, C_{SR}, Bill_{SR}\} \in Network \end{aligned} \quad (4.1)$$

Informally, a sender and receiver (SR) must each possess a unique identity in a valid numbering scheme (NS) in the $Network$ they must also be locatable (Loc) in the $Network$ and share a communications channel ($Comm$) provided by the $Network$ in order to communicate.

Once communication is complete, the $Network$ imposes a cost associated with the service it provided. Furthermore, should either the S or R be roaming in a foreign domain, communication and billing must be accounted for by the $Network^*$. $Network^*$ indicates a foreign network that has established a roaming agreement with the home serving network. Mobile communication across foreign domains ($MComm^*$) can thus be represented by the following:

$$MComm^* = MComm\ S \cup R \in Network^*; \quad (4.2)$$

Informally, the $MComm^*$ is possible only if there is a roaming agreement between the home and foreign network.

A legal component has access to $MComm$ and $MComm^*$ activities. A legal entity's disposition can be represented as follows, bearing in mind that a degree of trust is placed in the legal entity:

$$Legal = \langle MComm; MComm^* \rangle; 0 \leq Trust_{Legal} \leq 1; \quad (4.3)$$

Once privacy is enforced through privacy-enhancing technologies (see Section 1.2.2), a degree of trust is required if privacy-sensitive information is divulged. Trust, in this case, is placed in any *Legal* entity and in the $Network^*$ as a consequence of possible legal intervention. Trust is an important functional entity and forms the final layer of the model. Trust in it entirety is not dealt with in this thesis but is duly noted as having a potential impact on privacy-related issues.

For private mobile communication, privacy extends across all individual layers of the mobile communications model and constitutes the foundations upon which the Private Mobile Communications Model is built. In the remaining sections, we choose - for the sake of simplicity - to denote the combination of $Network$ and $Network^*$ as simply $Network$.

4.6 Formal Mobile Voice Communications Privacy Requirements

Section 3.2 presented privacy concerns in a mobile communications environment, using GSM as a reference. Ideally, formal definitions allow for a clear understanding as to the goal of obtaining a privacy-preserving mobile voice communications network. Even though they are theoretical, these definitions provide a basis for the privacy principles that real-world solutions are built upon.

We choose to describe these formal requirements using the privacy properties in ISO 15408 [83] namely anonymity, pseudonymity, unlinkability and unobservability within our Private Mobile Communications Model context. We formally describe privacy requirements in the next sub sections as they appear in Figure 4.1.

4.6.1 Formal Sender and Receiver Privacy Requirements

The privacy of a sender (S) and receiver's (R) privacy can be assured by hiding their identities from the $Network$. Choose $\langle S, S_P \rangle$ to represent a sender S that relates to a pseudonym allocated by the $Network$ such that S maps directly to S_P. Likewise, choose $\langle R, R_P \rangle$ to represent a receiver R that relates to a pseudonym allocated by the $Network$ such that R maps directly to R_P. Sender privacy can thus be expressed by the following probabilistic function $[P(\langle S, S_P \rangle | Network) = 0]$, namely that the true identity of S is indistinguishable by the $Network$ through the use of a pseudonymous identity S_P:

$$\forall S, S_P \in Network\ [P(\langle S, S_P \rangle | Network) = 0] \tag{4.4}$$

However, in any finite environment, as is the case in GSM, perfect anonymity is achievable if and only if the associated trusted set is large enough. In practice, anonymity is expressed as a zero limit probabilistic

function because the cardinality of the $Network$ tends towards infinity, given the trusted network of subscribers. This is expressed as follows:

$$\forall S, S_P \in Network \left[\lim_{|Network| \to \infty} P(\langle S, S_P \rangle | Network) = 0\right] \tag{4.5}$$

In the same way, all network communication denoted by an event (e) and performed by the subscriber must remain private. In other words, from a network's perspective, each event is seen as independent from another and unlinkable to the subscriber that performed the event $Network$. Choose O_N to represent the set of events performed by subscribers while connected to the $Network$. More formally, O_N contains any event (e_{P_i}) performed by a subscriber pseudonym (S_P), such that $O_N := \{e_{P_i} : 1 \leq i \leq M\}$ for some $M \in \mathbb{N}$. Let $\langle e_{P_i}, e_{P_j} \rangle_{S_P}$ represent the fact that two independent events (e_{P_i} and e_{P_j} where $i \neq j$) were performed by S_P. Then perfect ***event unlinkability***, given $i \neq j$, is achieved iff:

$$\forall e_{P_i}, e_{P_j} \in O_N \left[P(\langle e_{P_i}, e_{P_j} \rangle_{S_P} | i \neq j) = 0\right] \tag{4.6}$$

Let an event e_P constitute both public and private information denoted by $(p_u || p_r)$, where p_u represents public information and p_r private information. For example, the network cost of the event may be considered public information because no identifying or association information is revealed, whereas the recipient or sender element discloses identity and is therefore seen as private information. Let $\langle e_P, p_r \rangle$ represent the private information contained in an event performed by a pseudonymous subscriber. Perfect ***event unobservability*** of private event information in e_P, given e_P, is achievable iff:

$$\forall e_P \in O_N \left[P(\langle e_P, p_r \rangle | e_P) = 0\right] \tag{4.7}$$

4.6.2 Formal Numbering Scheme Privacy Requirements

Once a mobile number is divulged, it enters the public domain. In other words, once a sender divulges his mobile number (identity) to an intended recipient, the receiver may distribute this identity without the consent or knowledge of the sender.

A private numbering scheme (NS) is one where the identity associated with either the sender (S) or receiver (R) can be instantiated and contained between S and R. This means that the numbering scheme possesses the property of a virtual private numbering system, effectively preventing private subscriber identity information from being exposed into the public domain. Ideally, the numbering scheme used between S and R is difficult to associate given a particular NS. Numbering scheme privacy is thus expressed as the following probabilistic function:

$$\forall S, R \in Network\ [P(\langle SR, NS\rangle | NS_{SR} \in Network) = 0] \tag{4.8}$$

4.6.3 Formal Location Privacy Requirements

The location (Loc) of both the sender (S) and receiver (R) is privacy-sensitive information which the $Network$ requires in order to route calls. The privacy requirement is such that, given the location of S and R, the $Network$ will be able to route calls without knowing the true identity of S or R. In other words, given the sender location Loc_S, the $Network$ will be unable to determine the association between this location Loc and its mapping directly to S. This is expressed by the probabilistic equation:

$$\forall S, Loc_S \in Network\ [P(\langle S, Loc_S\rangle | Loc \in Network) = 0] \tag{4.9}$$

4.6.4 Formal Communications Channel Privacy Requirements

The $Network$ may provide the underlying communications channel, however all communication transpiring from this connection must not indicate the users communicating over the medium. In other words, if a sender (S) and receiver (R) communicate over a communications channel (C), the underlying $Network$ has no means of determining this association. This is expressed by the probabilistic equation:

$$\forall S, C_S \in Network\ [P(\langle S, C_S\rangle | C \in Network) = 0] \tag{4.10}$$

Furthermore, assuming the $Network$ controls the underlying infrastructure, the user who is utilising the communications channel C must not be observable from a network perspective. Thus an event (e) performed by S, given S_P and e_P in a $Network$ is unobservable iff:

$$\forall e_P \in O_N \forall S_P \in Network\ [P(\langle S_P, e_P\rangle | C, S_P, e_P) = 0] \tag{4.11}$$

In practice, pseudonym ***communication event unobservability*** is expressed as a zero limit probabilistic function as the cardinality of the $Network's$ size tends towards infinity (given S_P and e_P). This is expressed as follows:

$$\forall e_P \in O_N \forall S_P \in Network\ [\lim_{|Network| \to \infty} P(\langle S_P, e_P\rangle | C, S_P, e_P) = 0] \tag{4.12}$$

4.6.5 Formal Billing Privacy Requirements

All communication transacting over the $Network's$ infrastructure results in a billable event. As network events contain privacy-sensitive information,

billing privacy constitutes both event unlinkability (see Equation 4.16) and event unobservability (see Equation 4.7). This is combined with subscriber anonymity (see Equation 4.4) in order to hide billable information linked to a particular subscriber and from the underlying $Network$.

4.6.6 Formal Roaming Privacy Requirements

In a mobile voice communications architecture there exists the following three components: a home or trusted network (TN), a foreign or untrusted network (UN), and a subscriber (S) who is connected to either a trusted network ($S \in TN, S \notin UN$) or to an untrusted network ($S \in UN, S \notin TN$). In this context, assume the existence of only two networks, namely TN and UN. Thus, the intersection of the trusted and untrusted network in terms of its connected subscriber base results in an empty set:

$$TN \cap UN = \emptyset \tag{4.13}$$

and conversely the union of the trusted and untrusted network represents the entire connected mobile voice communications network subscriber set:

$$TN \cup UN = Network \tag{4.14}$$

The following are requirements for our architecture: a subscriber (S) that exists in the set of roaming subscribers such that S remains anonymous to the untrusted network ($S \in UN$) and that all events (e) performed by S are unlinkable to S and unobservable to the untrusted network (UN). Each privacy property is expressed as a probability function P, as all sets within the mobile voice communications network context, although large, are finite. In this section, $P(X|Y)$ will be used to denote the probability of some event X, given that the contents of set Y are known. For completeness sake, we also explore perfect versus practical privacy property definitions.

4.7 Perfect versus Practical Privacy Property Definitions

4.7.1 Formal Definition of Roaming Anonymity

From Equation 4.4, which ensures subscriber privacy through a network pseudonym, this anonymity principle is extended to a roaming environment. Choose $\langle S, S_P \rangle$ to represent a sender (S), which relates to a pseudonym allocated by the TN such that S maps directly to S_P. In other words, choose S associated with S_P where S is only known to UN as S_P.

Perfect roaming anonymity, given the trusted network of subscribers, denoted by TN, is achievable iff:

$$\forall S_P \in UN, \forall S \in Network\ [P(\langle S, S_P \rangle | Network) = 0] \tag{4.15}$$

4.7.2 Formal Definition of Roaming Event Unlinkability

Choose O_{UN} to represent the set of events performed by roaming subscribers while connected to the untrusted network. More formally, O_{UN} contains any event (e_{P_i}) performed by a subscriber pseudonym (S_P), such that $O_{UN} := \{e_{P_i} : 1 \leq i \leq M\}$ for some $M \in \mathbb{N}$. Let $\langle e_{P_i}, e_{P_j} \rangle_{S_P}$ represent the fact that two independent events (e_{P_i} and e_{P_j} where $i \neq j$) were performed by S_P while roaming. Then, perfect ***roaming event unlinkability***, given $i \neq j$, is achieved iff:

$$\forall e_{P_i}, e_{P_j} \in O_{UN} \; [P(\langle e_{P_i}, e_{P_j} \rangle_{S_P} | i \neq j) = 0] \tag{4.16}$$

As roaming subscribers are involved in performing an increasing magnitude of network events, the probability of an untrusted network randomly guessing the association between two events decreases. In practice, event unlinkability is therefore expressed as a zero limit probabilistic function because the cardinality of the O_{TN} tends towards infinity given $i \neq j$. This is expressed as follows:

$$\forall e_{P_i}, e_{P_j} \in O_{UN} \; [\lim_{|O_{UN}| \to \infty} P(\langle e_{P_i}, e_{P_j} \rangle_{S_P} | i \neq j) = 0] \tag{4.17}$$

Likewise, let $\langle S_P, e_P \rangle$ represent the direct relationship between S_P who performed an event e_P. Then, perfect ***roaming event unlinkability*** is achieved iff:

$$\forall e_P \in O_{UN} \forall S_P \in UN \; [P(\langle S_P, e_P \rangle) = 0] \tag{4.18}$$

In practice, pseudonym subscriber and event unlinkability is expressed as a zero limit probabilistic function because the product of cardinality UN and cardinality O_{UN} tends towards infinity. This effectively means that the chance of the untrusted network finding a direct relationship through a random guess is negligible if either UN or O_{UN} or both grow infinitely large. This is expressed as follows:

$$\forall e_P \in O_{UN} \forall S_P \in UN \; [\lim_{|O_{UN}| \bullet |UN| \to \infty} P(\langle S_P, e_P \rangle) = 0] \tag{4.19}$$

Now that we have formally defined the desired privacy requirements in a mobile voice communications network, we suggest a possible approach in defining a high-level formal policy for these privacy requirements.

4.8 Formal Definition of a High-Level Mobile Privacy Policy

The Platform for Privacy Preferences (P3P) [35] developed by the World Wide Web Consortium (W3C) is a protocol that allows websites to declare their intended use of information collected from browsing users. P3P

was designed to give users more control of their personal information when browsing.

The Enterprise Privacy Authorisation Language (EPAL) [13] is an XML-based language used to describe and enforce internal enterprise privacy rules. EPAL is used in writing enterprise privacy policies to govern data-handling practices in IT systems according to fine-grained positive and negative authorisation rights. The language uses a client-server architecture, where each action on private information must first be submitted as a formal request to a "privacy server" that processes the request and returns an answer. An EPAL policy defines lists of hierarchies of data categories, user categories and purposes, and sets of (privacy) actions, obligations and conditions. A request includes information on who the requester is, the proposed action, the purpose of the proposed action, and what class of data is being acted upon. The privacy server has a policy in the form of a rule-set and uses a matching algorithm to compare the rules to the requests.

Thus, the main difference between P3P and EPAL, from a specification perspective, is the information focus of each language. P3P statements are data-centric, whereas EPAL rules are access-centric [147]. EPAL language does not define any actions, obligations, purposes or even data classification. Therefore, EPAL is accompanied by what is termed a vocabulary document that is understood and enforced by a computer system.

For our purpose, defining rules around ensuring privacy in a mobile voice communications network is intuitive but may not be absolutely definitive. However, in ensuring privacy at a technical level, it does provide an excellent high-level starting point.

4.8.1 Definition of an EPAL Mobile Communications Privacy Policy

Listing 4.1 describes our associated vocabulary for our EPAL Mobile Communications Privacy Policy.

Listing 4.1: Example EPAL Mobile Communication Privacy Policy Vocabulary

```
<?xml version="1.0"?>

<!-- EPAL Vocabulary definition for mobile communication privacy.-->

<epal-vocabulary version="1.2"
xmlns="http://www.research.ibm.com/privacy/epal"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.research.ibm.com/privacy/epal
epal.xsd http://www.w3.org/2001/XMLSchema xs-dummy.xsd ">
    <vocabulary-information id="MobilePrivateCommunicationVocabulary">
        <short-description language="en">
            Privacy in Mobile Communication Vocabulary
        </short-description>
        <long-description language="en">
            EPAL vocabulary that provides for privacy in mobile communication
        </long-description>
        <issuer>
            <name>Privacy Company</name>
            <organization>University of Pretoria</organization>
```

```
            <e-mail>privacy@up.ac.za</e-mail>
            <address>Pretoria, 1804</address>
            <country>South Africa</country>
        </issuer>
        <location>http://www.privacy.example.com</location>
        <version-info end-date="2008-07-23T12:00:00"
            last-modified="2007-07-23T15:17:00"
            revision-number="" start-date="2007-07-23T15:17:00" test="true"/>
</vocabulary-information>

<!--User Categories-->
<user-category id="Subscriber">
    <short-description language="en">Subscriber</short-description>
    <long-description language="en">
        Subscriber who wants privacy protection
    </long-description>
</user-category>

<user-category id="Network">
    <short-description language="en">Network</short-description>
    <long-description language="en">
        Network who wants to protect subscriber privacy
    </long-description>
</user-category>

<user-category id="Legal">
    <short-description language="en">Legal Authority</short-description>
    <long-description language="en">
        Legal Authority who wants to protect mobile communication privacy
    </long-description>
</user-category>
<!--End User Categories-->

<!--Data Categories-->
<data-category id="SenderReceiver">
    <short-description language="en">
        Sender and Receiver Information
    </short-description>
    <long-description language="en">
        Data about the Sender and Receiver
    </long-description>
</data-category>

<data-category id="Numbering">
    <short-description language="en">
        Numbering Scheme Information
    </short-description>
    <long-description language="en">
        Data about the subscriber Numbering Scheme
    </long-description>
</data-category>

<data-category id="Location">
    <short-description language="en">Location Information</short-description>
    <long-description language="en">
        Data about the subscriber's Location
    </long-description>
</data-category>

 <data-category id="Channel">
    <short-description language="en">Channel Information</short-description>
    <long-description language="en">
        Data about the subscriber's Communications Channel
    </long-description>
</data-category>

<data-category id="Billing">
    <short-description language="en">Billing Information</short-description>
    <long-description language="en">
        Data about the subscriber's Billing
    </long-description>
</data-category>

<data-category id="Roaming">
    <short-description language="en">Roaming Information</short-description>
    <long-description language="en">
        Data about the subscriber's Roaming
    </long-description>
</data-category>
<!--End Data Categories-->

<!--Purposes-->
<purpose id="Voice" parent="Services">
    <short-description language="en">Voice</short-description>
```

```
        <long-description language="en">
            Used for providing voice services to the subscriber
        </long-description>
    </purpose>

    ...

    <purpose id="Services">
        <short-description language="en">Services</short-description>
        <long-description language="en">
            Used for providing services to the subscriber
        </long-description>
    </purpose>
    <!--End Purposes-->

    <!--Actions-->
    <action id="SendAnonymously">
        <short-description language="en">
            Send a message anonymously
        </short-description>
        <long-description language="en">
            Send a message to a subscriber for some purpose
        </long-description>
    </action>

    ...

    <action id="TransferUnlinkable">
        <short-description language="en">
            Transfer unlinkable data
        </short-description>
        <long-description language="en">
            Transfer unlinkable data information to a third party
        </long-description>
    </action>
    <!--End Actions-->

    <!--Data Containers-->
    <container id="SubscriberInfo">
        <short-description language="en">
            Subscriber information
        </short-description>
        <long-description language="en">
            Full subscriber information available
        </long-description>
        <attribute id="MSISDN" maxOccurs="1" minOccurs="1"
        simpleType="http://www.w3.org/2001/XMLSchema#string" auditable="true">
            <short-description language="en">
                The MSISDN identifier of the subscriber
            </short-description>
        </attribute>

        ...

        <attribute id="IMEI" maxOccurs="1" minOccurs="1"
        simpleType="http://www.w3.org/2001/XMLSchema#string" auditable="true">
            <short-description language="en">
                The IMEI identifier of the subscriber
            </short-description>
        </attribute>
    </container>
    <!--End Data Containers-->

    <!--Obligations-->
    <obligation id="AnonymousGrantAccess">
        <short-description language="en">
            Grant access anonymously
        </short-description>
    </obligation>

    ...

    <obligation id="ForeignNetworkPolicy">
        <short-description language="en">
            Check Foreign Network Policy for level of compliance
            with privacy rules
        </short-description>
    </obligation>
    <!--End Obligations-->
</epal-vocabulary>
```

In our EPAL vocabulary the following user classes are defined, namely *Subscriber*, *Network* and *Legal*. They will have different privacy rights based on their level of intent, degree of control and authorisation to access privacy-sensitive information. We defined our seven areas of privacy concern in the following data categories: *Sender and Receiver*, *Numbering*, *Location*, *Channel*, *Legal*, *Billing* and finally *Roaming*.

Purpose has been illustrated with one hierarchy of terms. Services in the mobile voice communications environment is the parent of all purposes. For simplicity, we have not listed all available network services. As an example, *Voice* is a child node of parent *Services*. Service implies some service or content delivery as agreed to by contract with the subscriber. The hierarchy of purposes is inclusive, which means that granting permission to act with one or more general purpose implies downward permission to any child purpose as well.

Action lists the items that would most likely be used, for example, *SendAnonymously* and *TransferUnlinkable*. Many more actions may be listed here, highlighting our privacy concerns. Such examples may include actions relating to unobservability of network event information and pseudonymity allocation or mapping, to name a few. Actions are not defined in a hierarchy, so there is no ordering on them.

Many data containers may be defined. However, for illustration purposes we choose to define one container for subscriber information called *SubscriberInfo*. *MSISDN* and *IMEI* are just two of many possible attributes chosen which could constitute the makeup of *SubscriberInfo*.

A few obligations are defined, for example *AnonymousGrantAccess* and *ForeignNetworkPolicy*. These are all requirements outside of the powers of the EPAL system. Obligations of this type must be enforced by either the underlying network or by some enforcement application that understands and is capable of interpretation of these obligations.

All that remains is to write a set of rules, which should ideally be based on Section 4.5. The set of rules that govern privacy in EPAL is not included in the vocabulary file. Instead it is included in a separate policy file. In Listing 4.2, we show the policy file that contains rules that use the vocabulary defined above.

Listing 4.2: Example EPAL Mobile Communication Privacy Policy Rules

```
<?xml version="1.0"?>

<!--EPAL policy definition for mobile communication privacy-->

<epal-policy default-ruling="deny" version="1.2"
xmlns="http://www.research.ibm.com/privacy/epal"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.research.ibm.com/privacy/epal
epal.xsd http://www.w3.org/2001/XMLSchema xs-dummy.xsd ">

    <policy-information id="MobilePrivateCommunicationPolicy">
        <short-description language="en">
            Policy controlling messages sent, location based
            services rendered, retention, and transfer of location
```

```
            data
        </short-description>
        <long-description language="en">
            This policy defines rules for some aspects of mobile
            communication privacy.
            (1) As an example, it allows a rule for a subscriber
            to use the underling network infrastructure anonymously.
        </long-description>
        <issuer>
            <name>Privacy Company</name>
            <organization>University of Pretoria</organization>
            <e-mail>privacy@up.ac.za</e-mail>
            <address>Pretoria, 1804</address>
            <country>South Africa</country>
        </issuer>
        <location>http://www.privacy.example.com</location>
        <version-info end-date="2008-07-26T12:00:00"
            last-modified="2007-07-26T15:17:00"
            revision-number="" start-date="2007-07-26T15:17:00" test="true"/>
    </policy-information>

    <epal-vocabulary-ref id="MobilePrivateCommunicationVocabulary"
    location="http://www.lbs.example.com"/>

    <!--Rules-->
    <!--Allows subscriber to access network services anonymously-->
    <rule id="AnonymousService" ruling="allow">
        <short-description language="en">
            Deliver content and data to the subscriber anonymously
        </short-description>
        <user-category refid="Subscriber"/>
        <data-category refid="SendReceiver"/>
        <purpose refid="Services"/>
        <action refid="SendAnonymously"/>
        <obligation refid="AnonymousGrantAccess"/>
    </rule>

    ...

    <!--End Rules-->
</epal-policy>
```

The default ruling of the policy is “deny” (default-ruling=”deny”). This means that in the event that no rule is satisfied, the policy will deny any request. Options for the default ruling include “deny”, “accept” and “don’t care”.

The Mobile Communications Privacy Policy contains rules that define allowed privacy-preservation behaviour. Rules are defined by either an option for “accept” or “deny”. Furthermore, rules include references to one or more User categories, Data categories, Purposes, Actions and zero or more Obligations.

In terms of our Mobile Communications Privacy Vocabulary and Policy, a privacy server accepts requests from subscribers and returns rulings accordingly. Requests can be either simple or compound. A simple request contains one User, one Purpose, one Data category and one Action, while a compound request may contain multiple entries for each. An interpretation of the request is necessary to determine whether any subscriber can perform all the actions on all the categories for all the purposes.

The EPAL privacy language allows for the creation of query-response style privacy policies. Furthermore, these policies can use an arbitrarily defined set of terms including user classes, data classes, purposes, actions and obligations as shown in our example EPAL Mobile Communications Privacy Policy and Vocabulary. A listed set of rules governs the privacy policy

using a vocabulary as shown in our example EPAL Mobile Communications Privacy Policy Rules.

4.9 Conclusion

In this chapter we showed that privacy protection is a requirement in mobile voice communications networks. Based on a defined generic mobile communications architecture and highlighted privacy concerns, we proposed a Private Voice Communications Model using UML component diagrams. Our formal privacy requirement definitions ensure privacy through anonymity, pseudonymity, unobservability and unlinkability from ISO 15408 [83]. Work in this chapter forms the basis of a privacy requirements analysis in Next Generation Networks (NGNs).

Each of the seven privacy threats identified is individually addressed in Chapters 5, 6, 7, 8, 9, 10 and 11. Our aim is to identify each specific privacy threat, using GSM as a reference, and to investigate possible solutions for enhancing privacy. Ultimately, we wish to enforce privacy with the aid of technology and identify novel techniques for privacy assurance, which may then be applied in NGNs.

Chapter 5

Sender and Receiver Privacy

5.1 Introduction

In any context, when two parties communicate, certain personal information must remain private during the communication. Such information may include: the sender's and receiver's identity and location information. One option to preserve privacy is to employ anonymising techniques. Sender anonymity refers to the situation where the originator of the communication wishes to keep their identity private. Receiver anonymity refers to the case where we wish to enable communication to a persistent pseudonym.

The following example illustrates the real-world requirement of GSM sender anonymity: A person "tips off" authorities about a crime and subsequently wishes to remain anonymous for safety reasons. The following example illustrates the necessity for GSM receiver anonymity: A person places an advertisement in a local newspaper in order to sell goods. However, the goods will only be on sale for a week after which the seller does not wish to be contacted further on the contact number displayed in the advert. The seller achieves GSM receiver anonymity through the use of an alias. This assigned alias we refer to as a virtual mobile number. This virtual number may be purchased from a third party or allocated to the user on request. From our example, the validity of the assigned virtual number is set to expire (at the third party) after a week. Subsequently the mapping of the virtual number to the seller's real mobile number or identity is removed, allowing for reallocation by the third party. Numbering schemes are covered in more detail in Chapter 6.

As GSM controls the underlying infrastructure, the focus here is on hiding personal aspects of the subscriber's identity to its serving GSM network. Our specific aim is to propose a mechanism that enables a user of a mobile handset to make and receive calls where the service provider cannot determine the identity of the other party involved in the call. More formally,

we investigate the possibility of achieving sender and receiver anonymity in GSM.

This chapter focuses on two means of ensuring sender and receiver privacy in a GSM network. In these approaches emphasis is placed on shifting the control and collection of personal information away from a subscriber's serving GSM network. Firstly, sender and receiver anonymity can be obtained in a GSM network through the use of a Trusted Third Party (TTP) Proxy. This is based on the fact that violations of privacy are known to frequently perpetrated by individuals who are "insiders" and authorised to access sensitive information. By allowing anonymous calls where the GSM network cannot obtain call details, this insider threat is eliminated. Cáceres et al. [26] suggests the use of Virtual Individual Servers that individuals themselves own and control. Having a decentralised framework for mobile services may be problematic given the control necessary (by an underlying network) to facilitate mobile voice communications. A second approach and alternative solution exists whereby anonymity is provided by the network provider which allows any authorised subscriber to access the GSM network, while completely hiding the subscribers true identity. This is referred to as Anonymous Channelling in GSM [120].

These two approaches only investigate the privacy in the individual subscribers capacity (sender and receiver). However anonymity in a group scenario, as is the case in a conference call facility is just as important. Due to space limitations this falls outside the scope of this thesis, however work considering anonymous conference calling is found in [42].

5.2 Privacy Concerns for Senders and Receivers

From Section 3.2.1 and taking our Private Mobile Voice Communications Architecture from Section 4.2 into account, it is evident that privacy for communicating parties is of concern. In providing the underlying infrastructure, it remains the networks prerogative to manage, relay and provide infrastructure necessary in facilitating communication. The fact that all communication in GSM is controlled and managed by the network provider, without immediate transparency, confirms suspicion from clients that private information may be misused or abused. The sender and receiver may wish to keep their identity private, thus remaining anonymous to the underlying network. In the context of a mobile network, providing anonymity to the sender and receiver may pose potential problems in areas such as billing, roaming, legal interception and forensic ability.

5.3 The Use of Trusted Third Party Proxies

A trusted third party (TTP) is an external entity which facilitates interactions between two parties who both trust the third party. This associated

trust is used to secure both parties interactions. In our case, we use a TTP proxy for the facilitation of private communication interaction between a sender and receiver.

We describe a modeled approach using TTP proxies in ensuring sender and receiver privacy. While our model's main objective in achieving sender and receiver privacy, it should still allow the network to bill the appropriate party for services rendered even though the network is unaware of the other party involved in the communication (see Chapter 7). The primary intention is to describe the high-level operation of the TTP, rather than to consider details of implementation.

Key aspects of our modeled approach include Personal Control and Identity Management. These constitute two of the four layers presented in the layered architecture for privacy-enhancing technologies [118]. Personal control is the guarantee that an individual's personal information is only divulged in accordance with the individual's privacy policy. The goal is to only release private information if the request is compatible (or at least to a negotiated level of agreement) with that of the owner's privacy policy. Identity management includes the possibility of acting anonymously and pseudonymously to hide aspects of an individual's true identity.

5.3.1 Sender and Receiver Anonymity

The technology for email anonymity, also known as anonymous remailers [70], [68], [66], [75], has addressed the problems of achieving both email sender and receiver anonymity. Remailers work in a store and forward manner at the mail application layer, by stripping off headers at each mix, and forwarding the mail message to the next mix [69]. An anonymous remailer is merely a third party proxy that replaces information with pseudo anonymous information, also known as a persona or alias. Chaining is simply a technique to achieve even more robust security by sending a message through several anonymous remailers, so that the second remailer sees only the address of the first remailer and not the address of the originator [68]. The advantage of chaining lies in the knowledge that every remailer must be compromised in order to trace the original sender of the message. The technology for web browsing anonymity [61], which employs cryptographic engines [62], allows for a user to browse the web in a personalised, simple, private and secure fashion by making use of generated aliases and maintaining pseudonomynous relationships with multiple servers. Some work has addressed the need for untraceable authentication protocols suitable for mobile subscribers [109]. However this does not undermine the fact that the mobile subscriber's serving network still maintains and monitors personal interactions of its subscribers.

5.3.2 Sender and Receiver Anonymity

We apply a similar approach to that used in remailers and consistent anonymous web access within the GSM environment. Mobile subscriber sender and receiver anonymity are achieved through the use of a Trusted Third Party Privacy Proxy. Our solution will also make use of aliases to realise sender and receiver anonymity. An alias in the GSM realm is simply a unique identifier assigned to a mobile subscriber. The alias will resemble an MSISDN, but could, in principle be identified with the TTP. One possibility is to use a special prefix or network number range (e.g. 085 in South Africa) to indicate an alias served by a TTP. An example of such an approach is FWD [124] (formally known as Free World Dialup), a non-profit commercial Voice over IP (VoIP) provider, which allocates each subscriber a 1-700-xxx virtual number upon registration. For more on Voice over IP, refer to [152].

A number of problems exist in the GSM environment where sender and receiver anonymity is concerned. There are three major issues that arise. One problem is that a subscriber needs to be reached at any moment; the serving network always needs to know the location of the mobile user in order to route incoming calls to the user. Hence in a two way communication, although the receiver may not know the identity of the sender, the underlying network possesses location information of both in order to establish and maintain an open communications channel.

The second problem is that someone's mobile number (contact details), once known, is considered public information; i.e. once the mobile number of someone is known it can be disclosed to many others via different mediums without the consent of the owner.

The third problem - and perhaps the most pertinent difference between GSM and other forms of communication - is that GSM conversations have to occur in real-time and are billed based on time, contract options and (sometimes) distance. The sender must be linked to one particular identifiable entity so that within a time frame (usually once a month) all network events conducted by the subscriber are summed and the monetary equivalent calculated thereof. The service provider holds its subscribers accountable for their network-related actions and presents each user with an itemised bill, usually at month end.

There are a number of requirements that must be met in order to realise GSM sender and receiver anonymity:

- Each sender and receiver must (in principle) be able to create a large number of anonymous identities (aliases), such that the network will be unable to map any of these identities to the same sender or receiver unless for the purpose of billing - i.e. identities must be incomparable.

- The sender and receiver are empowered to control all anonymity requirements if need be, leaving basic anonymity requirements to the

serving GSM network.

At present, the only degree of anonymity that is controlled by the user is where the sender may choose to disclose their identity by allowing "own number sending" from the mobile device when contacting a particular receiver. At the receiver end, the identity of the caller will be unknown as usually the text "Private Number" is displayed on the mobile device. When calling across borders or international boundaries, "Call" is simply displayed on the mobile device as displaying this identity is controlled by international mobile communication regulations.

Anonymity clearly holds implications for reputation and trust: in many cases a receiver would decide whether or not to accept a call (and sometimes whether or not to make a call) on whether the receiver (or caller) is able to identify the caller (or receiver) before establishing the connection. Clearly, when anonymity (or even pseudonymity) is used, it is up to the prudence of the receiver whether to accept or deny an incoming call. Similarly, whether a call is made depends to some extent on knowing whom one is calling. As a practical example of the latter case, consider the implications from buying an item from someone for whom one only has a temporary number available; since one may not be able to contact the seller after the transaction, one may be afraid of proceeding with the transaction. Furthermore, sender and receiver anonymity in GSM will be subscriber influenced and maintenance intensive; such conscious safeguarding may provide a greater level of aggravation to the user opposed to benefit gained.

In figure 5.1, we define an actions map underlining GSM communication governing privacy, enforced by a sender on a receiver and vice versa. These actions are administered through Personal Control and Identity Management taken from [118]. The map includes the following defined actions: access, deny, disclose, utilise, anonymise, depersonalise and repersonalise. Influenced by trust and reputation, identity is enforced locally by a subscriber. The GSM pseudo anonymity actions map provides a generic solution in achieving anonymity. The underlying GSM network can play a substantial role in control and maintenance, thus eliminating subscriber involvement for basic privacy requirements, such as ensuring that the communications channel is secure.

From figure 5.1, the four quadrants represent different situations where a sender may be known or unknown to a receiver and vice versa. All four quadrants are administered by Personal Control and Identity Management. For example, in quadrant 3, we assume a communication channel may be established where the receiver is known to the sender, however the sender is unknown to the receiver. The receiver trusts the anonymous sender enough to allow the creating of a communications channel. The sender may choose action "disclose", revealing the sender's true identity. The true identity in this case would include the sender's mobile number and quite possibly other

personal information, such as a name and surname.

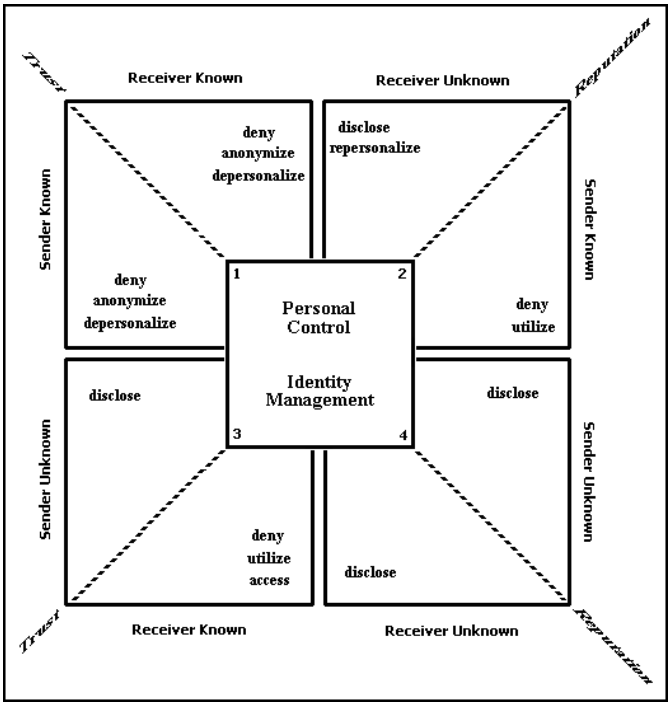

Figure 5.1: GSM pseudo anonymity actions map

5.3.3 GSM Trusted Third Party Proxy Privacy Model

This section describes our model for using a trusted third party to achieve sender and receiver anonymity in GSM.

It is relatively straightforward to achieve sender anonymity through the use of a TTP: using Caller Line Identity (CLI) preferences, one can call the TTP but withhold one's MSISDN from the TTP. One then has to somehow inform the TTP of the intended recipient of the call. Technically, this is easily achieved by using Dual-Tone Multi Frequency (DTMF) signals to communicate this number with the TTP. DTMF signaling, entered by keypad depressions on a phone, is used for telephone signaling over the line in the voice-frequency band to the call switching center. Today, in GSM, DTMF is now done out of band using the SS7 signaling system [97]. The TTP can then complete the call by calling the number entered by the original caller. Since the TTP does not have access to the CLI of the original caller, it cannot compromise the privacy of the caller - to the called or any other party.

A number of issues, however, remain with this proposed solution; the most important issues are security and billing. The major security issue

relates to the requirement that the call should be anonymous not only to the recipient, but also to the network. If anonymity was only required towards the called party, simply not sending one's own number would have sufficed. One's serving network will know that a TTP has been called. We also have to assume that the network is familiar with the process of sending the eventual called party's MSISDN using DTMF (or other means). The network will thus, in principle, be able to establish whom the call is made to, by eavesdropping on the connection. In defence of the technique, it is worth pointing out that such eavesdropping does not happen routinely (as logging of dialled numbers usually does) and it requires a perpetrator to monitor the connection when the call is made. Again, note that the actual connection is encrypted, but we are assuming an attacker on the inside of the GSM network as the current threat. The proposed solution will thus be adequate for many purposes, but would not be absolutely secure.

Below we will consider another alternative that eliminates this problem. Since the TTP does not (and should not) know the identity of the caller, the TTP is not in a position to bill the caller for services rendered. In the general case, the TTP will have no agreement with the called party and will not be able to bill him or her either. The only solution therefore is to bill the caller's network. This implies that calls to the TTP should be billed at a premium rate (by the usual service provider). This could have the undesirable effect of attracting more attention to the specific call, than other "normal" calls would have attracted, but this does not seem to be a critical weakness. The fact that the billed rate would cover the call costs to the TTP, the TTP's service charge as well as the call from the TTP to the eventual recipient, means that the call will be relatively expensive; however in cases where hiding the CLI from the called party is not sufficient, a higher call rate would probably be acceptable. Of a larger concern, with the proposed billing approach, is the fact that the cost of calling the TTP would best be based on a known cost for the call from the TTP to the called party. This clearly implies that one cannot have an indefinite sequence of TTPs through which the call is to be routed to better protect privacy. Remember that this process, known as chaining, is indeed often used where privacy is to be protected.

We now turn our attention to receiver anonymity. In this case the TTP clearly needs to know the identity of the receiver - otherwise it will not be able to route calls to the receiver. Therefore the receiver is required to register with the TTP before using the service and to provide a real number where the recipient can be contacted. Thus, some trust in the TTP is required.

When registering, the recipient receives one or more aliases. Depending on the intended application, an alias could be used to work for a limited or an extended time period.

The fact that the contact number of the recipient is known to the TTP

could be alleviated by using chaining: The contact number given to a TTP could be an alias registered at a second TTP, where the second TTP knows the real MSISDN. This can be repeated as often as required. To associate the alias at the first TTP with the real MSISDN would require collusion between the two (or more) TTPs.

Two options exist for billing: Charging the caller is an option. Calls to aliases can be charged at a premium rate as was suggested above for sender anonymity. However, since the recipient is known to the TTP, it is also possible to adopt a different billing model, where the caller is charged for a normal call and the recipient for the second half of the connection. Even where the recipient is not entirely known to the TTP (for example, when the contact details given were an alias at a second TTP) it is still possible to charge the recipient: The recipient can easily buy "vouchers" anonymously (at a normal shop) and use these to "recharge" his or her account at the TTP, without revealing any true identifying data to the TTP. In fact, this second billing model is the appropriate one to use when using chaining: The network will not know through how many TTPs a call will eventually be routed and therefore cannot bill in an appropriate manner for the call. The recipient can, in contrast, quite easily pay for each (anonymised) leg of the call.

Finally, consider the integration of sender and receiver anonymity: As presented above, it is obvious that the two approaches are simple to integrate. This solves the problem (referred to earlier) that the service provider is, in principle able, to breach sender anonymity if it eavesdrops when the caller enters the recipient's MSISDN. If an alias is used for the recipient, the service provider will be able to infer much less than would otherwise have been the case.

An integrated solution also offers an interesting confidentiality versus convenience trade-off: Assume that two parties are communicating with one another using both sender and receiver anonymity. Using the (combined) solutions offered above, the CLI of both parties will be hidden from the TTP. If, however, the CLI is revealed to the TTP, the TTP will be able to translate the incoming CLI to the alias it associates with the CLI and use this alias as the CLI of the outgoing call. This would enable an anonymous call to be made and will allow the called party to (automatically) return the caller's call. Both parties will be pseudonymous towards each other, as well as the network. However, in this case the TTP will know the real contact details of both communicating parties. Chaining is one possible solution for this, but the billing approach described for a sender anonymous call described above cannot deal with this option. A simple extension to the billing approach for receiver anonymous calls given above, will solve the billing problem introduced here.

An alternative to the introduction of a TTP, is to effectively adjust the existing GSM infrastructure in order to accommodate the need for

anonymity of sender's and receivers using the network. Such a provision is referred to as anonymous channelling.

5.4 Anonymous Channelling Protocol

In [120], a new authentication protocol is proposed, allowing anonymous channelling over GSM. In this solution no TTP component is present and is concerned with the modification of the authentication process at a network level. The protocol is based on the generation of temporal keys defined in the LHY protocol [92] and the utilisation of prepaid tickets in a similar way to that of the LJ protocol [96]. The main objective of this new protocol is to allow the legal subscribers anonymous access to the GSM networks resources [120]. This protocol addresses and solves the following problems in GSM outlined by [92]: mutual authentication, Home Location Register (HLR) and Visitor Location Register (VLR) overheads and network component bandwidth consumption.

In anonymous GSM channelling mutual authentication is provided without any modifications in the GSM system architecture. In the same way, every mobile subscriber MS has its own secret key Ki which is shared with HLR. The protocol is based on the generation by the HLR of a temporal key TKi. The temporal key allows the VLR to authenticate the subscriber without further connections to the HLR, and having no knowledge of shared secret key Ki. Like the LJ protocol [96], the existence of a Public Key Infrastructure (PKI) is assumed. Hence, the MS must store the *HLR's public key* while the HLR must store its own private key. The anonymity provided allows any authorised subscriber to access the GSM network, while completely hiding the subscribers true identity to the home VLR. The protocol is divided into two parts namely, the ticket issuing phase and the utilisation of these prepaid tickets, where the ticket is generated by the HLR [120]. The ticket is defined as follows:

$$(Auth\_VLR_h; TK_i; Time_{expire}) \tag{5.1}$$

where $Auth\_VLR_h = A3(K_i; Time_{stamp})$ and $TK_i = A3(K_i, Time_{expire})$. Recall from Section 2.3.1.1, $A3$ is the mobile subscriber authentication algorithm which forms part of the GSM specification and exists at both the mobile device and home network operator.

5.4.1 Ticket Issuing Phase

In this phase a prepaid ticket requested by MS is generated by HLR. Furthermore, MS is previously authenticated by HLR, and later, after the ticket generation, HLR is authenticated by MS. The protocol is as follows (refer to figure 5.2). The protocol is described in verbatim from [120]:

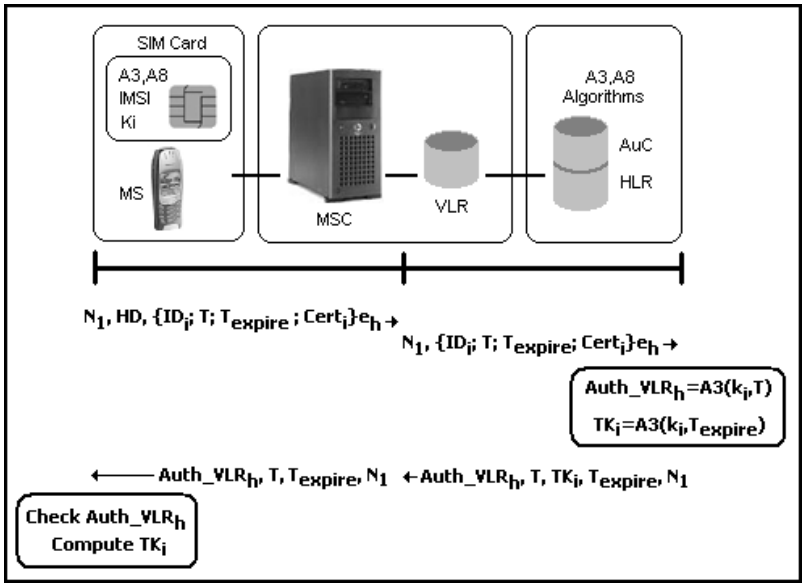

Figure 5.2: GSM Anonymous Authentication - Ticket Issuing Phase [120]

Step 1: $MS \rightarrow VLR : HD, N_1, \{ID_i, T, T_{expire}, Cert_i\}e_h$ where N_1 is a random word, T and T_{expire} are *timestamps*, and $Cert_i$ is the authentication information, such that:

$$Cert_i = A3(K_i, (ID_i, T, T_{expire})) \tag{5.2}$$

In this step, MS sends to VLR the information to be passed to HLR, in such a way that VLR cannot access it. That is, MS encrypts the information using HLR's public key e_h. The only thing VLR has to do is to re-send this information to HLR with identity HD.

Step 2: $VLR \rightarrow HLR : N_1, ID_i, T, T_{expire}, Cert_i e_h$

Step 3: $HLR \rightarrow VLR : N_1, Auth\_VLR_h, T, TK_i, T_{expire}$ where $(Auth\_VLR_h, TK_i, T_{expire})$ is the ticket generated by HLR, with

$$Auth\_VLR_h = A3(K_i, T) \tag{5.3}$$

and

$$TK_i = A3(K_i, T_{expire}) \tag{5.4}$$

Step 4: $VLR \rightarrow MS : N_1, Auth\_VLR_h, T, T_{expire}$

In this case, VLR broadcasts this message to every user. N_1 is used by the legal destination user to identify the correct message.

Step 5: MS checks the ticket validity by means of A3 algorithm, that is, $Auth\_VLR_h = A3(K_i, T)$. Then the temporal key is recover computing $TK_i = A3(K_i, T_{expire})$.

As one can observe, this phase of the protocol implements a mutual authentication between MS and HLR. First, HLR authenticates MS by means of the identity ID_i and the shared key K_i. Next, MS authenticates the originator of the ticket. Moreover, MS verifies that the ticket has been issued to be valid for a period of time bounded by T_{expire}.

5.4.2 Ticket Utilisation Phase

When a mobile user wants to use an anonymous channel, he must use the previous ticket generated by HLR (refer to figure 5.3).

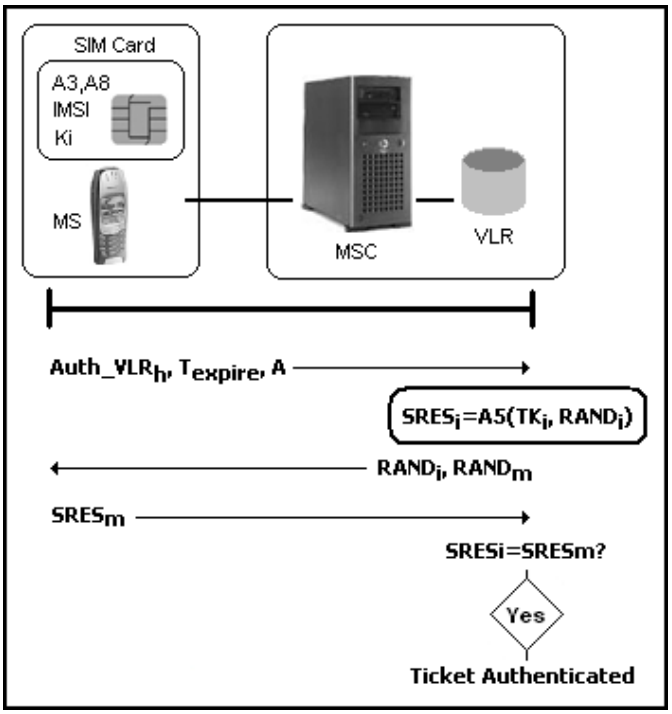

Figure 5.3: GSM Anonymous Authentication - Ticket Utilisation Phase [120]

Step 1: $MS \rightarrow VLR : Auth\_VLR_h, T_{expire}, A$ where
$A = A5(TK_i, RAND_m)$, $RAND_m$ being a random number chosen by MS.

Step 2: $VLR \rightarrow MS : RAND_i, RAND_m$ where $RAND_i$ is a random challenge. When VLR receives the MS request, VLR selects the TK_i corresponding to the pair $(Auth\_VLR_h, T_{expire})$. Then, VLR deciphers A and computes

$$SRES = A5(TK_i, RAND_i) \tag{5.5}$$

and sends $RAND_i$ to MS. In this way, MS authenticates VLR.

Step 3: $MS \rightarrow VLR : SRES_m$ with

$$SRES_m = A5(TK_i, RAND_i) \tag{5.6}$$

Step 4: VLR checks the correctness of $SRES_m$ As one can observe, HLR does not participate in this authentication phase. On the other hand, the session key Kc to encrypt the forthcoming communications between MS and Base Station (BS) may be computed in the same way as in the original GSM scheme, that is

$$Kc = A8(TK_i, RAND_i) \tag{5.7}$$

The only situation in which VLR and MS will communicate with HLR corresponds to expiration time T_{expire} previously established by MS.

5.5 Privacy Analysis

We provided two possible alternative approaches in achieving sender and receiver anonymity. Firstly, by abstracting control away from the network provider using a TTP and secondly by providing an anonymous channel for communication.

5.5.1 Trusted Third Party Proxy

By using a TTP, sender and receiver privacy is achieved by removing responsibility away from the network provider. However, in doing so, we encounted three problems which were addressed. This being i) availability of the subscriber and knowing it's location for routing calls ii) the release of a MSISDN into the public domain and iii) that GSM conversations have to occur in real-time and are billed based on time. Through the introduction of an MSISDN alias, possibly TTP chaining techniques, premium rated billing options, sender and receiver is enhanced using a TTP Proxy.

5.5.2 Anonymous Channelling

Anonymous channelling provides a means of disassociation between entities controlling private identification information in a GSM network. This abstraction ensure authentication to the network without revealing the subscriber's true identity. Through the introduction of a temporal key TKi, this allows the VLR to authenticate the subscriber without further connections to the HLR, which in turn has no knowledge of shared secret key. This ensures sender and receiver privacy internally to the GSM network without having to alter the underlying infrastructure.

5.6 Conclusion

In this chapter, two means of ensuring sender and receiver privacy in a GSM network were discussed. Sender and receiver anonymity is achieved in a GSM network through the use of a Trusted Third Party (TTP) Proxy. By allowing anonymous calls where the GSM network cannot obtain call details, any personal information that may be exposed due to an insider eavesdropping is eliminated. Alternatively, anonymity provided by the network provider allows any authorised subscriber to access the GSM network, while completely hiding the subscribers true identity. Anonymous Channelling details, from a technical standpoint, how authorised anonymous access to a GSM network is attained.

Chapter 6

Numbering Scheme Privacy

6.1 Introduction

Unique identification is imperative in a successful communications environment. Numbering plans detail information regarding the country and network of an individual using a communications system. This network-assigned number to a large extent, is considered private information, as it uniquely identifies and links a subscriber to a particular country and network for routing and billing purposes. Mobile numbers are exchanged for business purposes and among friends, stored in network and third party databases and distributed sometimes without the consent of the owner.

This chapter investigates methods for ensuring virtual private identification for senders and receivers. Various techniques available include: i) the receiver assigning a new "virtual" identity (known only to the receiver) to the sender and ii) identification through zero-knowledge, which provides knowledge of an identity without revealing any information and lastly, iii) secret sharing between the sender and receiver.

6.2 Virtual Numbers

The concept of using virtual numbers for achieving privacy is not new [37]. Numbering plans have been instrumental in all forms of telephonic communications. A valid numbering plan is a sequence of digits governed by mobile or fixed line regulating bodies that have standardised prefixes with minimum and maximum digit length requirements. A virtual number can best be described as a valid numbering plan that does not map to a valid number belonging or assigned to an entity, whether it be a person, organisation or Interactive Voice Response (IVR) system. A network or regulating authority may choose to allocate and assign a virtual number for a specific purpose, for example a disaster relief fund. A form of virtual numbers is already in use by most mobile network operators with the inception of mobile "short code" numbers. Such numbers are primarily 6 digits in length and are used in Value Added Services (VAS) such as competitions, voting or

mobile content delivery services. A short code is purchased from a wireless application service provider, sometimes referred to as a WASP, or from the serving GSM network. We use the concept of virtual numbers to directly map to a Trusted Third Party (TTP) service and an individual subscriber. Accuracy in virtual number distribution and its user is critical for anonymous communication. Properties may include a validity period (set at the TTP) which expires after a designated period.

6.2.1 Assigning Virtual Number Identification

Setting up the TCP connection between a web application and database can be an expensive operation. Developers have been able to take advantage of database connection pooling for some time now, allowing them to reuse connections to a database. Rather than setting up a new TCP connection on each request, a new connection is set up only when one is not available in the connection pool. When the connection is closed, it is returned to the pool where it remains connected to the database, as opposed to completely tearing down that TCP connection.

Database pooling is one methodology which may effectively be used in assigning a large number of virtual numbers for use by individuals. Using this practically means a Virtual Number acts as an alias until such time it is no longer needed. After a new Virtual Number is mapped to a particular user, used and discarded, the old number is released back into the pool for future use. This Virtual Number may be delivered in such a way that it is only known to the recipient.

6.3 Anonymous Identification Schemes

Anonymous identification schemes allow a user to identify themselves to a verifying authority in a secure way without revealing their identity or secret key. Virtual Numbers play a significant role in identification and re-identification of an anonymous user. Incomparability of identities is realised through the creation of a large number of anonymous identities; virtual numbers fulfils this requirement. Virtual Numbers form part of the user identification to a resource.

Current identification are based on the number-theoretic problem of quadratic residuosity modulo a composite integer. Some use the general paradigm of zero-knowledge proofs to prove the knowledge of an identity without revealing any information. The basic idea of the *zero-knowledge paradigm* is that it is not used to prove existence of witnesses but rather "knowledge about knowledge" [30]. The concept of "zero-knowledge proofs" was first introduced by [71] such that a user can convince a polynomial bounded verifier of identity whilst not relinquishing any information that would otherwise identify the user. Take for example U whose goal is not to

prove that X belongs to Y but to show that it knows the status or relationship that exists between X and Y. A verifier V thus only obtains U's state of knowledge and no information with respect to U.

6.3.1 Anonymous Group Identification Schemes

Substantial work has been done on the design and security analysis of anonymous group identification schemes [91]. Such anonymous group identification schemes have been extended for a mobile environment [31] where every anonymous user checks to see if it belongs to a specific group. However, such an approach is not feasible in large mobile user sets, as is the case in GSM.

Generally, a group identification scheme is a method that allows a user of a system or member of a group denoted by $G = \{M_1, ..., M_i\}$ to convince a third party that they in-fact belong to G. The additional property of being anonymous requires that the scheme is firstly secure and secondly that the member (M_i) of the group (G) does not reveal its identity to G at any stage in the communication process.

A group identification scheme is a distributed protocol executed by a trusted party, usually referred to as the Center (denoted by C), many participants called the Users (denoted by U_i), and another trusted participant, called the Verifying Authority (denoted by V_A). The group identification scheme is divided into two phases, namely the *Initialisation phase* and the *Identification phase*. This illustrates an efficient "zero-knowledge" group identification for a single user.

One way of achieving "zero-knowledge proofs" is by exploiting the properties of Blum integers. For a more formal definition of Blum integers see [21, 106, 114].

Briefly, a Blum Integer is the product of two primes p and q which are both congruent to the form $4r + 3$ n=pq. If n is a Blum integer, each quadratic residue has exactly four square roots, one of which is also a square; this is the principle square root [138].

Quadratic Residuosity: For each integer $x > 0$, the set of integers less than x and relatively prime to x form a group under multiplication modulo x denoted by Z_x^*. We say that $y \in Z_x^*$ is a quadratic residue modulo x if and only if there is a $w \in Z_x^*$ such that $w^2 \equiv y \bmod x$.

For example, the principle square root of 23 mod 77 is 67. The other three square roots are 10, 32 and 45. This is the case because $10^2\, mod\, 77 = 32^2\, mod\, 77 = 45^2\, mod\, 77 = 67^2\, mod\, 77 = 23$; 67 is the principal square root, since (amongst others) $12^2\, mod\, 77 = 67$. Usually, it is easy to construct a Blum integer; however, it is very difficult to prove directly as the composite integer (the Blum integer) must first be factored in order to prove its type.

De Santis et al. [137] presents a communication-efficient group identification scheme whose security property is based on the computational difficulty of factorising Blum integers.

Using this mechanism practically means a user will need to prove membership to a group in order access the network. In other words, a challenge/response confirmation is necessary before access to use the network is granted.

6.4 Secret Sharing

Secret sharing refers to any method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together. Individual shares are useless on their own.

More formally, a secret sharing scheme involves one dealer and n participants. The dealer accomplishes this by giving each participant a share of a secret after certain conditions have been met. If any group t or more participants together combine their shares, the secret is reconstructed. Such systems are often referred to as (n, t)-threshold schemes. Secret sharing schemes were first introduced independently by Blakley in [20] and by Shamir in [143].

Practically this means in order to communicate, each user must prove knowledge of a shared secret between the parties. The secret may form part of the number being dialled, for example +2782 123 456 xxx xxxx where xxx xxxx is part of a secret share. A recipient of a call from +27 82 123 456 xxx xxxx, to complete the connection, must punch in an appropriate shared secret (possible using DTMF) to connect the call.

6.5 Privacy Analysis

Mobile numbers form part of an individual's identity. As mobile numbers are publically available (distributed without ones consent) the threat for a violation is possible and probable. We suggest three possible number scheme privacy techniques. These mechanisms can be summarised as: providing an assigned "virtual" identity (pseudonym), proving group participation before connecting and finally possessing a secret share in order to complete a connection. Although each may have its own pitfalls (not explored here), what they do is illustrate the potential for various privacy enhancements to numbering schemes in order to protect mobile number use and distribution.

6.6 Conclusion

The dissemination of mobile numbers is currently not controlled and regulated. This chapter briefly explore some techniques which when used enhance the privacy protection of numbering schemes.

A mobile number is the primary identifier used in the billing of a user. In the next chapter we explore privacy in the realm of billing within a mobile network.

Chapter 7

Billing Privacy

7.1 Introduction

Mobile network operators require comprehensive billing engines in order to bill their subscribers. However, little thought has been given to providing privacy where Call Data Records (CDRs) are concerned. Wholesale billing engines are required to house full details of any form of communication between parties for the sole purpose of creating and presenting an itemised bill to subscribers. Privacy-sensitive information, such as whom a subscriber calls and the duration thereof, can easily be combined with personal information in order to profile a subscriber.

A Billing Engine (BE) is an integral part of a network operator's infrastructure. Its core functions include storage of communication interaction detail, rating systems and managing of charges. The implementation of billing for telephone services is based on an offline billing system and on having CDRs generated in the network [65]. The CDRs are stored as receipts for the performed network transaction; a subscriber is thus accountable for all received and correctly signed records. GSM includes a comprehensive billing model, however, privacy concerns arise as CDRs are created, stored and managed at a network level. This information is beyond the control of the individual.

With the increase of network value added services offerings, comes a new demand for billing architectures to charge for these services [59]. These extensions result in distributed billing systems and subscribers receiving itemised bills from different service or content providers. One such example is the billing for digital content by a third party [65].

In the current mobile communication networks, subscribers have to trust network operators to make correct charges over the calls they made [160]. Inadequacies in the process of just how these CDR's are generated may result in disputes with the network.

Peinado et al. [120] provides a means to achieve anonymous channelling in GSM, however no consideration is afforded regarding how the

anonymous subscriber is billed. Achieving total subscriber anonymity is evidently hard as the network operator is responsible for the switching of network events (e.g. voice calls). Furthermore, the generating and maintaining of CDRs is the sole responsibility of the network. In this chapter we define a CDR anonymity model to obscure GSM communication information and provide complete subscriber, network and communications anonymity. We propose an anonymous billing channel protocol allowing access to subscriber CDRs through the use of compatible keys (based on our CDR anonymity model). The desired result in one in which the anonymous GSM subscriber remains accountable, while the network retains a private and accurate itemised billing infrastructure.

7.2 Privacy Concerns in Billing

From Section 3.2.3 and taking our Private Mobile Voice Communications Architecture from Section 4.2 into account, how privacy sensitive billing information is handled is of concern.

In the current mobile communication networks, subscribers must trust network operators to make correct charges. Therefore, a subscriber requires an undeniable means of ensuring billing information is private and the integrity is uphold should a dispute arise.

These communication records, may infringe on basic subscriber privacy principles. The main problems are summarised below:

- The mobile subscriber has no control in the creation of the CDR and has no means to verify the accuracy of the CDR generated.
- The network has full control over storage, distribution and utilisation of the CDRs.
- The subscriber has no direct uncontested access to view personal CDRs generated by the network if a dispute should arise.
- CDRs reveal subscriber usage patterns, this privacy-sensitive information is susceptible to subscriber profiling.

In addition, a distributed billing system is necessary for receiving itemised bills from different service or content providers. Having external billing parties contributes to privacy concern surrounding privacy-sensitive billing information.

Our approach in achieving billing privacy is based on the notion of compatible keys a topic we briefly consider next.

7.3 The Theory of Compatible Keys

RSA is a public key cryptosystem that offers both encryption and digital signatures (authentication) [135]. RSA is often used in modern environments

— especially on the Internet,since individuals need not send any secret key to others when communication is established. Ray et al. [130] proposed a new protocol for secure multi-casting describing the theory of compatible keys based on the RSA algorithm. Although still unproven, [130] suggests the protocol is scalable, meaning the encrypted message is independent to the number of consumers subscribing to it. Ray et al. [131] further applies the use of compatible keys in a hierarchical implementation where a leaf node have less decryption capability than its parent node.

Briefly the theory follows which we apply later to our subscriber CDR anonymity model: For each subscriber S_i, a key pair $(K_i;K_i^{-1})$ is generated. This key pair is mathematically related to all other existing key pairs $(K_j;K_j^{-1})$ belonging to subscribers S_j. The subscriber S_i uses key K_i^{-1} to decrypt any message which has been encrypted with a combination of keys including his own. To illustrate the encryption and decryption process, we give an example. Suppose subscribers S_2 and S_4 require access to a message m. The key pair $(K_4;\ K_4^{-1})$ is prepared for S_4 such that K_4 is compatible with K_2. The message m is now encrypted with the key K_2 and K_4, denoted by $[m;K_2K_4]$. Now subscriber S_2 is able to obtain message m by decrypting using K_2^{-1} and likewise, subscriber S_4 is able to obtain m by decrypting using K_4^{-1}. Note that multiple decryptions are not necessary to obtain the message.

Compatible keys provide a foundation for access control to privacy-sensitive billing information. Depending on initial encryption, decryption capability is intended for those in possession of the necessary compatible key. This ensures that access to privacy-sensitive information is controlled such that only the relevant information is revealed accordingly to the intended parties.

7.4 CDR Anonymity Model

In defining CDR anonymity, we first identify the most common piece of information (elements) that constitute the makeup of a CDR. Furthermore, we identify the authorised parties involved in access to private CDR information, namely: the legal or forensic user, the subscriber and the network itself.

7.4.1 CDR Elements

Certain elements are required in order to record and charge for a network event. We define the following elements in the creation of a Call Data Record. This includes: *From* (the source), *To* (the destination), *Communications Type* (e.g. voice call, SMS message or data transfer), *TimeDate* (the start time and date of the network event), *Duration* (event lifetime) and *Cost* (event price). With any piece of relational information there exists the

potential for a rudimentary relationship between certain pieces.

Figure 7.1 illustrates the relationship(s) we have identified that exist between the pieces of CDR information (elements). It is important to note that by removing any one of the described elements results in various types and degrees of CDR anonymity. This is discussed in detail below.

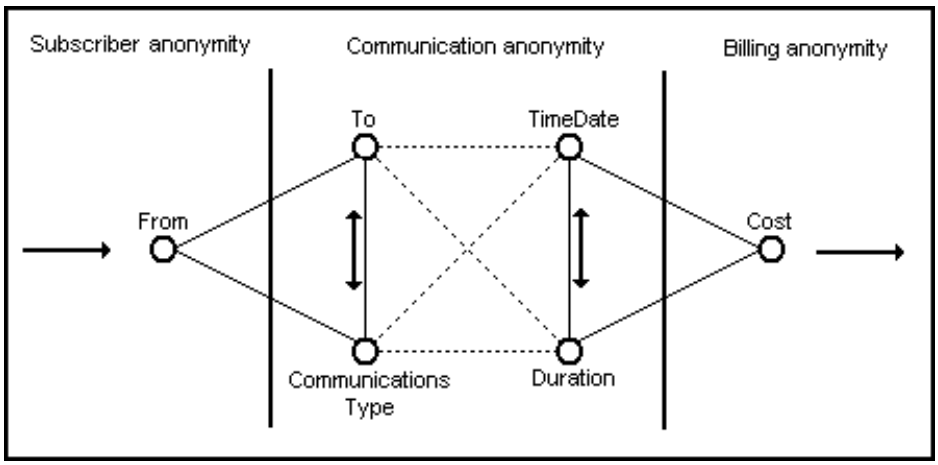

Figure 7.1: CDR relational diagram

In order for a network to bill subscribers, it requires the following information: *From* and *Cost* (who performed a network event and the cost charged for the service provided). In order to complete an itemised bill for each subscriber, the network requires the following information: *To*, *Communication Type*, *TimeDate* and *Duration*. Sender anonymity is achieved by excluding or obscuring the *From* element from the CDR relational diagram. By the same token, cost anonymity is achieved by obscuring the associated *Cost* element from the CDR relational diagram. Finally, communication anonymity is obtained by obscuring all of the remaining CDR elements. Our solution allows the network to provide this information to the subscriber. However, it will be provided in a form where the network does not know the contents it does not need to know, but it will be available to those parties that do have a reason to know it — such as the subscriber.

7.4.2 CDR Access Control

A hierarchical access level structure is needed for access control to the generated CDR. We assign compatible keys K_1 to Legal/Forensics, K_2 to the GSM subscriber and lastly K_3 to the serving GSM network operator. For obvious reason, Legal/Forensics' compatible key K_1 allows decryption and access to the entire CDR content.[1] The subscriber's compatible key K_2 al-

[1]We do not discuss the ethics of giving Legal/Forensics full access to CDRs (when required) and therefore accept it as a given requirement.

lows for the decryption of CDR core elements while the compatible key of the serving network, K_3 merely reveals the *From* and *Cost* elements.

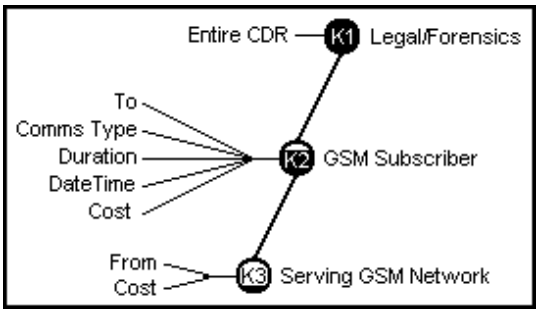

Figure 7.2: CDR privacy security levels

7.4.3 The CDR Anonymity Model

The CDR anonymity model divides a CDR's elements into four quadrants — refer to Figure 7.3. Fuzzification of any of the quadrants allows for CDR information privacy protection. Quadrant 1 and 3 focus on sender and receiver anonymity respectively, while quadrant 2 and 4 allow for billing and temporal (time frame) anonymity. Quadrant 3 and 4 also constitutes the CDR communication elements and if obscured, complete communication anonymity is achievable.

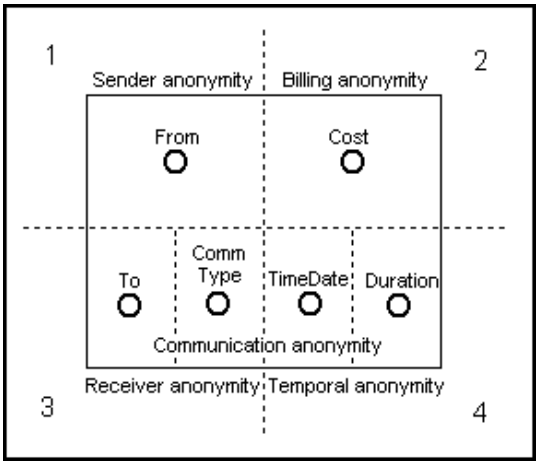

Figure 7.3: CDR anonymity model

7.5 Anonymous Billing Channels

Some work as been conducted in the field of anonymous billing channels. Zhou et al. [160] proposed a scheme based around the use of one-way hash

chaining for achieving undeniable billing in mobile networks where roaming may be concerned, home network anonymity where CDRs are concerned is not considered. Wang et al. [154], also provides a scheme for ticket-based service access model and anonymous service usage in mobile application and access, however privacy surrounding the communication detail and billing is omitted. Our anonymous billing channels protocol — to be discussed here — combines the concept of anonymous channelling together with the CDR anonymity model and CDR access control levels defined through the use of hierarchical compatible keys [131].

7.5.1 Anonymous Billing Protocol

In this section, a new anonymous billing protocol is presented. The main objective of this new protocol is to allow the legal subscribers anonymous access to the networks resources, while at the same time providing an undeniable and accountable network billing infrastructure. Our protocol can be divided into two phases: the ticket consumption (CDR creation phase) and the ticket stubbing phase.

7.5.1.1 The Ticket Consumption (CDR Creation Phase)

Suppose we have a network assigned ticket ($Auth_{VLR}$; TK_i; T_{exp}) where T_i is the ticket to be consumed and T_{exp}) is the ticket expiry.

Step 1: The ticket ($Auth_{VLR}$; TK_i; T_{exp}) is authenticated by the VLR, checking if $SRES_i$ corresponds to $SRES_m$ (refer to 2.3.1). The subscriber may then perform a network event.

For the sake of brevity, the components of the ticket are not described in full here (they depend on earlier steps in the ticket issuing process). The components that are used below will be described in more detail when they are used.

Step 2: Upon the completion of the network event, the VLR generates the CDR.

At this stage the CDR will contain the following elements, assuming anonymous channelling is used — refer to [120] for details.

CDR id	From	To	Comms Type	Time Date	Duration	Cost
?	($Auth_{VLR}$; TK_i;T_{exp})	Receiver	C_{type}	T_s	T_{dur}	?

Table 7.1: VLR initial CDR creation

Step 3: The VLR encrypts the CDR with the Billing Engine's (BE) public key and sends $E(CDR)_{BE_{pub}}$ to the BE.

At this point, we assume the BE is an independent entity and therefore not controlled by the network. The scheme is further enhanced if mutual au-

thentication between the VLR and the BE and even between the subscriber and the BE, exists. The BE maintains Legal/Forensic (K_1), subscriber (K_2), and network (K_3) related compatible keys.

Step 4: The BE decrypts $E(CDR)_{BE_{pub}}$ with its private key, obtaining the original CDR message, rates the CDR and derives associated cost. K_i, which identifies the sender (*From*), can be derived using the A3 algorithm (as in [120], again referring to 2.3.1) from the ticket:

$$TK_i = A3(k_i; T_{exp}) \tag{7.1}$$

The $Auth_{VLR}$ identifies the associated network, also obtained from the ticket.

Step 5: The BE encrypts the CDR using the compatible keys K_1, K_2 and K_3 as described in Table 7.2:

CDR id	From	To	Comms Type	Time Date	Duration	Cost
-	(K_1;K_2; K_3)	(K_1;K_2)	(K_1;K_2)	(K_1;K_2)	(K_1;K_2)	(K_1;K_2; K_3)

Table 7.2: BE CDR encryption

Step 6: The BE creates and distributes a ticket stub.

A ticket stub may be used at any stage by any of the hierarchical parties involved in retrieving the necessary CDR information (they have access to). The ticket stub denoted by T_{stub} is calculated using the A3 algorithm as follows:

$$T_{stub} = A3(K_i; (BE_{id}, CDR_{id}, T, V)) \tag{7.2}$$

where BE_{id} is the Billing Engine identifier, CDR_{id} represents the CDR identifier, T indicates the TimeStamp of the CDR creation and finally V is the validation period of the ticket stub. The CDR_{id} has the following composition:

$$CDR_{id} = (BE_{id}; Ticket) \tag{7.3}$$

Step 7: The BE returns the ticket stub to the VLR.

The subscriber with its compatible key K_2 has access to the CDR. Ticket stubs in conjunction with the subscriber compatible key on encrypted CDRs results in an itemised bill. Ticket stubs (T_{stub}) expire as soon as the designated maximum validity period is reached and should be archived.

7.6 Privacy Analysis

Our system provides a means to anonymous billing while maintaining creditability and accountability for undeniable billing should a dispute arise. Our CDR anonymity model extracts pieces of relational information (elements) making it easier to anonymise information and assign access to it. We define an anonymous billing protocol, which makes use of compatible keys. In allocating related compatible keys (Legal/Forensic (K_1), subscriber (K_2), and network (K_3)), providing access to certain privacy-sensitive parts that constitute a CDR. This ensures a degree of privacy based on a hierarchical access control mechanism to network-generated CDRs.

7.7 Conclusion

Billing information contains private information. Billing information is currently controlled, maintained and disseminated by the network. Should a dispute arise, the subscriber is presented with no auditable data or even access to their private CDR information. Our CDR anonymity model outlines a foundation for separating, billing information into relational pieces of information. Using anonymous billing channels we develop a means to ensure access to information in a privacy-preserving manner. In essence our solution presents a mechanism for accountable and private billing for all parties concerned.

Chapter 8

Roaming Privacy

8.1 Introduction

GSM requires that a user trusts his or her home network with details of calls made. More specifically, the home network must know the location of subscribers in order to route calls. Work on location privacy (refer to Chapter 11) looks specifically at subscriber location privacy in the home network. However, new privacy concerns arise when subscribers "roam" away from their home network into the jurisdiction of a foreign network service provider. In the case of roaming, trust and privacy assurance is extended to the foreign network operator.

Transferred Account Procedure (TAP) is the global telecommunications industry billing standard which allows network operators to exchange billing information (Call Data Records). This central repository for TAP records, known as a clearinghouse, contains large amounts of privacy-sensitive network event data of roaming subscribers. The home network and roaming subscribers (as discussed in Chapter 7) have no control as to the extent to which these CDRs are analyzed, stored and transferred for billing purposes.

Number portability makes the switching of network providers for the subscriber relatively easy. Number portability occurs when a subscriber changes its home network providers while maintaining its original mobile number. With network operators continually looking to increase their subscriber base, such roaming information may be critical in luring subscribers away from their home network providers. This highlights the need for the home network provider to protect the privacy of all subscriber activities from foreign network operators.

Assigning pseudonyms is one approach to achieve sender anonymity, where subscriber information is replaced with pseudo anonymous information [37]. Having their identity divulged is not the only privacy concern for roaming subscribers; privacy-sensitive network event information for billing purposes is also controlled by the foreign network.

Our purpose is to eliminate the privacy concerns of the home network

and subscribers where roaming GSM subscribers are concerned. This is achieved by restricting the foreign network operator and clearinghouse access to privacy-sensitive CDR billing information. It is evident that it becomes necessary to include the subscriber in the audit process directly should an issue arise. We do this by proposing (in addition to the local roaming CDR collection) to include an additional CDR store on the handset. This ensure non-repudiation of roaming network events.

Our goal is that privacy is preserved for the home network and subscriber in roaming. We illustrate this through our proposed Privacy-Preserving Roaming Architecture. All components involved in a roaming network event are addressed, namely: the roaming subscriber, the foreign and home network operator and TAP record clearinghouse.

8.2 Privacy Concerns when Roaming

From Section 3.2.4 and taking our Private Mobile Voice Communications Architecture from Section 4.2 into account, it is evident that privacy for roaming subscribers is of concern. Subscriber mobility complicates the process of identifying and later billing subscribers.

A central repository of foreign billing records, contains large amounts of privacy-sensitive network event data of roaming subscribers. The home network and roaming subscriber has no control as to the extent to which these billing records are analyzed, stored and transferred solely for billing purposes. Furthermore, all communication conducted by the visiting subscriber is susceptible to abuse in a foreign domain.

Privacy concerns all relate to the current capabilities the foreign network and clearinghouse in having access to and analyzing privacy-sensitive roaming data for billing purposes. Of real concern is the potential for data mining for the sole purpose of information extraction by the foreign network. Techniques that the foreign network may employ include:

- Pattern matching (based on association rules or CDR sequence of events)
- Clustering (grouping CDR data)
- Classification models (using existing CDRs for future prediction)

Such techniques clearly illustrate the extent at which the foreign network may exploit privacy-sensitive subscriber information and derive benefit from this. These privacy threats have a direct impact on the subscriber and the home network operator. From a subscriber and home network privacy perspective, the following concerns are highlighted below, namely:

- How to retain subscriber anonymity from the foreign network operator;

- How to prevent the foreign network operator from using data mining methodologies on roaming subscribers' network event data (pattern, clustering and inference analysis); and
- How to protect the privacy of roaming subscribers against the misuse of network event data at a clearinghouse.

In a private communications network, subscribers are verified to perform events without revealing information about their identity. This disassociation is often referred to as *unlinkability*. Unlinkability is described as two or more items that are no more and no less related than they are related concerning a prior knowledge [123].

A home network allocated pseudonym [37] is one means to protecting the identity of the subscriber. From privacy terminology, allocating such a pseudonym is commonly used in achieving *unobservability*. Remember, unobservability is the state of items of interest being indistinguishable from any items of interest at all [123].

Arising from the fact that number portability is a real threat for network operators in retaining its subscribers, there exists a need to protect the associations and correlations between the data that is sensitive or private to roaming subscribers **and** network operators.

In a private communications network, the network provider is dutifully expected to provide privacy surety to its subscribers. This is magnified when the subscriber is outside the control of the network provider, roaming on an untrusted network. The home network must entertain the real possibility of competitive foreign networks from acquiring its subscriber base. Influencing subscribers to switch networks may be as a direct result by the foreign network performing a needs analysis according to the roaming subscribers' usage patterns. The foreign network may now target the individual subscriber and present a customised contract for a particular individual.

8.3 Roaming

Roaming is a key feature of any mobile communications network. Subscribers can seamlessly connect to other users in foreign domains (provided there are connectivity agreements between the roaming and the home network operators). Roaming refers to the extended service to a foreign network that is not the home network to which the subscriber is registered. The mobile subscriber roams in an area where the service provider does not have radio coverage; this usually occurs when the subscriber visits another country.

The functions needed for roaming are called roaming or mobility functions [51]. In GSM, they rely mostly on extensions of the Signalling System Number 7 (SS7) [97], which enables signalling between functional entities in the network system. The Mobile Application Part (MAP) [74] functions and

procedures used in roaming include amongst others Location Registration and Update, IMSI (handset) attached/detach and subscriber management. MAP functions correspond to the functions of Mobility Management (MM) [51] at the subscriber's interface which most importantly includes identification and authentication of the subscriber to the foreign network operator.

Take, for example, the scenario where a subscriber is outside the radio coverage of his home network. The home BTS (base transceiver station) has received an incoming call, and is required to deliver it to the subscriber, via a foreign network operator. This brief overview illustrates the functional entities (home and foreign) involved in handling such a network event.

- *Foreign VLR allocates MSRN to subscriber* - when the subscriber enters a foreign network operator location, the foreign VLR detects the subscriber's mobile and allocates a temporary Mobile Subscriber Roaming Number (MSRN).
- *Foreign VLR queries subscriber's Home HLR* - the VLR forwards the assigned MSRN to the home network, and queries the subscribers' home HLR (using the subscribers' mobile number). The home network now knows where the subscriber is, and can direct network events accordingly. The foreign VLR retrieves information from the home HLR to manage network events.
- *Home network routes incoming subscriber network events to the foreign network operator* - if an incoming call is received by the subscriber's home network, the home Gateway Mobile Switching Center (GMSC) dials the MSRN and routes the call to the foreign Mobile Switching Center (MSC).

8.3.1 Transferred Account Procedure (TAP) - Roaming Call Data Record (CDR)

The Transferred Account Procedure (TAP) [73], is the mechanism by which network operators exchange roaming billing information. This "roaming" Call Data Record (CDR) is a global telecommunications industry standard, developed by the GSM Association [72], which uses variable file format based on industry standard file encoding rules. The Transferred Account Data Interchange Group (TADIG) [73] was given the task of implementing and defining this roaming billing procedure. With TAP, roaming partners are able to bill each other for the use of networks and services of roaming subscribers through a standard process; refer to Figure 8.1.

The transfer of TAP records between the foreign and home network operator is either performed bilaterally (directly) between network operators, or, more commonly, indirectly via a clearinghouse. On receipt of the TAP records by the home network, the TAP record is converted for local billing purposes.

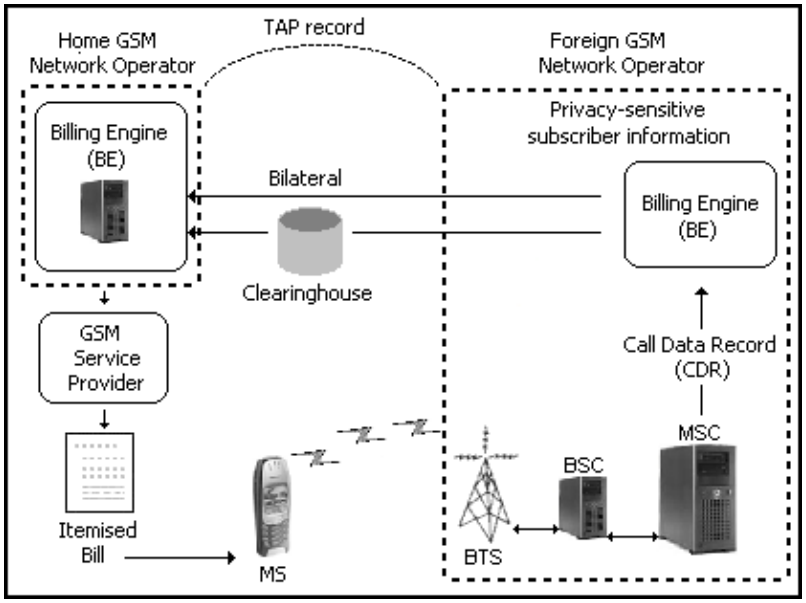

Figure 8.1: TAP information transfer between Foreign and Home GSM Network [36]

When roaming, all privacy-sensitive subscriber information and network event data resides on the foreign network. Furthermore, CDRs are passed between the foreign and home network Billing Engines (BEs) through a clearinghouse.

We design a Privacy-Preserving Roaming Network Architecture solutions to circumvent any privacy claims while roaming.

8.4 Privacy-Preserving Roaming Architecture

The purpose of the Privacy-Preserving Roaming Architecture is to eliminate the privacy concerns of the home network and subscribers where roaming GSM subscribers are concerned. As discussed earlier, privacy-preservation is achievable by restricting the foreign network operator and clearinghouse access to privacy-sensitive CDR information. In our design we choose to have a local store at the network and on the subscriber's mobile device as a means to enforce non-repudiation of roaming network events.

The Privacy-Preserving Roaming Architecture facilitates the following subscriber privacy concerns:

- The foreign network's ability to identify network events performed by the roaming subscriber
- The foreign network's ability to bill the roaming subscriber anonymously

- The foreign network's or clearinghouse's ability to perform data analysis, clustering or classification of CDR's describing roaming subscriber network events
- The verification of any network event confirmed by **both** the foreign and home network as well as the subscriber itself

The Privacy-Preserving Roaming Architecture (refer to Figure 8.2) identifies privacy critical components primarily from the roaming subscriber perspective, and secondly from the home network operator's viewpoint.

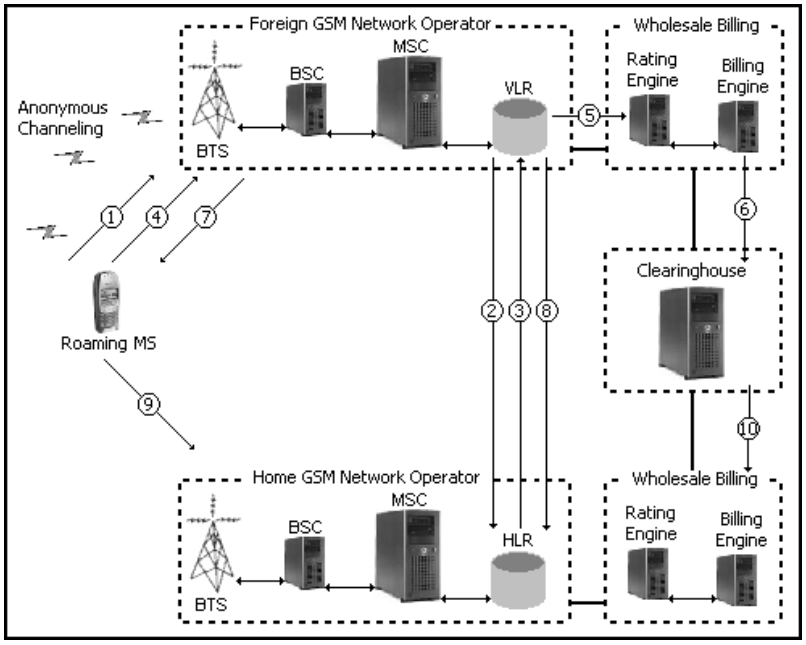

Figure 8.2: Privacy-Preserving Roaming Network Architecture

The aim of the architecture is to facilitate unlinkability between roaming subscribers and performed network events in the foreign network domain. Furthermore, sensitive information is unextractable via data mining techniques. In other words, such information is unobservable at both the clearinghouse and or the foreign network operator.

Figure 8.2 illustrates our proposed ten point process for preserving roaming subscriber privacy in order to remain anonymous to the foreign network and retain accountability for home network operator billing.

Our Privacy-Preserving Roaming Architecture uses pseudonymity to hide the roaming subscriber's details from the foreign network. However, in doing so, this complicates the authentication process - hence an appropriate authentication scheme needs to be devised. A ticket-based approach is the most logical. Once it has been established that the roaming subscriber

(known to the foreign network by a pseudonym) is allowed to make use of the foreign network's resources, billing remains an issue. Hence, an effective and accountable billing scheme needs to be devised which confirms non-repudiation of billable network events. A privacy-preserving ticket-stubbing approach is the most logical. We choose ticket-stubbing as sensitive information is not revealed in the billing record verification process and we are able to enforce non-repudiation of these network events.

Formally the ten steps taken are as follows:

Step 1: Roaming subscriber signs on to the foreign network anonymously. One approach to achieving anonymous subscriber sign on is by making use of anonymous channelling, which is discussed in detail in Section 5.4.

Step 2: Foreign network VLR assigns MSRN and queries the subscriber's home HLR. This confirms that the roaming subscriber has a valid home network operator. In using anonymous channelling it is important to note that the roaming mobile station MS (handset) possesses the home HLR's public key.

Step 3: Home network HLR returns pseudonym subscriber information (thus retaining subscriber anonymity) to the foreign VLR.

Step 4: Roaming subscriber performs a network event. In order to maintain foreign network event anonymity, we utilise the anonymous channelling ticket $(Auth_{VLR}; TK_i; T_{expire})$. For more on how this ticket is derived refer to Section 5.4.

Step 5: Foreign VLR generates a Call Data Record (CDR) and sends to wholesale billing for a costing calculation (also referred to as *rating*). In order to achieve anonymous billing, the CDR elements (To & Comms Type & TimeDate & Duration) are merely used in the CDR cost calculation and are not stored at the Billing Engine. To later confirm and verify any anonymous billable network event's occurrence, the Foreign VLR generates a ticket stub (T_{stub}) (refer to 7.5.1.1).

Step 6: Send ticket stub (T_{stub}) to clearinghouse where the ticket stub (T_{stub}) is a means of verifying a network event occurred relating to the anonymous channelling ticket $(Auth_{VLR}; TK_i; T_{expire})$ used. It is important to note that the ticket stub (T_{stub}) contains no privacy-sensitive CDR information and later plays a significant verification role for both the subscriber and home network.

Step 7: Send ticket stub (T_{stub}) and CDR elements (To & Comms Type & TimeDate & Duration) to MS (handset) using secure Over The Air (OTA) transmission. SIM Application Toolkit (refer to Section 8.4.1.1) is one means in getting information securely to the mobile device.

Step 8: Foreign network operator sends ticket stub (T_{stub}) together with the subscriber pseudonym to the home network operator (again for the home network to confirm that the roaming subscriber performed a billable network event).

Step 9: The MS (handset) returns to it's home network domain. The home network operator verifies the subscribers' ticket stubs and retrieves the associated cost from the clearinghouse and bills the subscriber. This allows the user to store all information pertaining to charges for roaming network events locally; this may be used by the home network for itemised billing purposes and by the subscriber for audit purposes. Using secure OTA, the home network operator deletes stored roaming stubs from the mobile device.

Step 10: If the ticket stub should expire at the clearinghouse before it is retrieved by the home network operator, the clearinghouse notifies the home network operator of the expired TAP record. It then remains at the discretion of the home network operator on how to bill these expired billing records.

8.4.1 Secure OTA transmissions and storage

Within the GSM network, the operator can at any given time order a change to data in the SIM card. This administrative management phase must be secured and protected. The European Telecommunications Standards Institute (ETSI) introduced the ETSI 03.48 [3] standard that supports the security services like integrity, confidentiality and peers authentication. This standard uses Short Message Service (SMS) [2] as bearer to exchange secured data between the SIM card and the network operator. In our Privacy-Preserving Roaming Architecture, secure OTA transmissions are used as a means to getting the ticket stub (T_{stub}) and CDR elements to the mobile (Step 7) as well as deleting this information after it has been verified at the mobile device (Step 9).

8.4.1.1 SIM Application Toolkit

ETSI further defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) within the digital cellular telecommunications system, known as"SIM Application Toolkit". SIM Application Toolkit is a set of commands that allows remote management of files on the Subscriber Identity Module (SIM) [58] in conjunction with SMS and the SIM Data Download feature [57].

In gauging the soundness of our architecture, this lends itself to a brief privacy analysis.

8.5 Privacy Analysis

This section describes how the initial privacy concerns of the subscriber and the home network have been addressed and later identifies the limitations of our Privacy-Preserving Architecture.

The Privacy-Preserving Roaming GSM Architecture has addressed the

privacy concerns by applying various privacy-enhancing techniques. Firstly, the identity of the roaming subscriber is unknown to the foreign network by making use of anonymous channelling. This is evident due to the fact that a home network assigned pseudonym is the only means for identification at the foreign network operator.

Through anonymous billing, privacy-sensitive subscriber information and network event data when roaming is unknown to the foreign network operator and clearinghouse. This is evident due to the fact that the TAP clearinghouse and foreign network billing engine only contains a large amount of ticket stubs (T_{stub}), and as a result, no sensitive CDR element information is stored anywhere.

The Privacy-Preserving Roaming GSM Architecture also addresses potential security vulnerabilities. By storing roaming network events both at the MS (handset) and home network operator, this enables verification and the authenticity of the roaming event (verification by ticket stubs). In addition, ticket stubs are stored securely on the SIM card, providing for non-repudiation of network events.

The Privacy-Preserving Roaming Architecture has the following potential limitations:

- Possible storage capacity of the SIM card, maximum ticket stub and CDR component threshold. This storage capacity depends entirely on the mobile device capabilities. This threshold calculation, however, remains outside the scope of this chapter.

- Lost or stolen mobile device. This effectively means that **only** the home network operator is able to perform the Roaming TAP records verification.

It may be important to note that some form of roaming subscriber profiling will still be possible. Take for example the traveler who frequently calls home may be linked by the daily call to the same number (buy yet still remain anonymous to the foreign network). However, if the traveler calls his office, these calls wont be linked to the home calls made.

All components involved in a roaming network event have been addressed in terms of privacy, namely: the roaming subscriber, the foreign and home network operator and TAP record clearinghouse.

8.6 Conclusion

This chapter is dedicated to finding a solution to protecting the subscriber's private CDR information while roaming on a foreign network. When private information is outside the jurisdiction of the owner and residing controlling authority it is susceptible to abuse. Our Privacy-Preserving Roaming Architecture provides a means to circumvent any potential privacy concerns

by anonymising the subscriber's connection and enhancing the privacy of the CDR through a ticket-stubbing mechanism. This allows for a subscriber based verification mechanism using the handset directly. Although possibly not the most elegant of solution (due to additional system overhead), given the available technologies we are able to construct a working solution given the roaming privacy requirements.

Chapter 9

Legal Privacy

9.1 Introduction

The needs of forensic investigators are often in direct conflict with the right to privacy of those whose actions are being investigated. Mechanisms have therefore been introduced to maintain an appropriate balance between these opposing needs and rights. For example, suppose investigator I suspects party S of having committed a crime, and a third party T has some information that may help to prove the guilt or innocence of suspect$S$. Furthermore, suppose there are certain conditions under which I may convince T to provide the information it has on$S$ and T may provide it without violating the privacy of$S$. When I obtains a warrant or court order stipulating that T should provide this information to investigator I, such warrant or order will only be issued when I has demonstrated to a judge or court that there are sufficient grounds to believe that the requested information will be useful to the investigation (and that the request does not impact unduly on the rights of$S$).

To illustrate the above concretely, suppose investigator I has demonstrated that the cellular (mobile) phone records of the suspect are relevant to a case – then a warrant may be issued that instructs the network operator (T in this example) to supply details of S's communication with I. However, access to information does (and should) not necessarily imply access to all information.

Suppose I wants to confirm whether S communicated with any of the other suspects$S_1, .., S_k$, and has demonstrated sufficient grounds that this could well have been the case. A typical warrant will then provide I with access to all the calls made by S. This is arguably more than was requested – I wanted to test some hypotheses (such as S communicated withS_1), but now has access to all numbers dialled by S. If S is indeed innocent, S has lost privacy, while I gained very little. The question is therefore whether the information can be provided in a form that allows the hypotheses to be tested without revealing all of the suspect's private information. Note

that providing the details of $S_1, .., S_k$ to I to only obtain "relevant" call information does not solve the problem, because sharing information about (other) suspects with a third party may compromise the investigation. (Note also that we are not addressing those investigations in which access to all numbers dialled by a suspect is warranted.)

Although the above illustrates that sometimes too much information is revealed to the investigator, too little is revealed in other instances. Suppose the revealed information shows that S sent an SMS (*short* or *text message*) to another suspectS_j and the network operator T retains copies of all such messages. The investigator will now have to present new evidence to a judge or other authority to obtain a new warrant to access the content of this message. If it is possible to encode the content such that it only becomes accessible once other required knowledge has been demonstrated, it may have been possible to release this "dependent" information with the first warrant.

A situation may arise where a forensic investigator may require multiple court orders to gain access to information. Information gathered from a data controller (the custodian of private information) is essential to the investigation. In our case, the desired result is evidence that is uncontested (from a technical perspective) when entered in a court of law. Furthermore, evidence should be gathered in a privacy-preserving manner. This chapter explores the technical feasibility of protecting information that is more sensitive until knowledge about less sensitive information has been demonstrated.

We introduce the notion of "privacy-accurate" information, which requires accurate knowledge about one part of a stored collection of private information before the next private part can be revealed. The idea is to create a self-preserving privacy object that releases undiscovered related information as knowledge about discovered information is shown.

The purpose of this chapter is to propose a mechanism that allows data to be packaged in such a way that more sensitive information only becomes accessible (for hypothesis testing) once knowledge about all layers lower in the hierarchy has been demonstrated. The intention at this stage is only to demonstrate the technical feasibility of such a mechanism – its usefulness in current (and future) legal regimes is not explored. It should also be noted that not all investigations can be conducted using this mechanism. Where it can be used (i.e. where the assumptions listed up to this point apply), however, we claim that the mechanism offers benefits for suspects (their privacy is protected until incriminating evidence has been shown), as well as for investigators (they may continue with an investigation without repeated requests for permission to do so).

9.2 Privacy Concerns of Legal aspects

People store private information on their phones, thus making the mobile itself a rich source of potential evidence for law enforcement officials. Likewise, stored network information for the purpose of billing a subscriber contains sensitive information which may be used in conducting a forensic investigation.

Often access to stored information, controlled by a presiding authority is necessary in order to conduct a forensic investigation. However, once a decision is made to proceed with a forensic investigation, current techniques do not allow for the accused to return to the original privacy-preserving state before the investigation began. Whether digital evidence is being used to implicate or exonerate a person, how reliably and accurately the data represents actual events can impact on an individual's liberty and life [115]. By the same token, inherent trust is placed in the forensic investigator when dealing with privacy-sensitive information during the investigation. The problem exists that once private information is revealed (enters into the public domain), it cannot be returned to its original private state.

At the core of forensic techniques is finding the identities of those responsible for a particular action. A forensic investigator seeks to know every detail about every aspect of every principal under investigation. Thus, the goals of privacy are apparently in direct conflict with the goals of forensics.

The problem exists in presenting a privacy-preserving means to conducting a forensic investigation on data records where accountable privacy is the goal, while providing a balance between the competing priorities of security, privacy and forensics.

9.3 Background

Privacy is well recognised as a fundamental human right. In technology, the term is generally used to refer to the security of data against various risks during transmission [32]. However, control of personal information is important regardless of where or what type of device or medium is used. Individuals have a right to control and protect their personal information in both virtual and physical worlds [113].

Rules of evidence govern whether, when, how and for what purpose evidence may be placed before a court of law for consideration. It may be considered "unprincipled" to simply retrieve, retain and process all related private information based purely on suspicion. Technical prowess aids in the masking of information for the purpose of creating a private forensic environment. The accused must be able to return to the original, private state held prior to the commencement of the investigation, should an initial suspicion prove to be incorrect. This necessitates the creation of distinctions concerning how information is abstracted, how it flows between people and

systems, and what constitutes a privacy violation.

In this section we use three fundamental concepts instrumental in the build-up to creating a privacy-preserving object that releases information sequentially. The first section focuses on privacy – in particular, information and expected flow. The remaining sections focus on the cryptographic technique used in creating privacy-accurate information.

9.3.1 Privacy, Information Spaces and Expected Flow

Recall from Section 1.1.2 that privacy is not an absolute notion, but rather a highly fluid concept about controlling the dissemination and use of one's personal information. Privacy protection is measured by assessing the appropriate physical, technical and procedural safeguards that are in place to protect the security and integrity of information.

There is a huge body of work that explores privacy. Studies are available on the direct conflict between of privacy and forensics [24], the impact of privacy on people's lives [27], the reasons why privacy is important [127] and ways to balance privacy using technology [9]. However, privacy protection must ultimately constitute the prevention of harm and protection of the free-flow of information. We are interested in preventing the free-flow of information where a forensic investigation is concerned in order to circumvent a privacy violation.

Taken verbatim from Section 1.1.2, Jiang et al. [2002] define a key set of abstractions that describe how information flows within a system of people and computers. The first abstraction considers the notion of *information spaces*, which is a collection of data delimited by physical, social or activity-based boundaries. Personal data is stored and used within an information space, and may flow into other information spaces. The second abstraction describes the life cycle of personal data, consisting of *collection*, *access* and *second use*. The third abstraction is a set of themes for minimising asymmetry that involves *prevention*, *avoidance* and *detection*.

The constant interactivity and change in information spaces makes it difficult to define explicit privacy boundaries. However, we can monitor and predict the flow of information. The capability to predict expected information flows allows for the formulation of a principle stating that information that is shared is not disclosed provided its flow is expected. Deviation from this expectation is considered a privacy violation. In general, once private information is exposed, deviation from the expected is not altogether probable, but possible. Indeed, a greater information exposure (even if the flow is expected) increases the potential of privacy violation. In summary, once private information is shared, the threat for exposure is real and, once divulged, cannot be rendered private again.

Cryptographic techniques do not prevent the unauthorised flow of information but rather render it useless if an unexpected flow does occur.

9.3.2 Hashing Techniques

Hashing techniques constitute one of the fundamental cryptographic techniques used in this chapter. The SHA1 [112] and MD5 [134] algorithms are two popular algorithms for generating cryptographic hash functions. Hashing algorithms possess two unique characteristics. First, given a hash value, it is difficult to construct new data resulting in the same hash. Second, given original data, it is difficult to find other data matching that original data's hash value.

9.4 Ordering and Privacy-Accurate Levels

In our privacy-accurate sequenced release of information, knowledge about one part of the private information justifies the interrogation of the next private part. One challenge is to determine what knowledge or which aspects of the private information justify revealing other parts. In other words, which parts of the available information are dependent on or independent of one another, and is there a distinct ordering?

9.4.1 Partitioning and ordering

To express the core problem of this chapter more precisely, assume that some set X of information may be useful during a forensic investigation. Further assume that some partition $P_1, ..., P_n$ of X exists (i.e. $\bigcup_{i=1}^{n} P_i = X$ and $1 \leq i, j \leq n, i \neq j, P_i \bigcap P_j = \{\}$). Initially we assume that the partitions are fully ordered in terms of sensitivity; in other words P_{i+1} contains more sensitive information thanP_i. (The partially ordered case is developed in Section 9.6.) If P_j contains more sensitive information than P_i (or equally sensitive information as P_i) it will be denoted by writing$P_j \succeq P_i$, given the assumption of fully ordered layers. Let P_i^+ indicate the immediate successor of P_i (if such a successor exists). In other words, if there exists a $P_j \succeq P_i$, then $P_i^+ = P_{i+1}$. Likewise, let P_i^- indicate a predecessor of P_i (if such a predecessor exists), denoted as $P_i^- = P_{i-1}$.

It is assumed that X contains facts. Assume, for example, that we are indeed working with a case related to telephones. Then it is possible that some fact $f_1 = DIAL(555 - 1234)$ may indicate that the number 555-1234 was dialled. If it was dialled from the phone in question, it will be the case that$f_1 \in X$. If this information is not sensitive, but is still private, then it may be the case that$f_1 \in P_1$. An example of private information that is easily inferred and not necessarily sensitive is the telephone number of an employer. Thus, the hypothesis $h(f_1 \in P_1)$ will evaluate to either true or false. Privacy protection ensures that no hypotheses about P_2 can be tested before a hypothesis about P_1 has been proven.

Suppose, for the sake of illustration, the numbers to which SMSs have been sent are seen as the least sensitive in a given investigation, that the

location of the user when sending such SMSs is deemed more sensitive and that the actual contents of the communication is deemed as the most sensitive information. Then this information, for the suspect, is partitioned inP_1, P_2 andP_3 respectively. Suppose f_1 is a claim that an SMS was sent to some number. Then $h(f_1 \in P_1)$ may evaluate to true if this is the case or otherwise return a negative result. Suppose, further, that f_2 is a claim that the user was in a given location when sending an SMS. Initially $h(f_2 \in P_2)$ should evaluate to *locked* because no evidence has been provided to "unlock" it. However, if $h(f_1 \in P_1)$ is true, then $h(f_2 \in P_2)|h(f_1 \in P_1)$ should evaluate to true or false, depending on whether f_2 is a fact or not. In general, hypotheses at a higher level may be tested the moment knowledge about a lower level has been demonstrated.

This example, however, also illustrates a special case: testing hypotheses about numbers used and locations from which messages have been sent is viable. However, testing a hypothesis about the content of a message will usually be less practical. Hence, in some cases it will be necessary to "open" the highest level for inspection rather than hypothesis testing. This can only happen on the highest level, since a revealed layer cannot be used to unlock higher levels. This means that full knowledge becomes available immediately and no further proofs of knowledge about the layer are necessary.

The general concern at this point is the possibility of getting to a higher layer without "knowing" the lower layers. Simply "testing" all alternatives via a brute force attack may yield the knowledge required to get to a higher layer. The concern is compounded when X (a set of facts $\{f_1...f_n\}$) from which the privacy-preserving object is created, is relatively small.

The strategy is to find a mechanism to limit the number of queries on a partition P_i. In other words, there is a requirement to limit the number of attempts (hypothesis tests) performed on a partition in order to thwart a brute force attack. The upper bound query limit should ideally be linked to the nature of the investigation and relate to the size of X. We need a mechanism to audit the number of query attempts without revealing the content of the hypothesis test to a third party. This is due to the fact that the information contained in the hypothesis test itself may contain privacy-sensitive information. To combat this problem, a signature scheme is used to sign each hypothesis test. This is discussed in more detail in Section 9.5.2.1.

9.4.2 Determining privacy-accurate levels

The notion of layering is a useful one: information is categorised, sorted according to certain criteria and ultimately structured in some hierarchy. Layering is important in the fully ordered case and of particular interest in the partially ordered case (see Section 9.6). It is just one viable strategy to illustrate the distinction between partitions.

Suppose at each layer the objective is to investigate the connection between the individual and his or her private information. From an unequivocal point of view, we may argue four basic but distinct layers. On the first level, information is unrelated to any specific individual. At the second level, information pertains to a set of individuals, which may imply individual involvement. At the third level, personal information of the individual is confirmed to exist in the given set and finally, the last layer contains only personal identifiable information of the specific individual. In other words, partitioned information is ranked from a low privacy-accurate level (denoted by P_1) to a high privacy-accurate level (denoted P_4). Each privacy-accurate level indicates a level of protection required for an association with the individual and strikes a balance between privacy and forensic ability.

To illustrate, take for example a case where illicit goods were bought by an individual believed to be associated in some way to the mafia. At P_1, we may want a hypothesis to test if a large amount of money has been transferred from one bank to another. Such information is unrelated to any personally identifiable information. AtP_2, we would want to confirm the particular banks involved in the transaction. Finding out which banks are involved may implicate a number of individuals, all who have accounts at the bank. At P_3, we need to confirm if the suspect is known to own an account at the bank in question. If this is the case, then this provides grounds for further investigation. On the last level (P_4), we wish to show the exact amount of money that was transferred out of the suspect's bank account.

In the general case, rules that classify information into partitions are as follows (refer to Table 1): on the first privacy-accurate level (P_1), information cannot be linked directly to the person with whom it is associated. In other words, private information is not necessarily identifiable information. Partitioned information does not explicitly divulge any personal information. At privacy-accurate level two (P_2), evidence may allude to personal information and imply involvement by certain individuals. At privacy-accurate level three (P_3), evidence may show personal involvement and result in possible inferences being made. The coupling of such evidence with other information may exonerate or implicate an individual. At privacy-accurate level P_4, evidence is undeniably linked to personal information. This confirms that evidence can be linked directly to the individual. Having used four layers to illustrate the concept of partitioning information, it is clear that the number of privacy-accurate levels P_n is dependent on the varying degrees of privacy required and may be influenced by the connection of personal information to the partition.

From the generic case and example above, facts in isolation do not always reveal personal information and as a consequence partitioning is not necessarily the immediate solution to privacy. Understanding the connection that exists between the individual and private information is what is

Privacy Accurate Level	Description	Qualification
PA_0	Evidence does not divulge any personal information	Unrelated
PA_1	Evidence may allude to any personal information	Implication
PA_2	Evidence may infer any personal information	Inference
PA_3	Evidence undeniably divulges personal information	Directly linkable

Table 9.1: A Proposed Scale for Privacy-Accurate Levels

important. It is only then that we are able to create a privacy-preserving object.

9.5 Sequenced Release of Privacy-Accurate Information

This section investigates how information is protected up until the point where it is released. Section 9.5.1 highlights the encryption process in creating a privacy-preserving object. Although the information is encrypted, there exists the possibility of getting to a higher layer without "knowing" the lower layers. Section 9.5.2 introduces a signing authority as an external counting party (to limit the number of queries against the privacy-preserving object).

Before encryption takes place, pieces of information are classified and partitioned into varying levels of privacy-accurate information. The idea is to create a self-protecting object. The use of self-protecting objects to prevent tampering with information in a specific environment is not new. Digital Rights Management (DRM) [125] is just one example that refers to access control technologies used by publishers, copyright holders and hardware manufacturers to limit the usage of digital media or devices.

After encryption has taken place, the aim is to find enough evidence based on previously gathered relational information (through a hypothesis test) to warrant the release of further information. When the correctness of a specific piece of information is shown (according to a hypothesis), additional "encrypted" piece(s) are made available for analysis. Through classification, partitioning and ordering, information extraction is conducted on structured information in a sequential manner.

At this stage the question of who should provide the self-protecting object becomes important. Before the entity may be extracted and compared to a hypothesis, it is suggested that the data controller present the information in a structured manner. For example, in a mobile communications environment, the network operator (custodian of mobile data records) is assigned the responsibility of providing a privacy-preserving object. As the data controller already possesses private information, it is possible to package data so as to not reveal it to another party.

We will demonstrate that cryptographic techniques provide the technical capability necessary for a sequenced release of privacy-accurate information. Information is extracted in a sequential manner through a hypothesis test. Such hypothesis test may form part of an overall theory that tries to confirm the facts surrounding a crime.

9.5.1 Creating a Privacy-Preserving Object for Forensic Analysis

The aim of the forensic investigator is to test a hypothesis in order to match individual pieces of partitioned information. Thus, if the forensic investigator does not possess a valid matching piece of information, he or she will not be able to continue to retrieve any relational information. This inability to verify against a hypothesis results in privacy preservation of the information and, in turn, protects the flow of information and privacy.

When creating a privacy-preserving object, the data controller begins by hashing each piece of information with a hash of itself. Each piece of information is then XORed with the key $k_{P_{(i+1)}}$at the next privacy-accurate level.

In order to formulate this more precisely, assume a piece of information (referred to here as an *element)* exists at a privacy-accurate level P_i where n represents the highest privacy-accurate level. We define each *element* such that:

$$element_{P_i} = \langle hash(element_{P_i}); element_{P_i} \oplus k_{P_{(i+1)}} \rangle \tag{9.1}$$

where $1 \leq i \leq n$ and

$$element_{P_i} = \langle hash(element_{P_i}) \rangle \tag{9.2}$$

for $i = n$

Keys are assigned that encrypt each element based on its privacy-accurate level and the privacy-accurate level of its successor(s). Remember, a successor refers to an element on a higher privacy-accurate level. If the case arises that access to an element at P_n is required, it is logical to simply "open" the element by confirming its hash (refer to Equation 9.2).

To illustrate, suppose four keys are assigned (as in Section 9.4.2), one for each privacy-accurate level, $P_1 ... P_4$. Then we define the encryption of the *element* with privacy level P_i as:

$$E(element_{P_i}) = [element_{P_i}; k_{P_i}] \tag{9.3}$$

where $1 \leq i \leq 4$.

Once a hypothesis proves correct, it is necessary to reveal the key for the next layer. In other words, once $hash(element_{P_i})$ (refer to Equation

9.1) has been confirmed, the successor key $k_{P_{(i+1)}}$ is retrievable with the $element_{P_i}$ in the following way:

$$(element_{P_i} \oplus k_{P_{(i+1)}}) \oplus element_{P_i} = k_{P_{(i+1)}} \tag{9.4}$$

Informally, if the hypothesised element (with privacy-accurate level P_i) is hashed with the $element_{P_i}$, revealing the $element_{P_i}$ information again, then we may use the $element_{P_i}$to retrieve the key, $k_{P_{(i+1)}}$. In other words, key extraction is based only on proving the correctness of the hypothesised element. The key for extraction at the next privacy-accurate level is achieved through a simple XOR operation shown in Equation 9.4.

If any hypothesis for a specific $element_{P_i}$ is incorrect, the forensic investigator may continue with the investigation but not proceed to the next level, as $k_{P_{(i+1)}}$is incorrectly extracted. This demonstrates the technical feasibility of a self-preserving object as a mechanism that allows data to be packaged in such a way that more sensitive information only becomes accessible (for hypothesis testing) once knowledge about layers lower in the hierarchy has been demonstrated.

In cases where we come up with a tenable theory on how the crime was committed (based on suspicion), we need to map out a path of what information needs to be confirmed. Assuming this theory comprises a sequence of hypotheses, then if each hypothesis proves correct; all information is revealed in a complete and accurately sequenced manner.

At this point it should be clear that there may be a number of ways of getting to a higher layer if more than one piece of information exists on a partitioned layer. In other words, a situation may arise where we can get to the top layer via any number of paths or sequences of hypothesis tests. In the partial ordering case, it is not necessary to know every piece of information on a particular layer to move to a higher layer (refer to Section 9.6).

9.5.2 How to Limit the number of queries against the Privacy-Preserving Object?

Recall the concern that was expressed earlier of possibly getting to a higher layer without "knowing" the lower layers. Thus there is a requirement to audit the number of query attempts, due to a possible brute force attack on the privacy-preserving object at P_i. This problem is similar to that of the digital cash problem, where a bank must ensure a digital coin is spent only once while not knowing who it was used by and for what purchase. In the digital cash scenario, the bank is not only a signing authority but also a counting authority. In our case, we require an authority to sign our privacy-preserving object so as to count and limit the number of hypothesis tests. Furthermore, no knowledge of the hypothesis tests ought to be gained. This

is due to the fact that the information that forms part of the hypothesis test may include privacy-sensitive information.

In a privacy-preserving forensic investigation, we envisage involvement of the following four parties: i) the data controller (DC), ii) the forensic investigator (FI), iii) the signing authority (SA) and iv) a court of law (CL). The DC is responsible for creating the privacy-preserving object. The FI's role is to confirm fact through hypothesis testing. The SA, by signing each hypothesis test, limits the number of queries against the privacy-preserving object. A prerequisite is that in the signing process the SA may not be exposed to the contents of the hypothesis test. The reason for the CL's involvement is to inform all parties with relevant information concerning the case. This might include information such as the case number, the privacy-accurate layers and data composition.

In brief, the DC sends the data to the SA, who signs it. The data is blinded, so the SA does not learn the contents of the data. These signatures(rather than the data) is used to build the privacy-preserving object, that is sent to the FI. The FI forms hypotheses and sends them to the SA, who signs them. Again the data is blinded so that the SA does not learn the contents of the hypotheses. If the FI finds a match between a signature in the privacy-preserving object and the signature of a hypothesis, it has proven knowledge about that specific data item. The SA signs only a prespecified number of hypothesis on a given level, so the number of tests is effectively limited. The SA only sees blinded data so it does not know the contents of the actual data or hypotheses. The FI only receives signatures, so no alternative way of extracting data from the privacy-preserving object is possible.

9.5.2.1 Blind Signing

In order to formulate the signing process more precisely – if the signing authority has a private/public key pair, then $element_{P_i}$ is signed with private key $priSA$ as follows:

$$sign(e)_{P_i} = [element_{P_i}; priSA] \tag{9.5}$$

If theDCcreates an encrypted message m as follows:

$$E(m) = [hash(element_{P_i}), pubDC] \tag{9.6}$$

then the encrypted message is signed by the SA as follows:

$$sign(e)_{P_i} = [[hash(element_{P_i}), pubDC], priSA] \tag{9.7}$$

The reason for the DC to $hash$ the $element_{P_i}$is to hide the original data. The rationale behind the encryption with$pubDC$ is to blind the message (to the SA) during the signing process.

If the DCchooses to decrypt $sign(e)_{P_i}$ with $priDC$ as follows:

$$D(sign(e)_{P_i}) = [[[hash(element_{P_i}), pubDC], priSA], priDC] \tag{9.8}$$

then the signature is "unblinded" by the $DC's$ private key $priDC$ and results in a signature that is now suitable to distribute and compare with a signed hypothesis:

$$sign(e)_{P_i} = [hash(element_{P_i}), priSA] \tag{9.9}$$

If we are to substitute $sign(e)_{P_i}$ for $element_{P_i}$ in $E(element_{P_i})$ when creating the privacy-preserving object, then the key extraction of the key at the next layer $k_{p_{(i+1)}}$ is indeed possible (refer to Equations 9.1- 9.4).

9.5.2.2 Hypothesis Testing

For any hypothesis test, suppose the FI generates a hypothesis hyp_{P_1} which is *hashed* and encrypted with $pubFI$ and signed by the SA so that it results in $sign(h)_{P_i} = [[hash(hyp_{P_1}), pubFI], priSA]$. Each time a request for a signature is received, the SA will return a signature provided that requests to do so have not been exceeded for a particular layer. If this is the case, $sign(h)_{P_i} = [hash(hyp_{P_i}), priSA]$ is returned to the FI. The latter confirms whether the element and hypothesis have both been signed, in other words, whether a match has been found ($sign(h)_{P_i} = sign(e)_{P_i}$). If this equality is true, then the hypothesis proves correct and the key $k_{p_{(i+1)}}$for the next layer is extractable (using Equation 9.4).

A possible security extension for the SA is to sign each layer with a different key pair ($pubSA_{P_i}$;$priSA_{P_i}$). A matrix of such information consisting of key pairs, layers, FIs and case numbers may be provided by the CL at the outset of the investigation. At the very least, this limits the number of allowed signatures per layer and eliminates the possible threat of collusion between FIs who may share "spare counts" in order to help one another.

9.5.3 Privacy Analysis

It has already been argued above that the SA does not learn the contents of the actual data or the hypotheses. Similarly, the FI does not learn the contents of the data unless proven by hypotheses.Since the data on a higher layer is still encrypted with that layer's key, a hypothesis on the lower layer still has to be proven before hypotheses may be tested on the higher layer.Collusion between parties is still possible, but collusion was not part of the problem the chapter addressed: The DC currently has the complete set of private data and may expose it - on its own or in collusion with any other party. Mechanisms to ensure the privacy of data held by a data controller falls outside the scope of the current chapter; the interested reader

is referred to [151]. The SA is trusted to only encrypt a limited number of hypotheses. If it colludes with the FI a brute-force attack may still be mounted. However, even if collusion is possible the suggested solution represents an improvement over the current situation where information is simply revealed and will be seen by investigators, whether they are trusted or not - effectively violating the privacy of the innocent.

9.6 Partial Ordering

In many cases, a number of individual pieces of private information may reside at a particular privacy-accurate level. These pieces of information may or may not relate to one another. This suggests the frequent adoption of a partial ordering privacy-accurate system (refer to Figure 9.1), as not all pieces of private information in the fact set X are mutually comparable under the relation. For example, Figure 9.1 shows that node x, y (which resides at privacy-accurate level P_3) is comparable under the privacy relation through either x or y (both of which reside at privacy-accurate level P_2). These, in turn, are both comparable under the privacy relation to 0 at privacy level P_1.

Take again our mobile example. If we are to assume that two mobile numbers exist on layer one, both may lead to the same location information on layer two and different SMS (*short message* or *text message*) information on layer three.

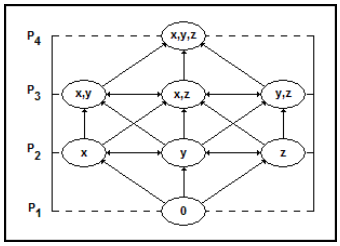

Figure 9.1: A Proposed Partial Ordering Privacy-Accurate System

In other words, a number of paths traverse to the highest layer and we may traverse through a number of nodes on a particular layer before moving to a higher layer. That is of course only if knowledge is shown about a particular node.

The only significant difference between a fully and partially ordered privacy-accurate system is the impact on the encryption process, key extraction and release of private information. Limiting the number of queries may alter the number of "proofs" required at a particular layer P_i in order to "move" to a higher layer. In the partial ordered case, sets of keys are needed that traverse different paths when information extraction takes place. Traversing a path to the highest layer discloses different key sets. It

appears there are no significant changes to the proposed mechanism for the partially ordered case.

9.7 Conclusion

We proposed a mechanism that allows data to be packaged in such a way that more sensitive information only becomes accessible (for hypothesis testing) once knowledge about all layers lower in the hierarchy has been demonstrated. The intention was to demonstrate the technical feasibility of such a mechanism. The mechanism offers benefits for suspects (whose privacy is protected until incriminating evidence has been shown), as well as benefits for investigators (who may continue with an investigation without repeated requests for permission to do so).

Although additional complexity is added to the investigation, evidence gathered sequentially does not infringe upon the individual's privacy should the hypothesis prove correct. Additional private information is not necessarily divulged by using this approach. However, failing to adequately protect a suspect's privacy increases the possibility of counter privacy violation litigation at a later stage.

The sequenced release of information is the key to preserving privacy and is achieved by assigning keys to govern the hierarchical release of private information during the forensics investigation. The forensic investigator is able to override (based on a hypothesis) any privacy classification to extract the relevant privacy-accurate information in a sequenced manner (if the hypothesis proves correct). This preserves privacy-sensitive information that is irrelevant to the case from being unnecessarily released during the investigation.

It is noted that in some cases it will be necessary to "open" the highest level for inspection rather than to do hypothesis testing. There is no significant change in the approach taken during such an investigation other than first verifying the most significant information that is able to sequentially release less privacy-sensitive information during an investigation. This method allows for the preservation of a suspect's private state only if a supporting hypothesis at a lower privacy-accurate level is needed.

We considered the possibility of getting to a higher layer without possessing the required knowledge to do so. A signing and counting authority was introduced to prevent a possible brute force attack. Throughout the chapter we adopted a fully ordered approach when creating and extracting information from the privacy-preserving object. We extended this briefly to the partially ordered case and discussed the impact on the privacy-preserving object and the forensic process.

Chapter 10

Communication Channel Privacy

10.1 Introduction

This chapter investigates ways of protecting the privacy of sensitive information traveling over the air waves. Encryption solutions can offer privacy protection however in some circumstances may have limited use. We draw on other wireless technologies in order to protect this sensitive information.

Devices used in ubiquitous computing often have limited computing power and/or access to limited bandwidth. A wireless sensor network [46] and GSM [128] are just two examples of such a technology where both these constraints apply. In such environments encryption may be too expensive or too slow to secure communications. Even worse yet, due to these constraints encryption techniques may be significantly weakened, augmenting the possibility of real-time attacks. This chapter explores the notion of codec-hopping and non-interactive key exchange as additional techniques to securing traditional voice in such environments, thus protecting communication channel privacy.

More specifically, we encompass the concept, benefits and techniques used surrounding frequency-hopping in current wireless technologies and apply to it the notion of codec-hopping as an additional security and privacy extension for end-to-end real-time voice communication in bandwidth constrained communication networks.

Non-interactive key exchange provides two parties, not sharing any secret information initially, the ability to generate a secure cipher key and encrypt messages using standard cryptosystems. This facilitates secure end-to-end communication which is unaffected by the underlying network.

Codec-hopping and non-interactive key exchange make it extremely difficult for an eavesdropper to listen in on a communication channel and in real-time decode (decipher) the communication. Codec-hopping is ideal where bandwidth is constrained and encryption is unnecessary or not possible,

however a degree of privacy in communication is required.

10.2 Privacy Concerns in Communication Channels

Speech coding can be defined as a conversion of analogue speech into a digital format (a sequence of binary digits). A voice codec, collectively called vocoders, is a routine that converts spoken word into digital code and vice versa. The major aim of vocoders is to compress (encode) the signal in such a way as to reduce its bit rate while maintaining both intelligibility and natural sound of speech. Intelligibility of voice includes, besides the actual literal content, the speaker's emotions, tone and quality. So an ideal codec is one where the reconstructed speech is identical (or nearly identical) to the uncoded speech and is represented by as few bits as possible. In practice, however, there is a trade-off between the quality of the reconstructed speech and the bit rate of the chosen codec.

10.3 Speech properties

Speech signals show a high degree of predictability; speech coders attempts to exploit this predictability in order to reduce the bit rate necessary for good quality voice transmission [156].

10.3.1 Speech Coding

Speech coding [16, 126] is defined as a way of representing analogue waveforms as a sequence of bits in order to speed up transmission and or save storage space. The basic idea of voice codecs is to benefit from the special properties of speech as discussed in Section 10.3 namely statistical redundancy, correlation and its periodic nature and to utilise the disadvantage in a human's ability to receive (hear) certain sounds.

Quantisation can best be described as taking a range of values and representing it in a single value. In terms of speech, it is the process of approximating a continuous voice signal by a set of discrete symbols or integers, converting an analog signal to a digital signal and vice versa. Quantisation is an integral part of lossy compression algorithms. Lossy compression is a data compression method which discards (loses) some of the data with the result that decompressing the data yields content that is different from the original content.

Statistical redundancy can be exploited by introducing prediction schemes, which quantise the prediction error instead of the speech signal itself. Due to the nature of voice and the issues regarding specific latency requirements, codecs aim to reduce the amount of delay in transmission. The delay of a speech codec is defined as the time from when a speech sample arrives at the input of its encoder to when the corresponding sample is produced at the output of its decoder. The fundamental idea behind speech coding can be

summarised as follows: to reduce redundancy by prediction and to minimise irrelevance by quantisation.

Bandwidth is easily quantified; however voice quality is completely subjective. Mean Opinion Score (MOS) is a means to rate voice codec quality and is described in [85]. A MOS value of 5 indicates excellent quality, while 1 shows a poor voice quality. A MOS value of 4.0 or higher is often referred to as toll quality.

Speech codecs are divided into three different speech coding methods, namely: i) Waveform codecs ii) Source codecs and iii) Hybrid codecs. Waveform codecs are typically used at high bit rates, and give a very good quality coded speech. Source codecs, on the other hand, operate at low bit rates and is inclined to produce synthetic sounding speech. Lastly, hybrid codecs use techniques from both waveform and source coding, which results in relatively good quality speech at intermediate bit rates.

In the sections that follow we explore these three speech coding methods in more detail and give some examples of each.

10.3.1.1 Waveform Codecs

Waveform codecs do not use any knowledge of the source of the signal, in other words, how it was generated. They simply sample the signal and code it. Waveform codecs produce are constructible digital signal whose waveform is as close to as possible to the original analogue signal.

The simplest, purest and most commonly used form of waveform coding is Pulse Code Modulation (PCM) [86]. PCM samples the analog waves and converts (quantises) each sample into an 8 bit number. PCM is often used in Public Switched Telephone Networks (PSTN), also known as landline networks, where the and width is limited. The international G.711 [84] standard is the most commonly used PCM, primarily used in telephony. G.711 is an International Telecommunication Union Standardisation Sector (ITU-T) standard that was released for usage in 1972 with a MOS of about 4.3. There are two main algorithms defined in the standard, u-law (America) and a-law (Europe). The a-law algorithm is sampled at 8 bits per sample and is sufficient to give a good quality speech with the advantage of low complexity and delay. By making use of a-law, a bit rate of 64kb/s (8 bits x 8kHz) is obtained.

Due to correlations present in speech, an attempt to predict the next value from the previous sample is possible. If the predictions are effective then the error signal between the predicted samples and the actual speech samples will have a lower variance than the original speech samples [156]. This is measured in terms of what is known as the Signal-to-quantisation-Noise-Ratio (SNR). A low SNR means it is possible to quantise this error signal with fewer bits than the original speech signal. By transmitting only the difference between the predicted value and the actual value there is no

algorithmic delay. Having said this, it is important to note that the receiver must perform the same prediction. This forms the basis of Differential Pulse Code Modulation (DPCM) schemes, which quantise the *difference* between the original and predicted signals.

Where costs are high and loss of voice quality is acceptable, DPCM results can further be improved if the predictor and quantiser are adaptive so as to change to match characteristics of the speech being coded. This is a further extension of PCM and is referred to as Adaptive DPCM (ADPCM). ADPCM maps a series of 8 bit PCM samples into a series of 4 bit ADPCM samples, effectively doubling the line capacity. Two examples of ADPCM are the G.721 and G.726 [33] standards.

10.3.1.2 Source Codecs

Source codecs try to produce a digital signal by using a model of how the source was generated, and attempts to extract from the signal being coded, the parameters of the model. In other words, source codecs match the incoming signal to a mathematical model where information of the signal is sent rather than the signal itself. These model parameters are then transmitted to the decoder [156]. Source codecs tend to operate at a low bit rate and produces voice which is intelligible but far from natural sounding (synthetic). A higher bit rate unfortunately does not improve the quality of speech.

10.3.1.3 Hybrid Codecs

Waveform codecs provide good quality coded speech at bit rates down to 16kbits/s while source codecs, on the other hand, provide intelligible non-natural sounding speech at 2.4kbits/s and below. Hybrid codecs, as the name suggests, attempt to bridge the divide between waveform and source codecs. The most commonly used hybrid codec is the Analysis-by-Synthesis (Abs) codec. Abs codecs work as follows: the input speech to be coded is split into frames (usually 20ms in length). For each frame parameters are determined for a synthesis filter, and then the excitation to this filter is determined [156].

Another hybrid codec example is the Multi-Pulse Excited (MPE) codec [138] which differs from Abs in that the excitation signal to the filter is given by a fixed number of non-zero pulses for every frame of the speech. However, in Regular Pulse Excited (RPE) codecs these pulses are regularly spaced out at some fixed interval. Therefore, the RPE codec has to transmit less information about pulse positions.

One last example is the Code Excited Linear Prediction (CELP) codec [138]. It differs from MPE and RPE in that the excited signal is effectively vector quantised. In CELP codecs, the excitation is given by an entry from a large vector quantiser codebook, and a gain term to control its power.

10.4 GSM Speech Encoding

Channel bandwidth limitations and device limitations in ubiquitous networks, like those present in Global System for Mobile Communications (GSM) [110] [128], prohibit the use of certain codecs over a specific bit rate (13kb/s). In GSM's case, speech is divided into 20 millisecond intervals (i.e. 50 intervals per second). Each interval is encoded as 260 bits, resulting in a total bit rate of 13kb/s [56] [36]. Bandwidth limitations and associated cost thereof is a restricting factor that determines the use of a specialised or low bit rate propriety codec. This bandwidth limitation may prohibit the use of encryption completely as a security measure and/or could possibly lead to the implementation of cryptographically weak algorithms, as is the case in GSM [121]. The problem is evident, network latency issues may exclude the use of encryption as means to providing security and privacy in communication.

10.5 Frequency-Hopping

Frequency-hopping is a technique used in signal transmission deployed in wireless technologies such as Wireless Local Area Network (WLAN) and Bluetooth. It is the repeated switching of frequencies during radio transmission, often to minimise signal interference from other transmissions in its environment and sometimes as a security enhancement to prevent unwanted communication interception. A transmitter "hops" or "jumps" between available frequencies according to a specified predetermined, pseudo-random pattern. The transmitter thus has to synchronise with a receiver according to this hopping pattern in order for communication to take place. A short burst of data is transmitted after which the transmitter "tunes" or "switches" to another frequency to send its next short burst of data. The transmitter thus is capable of hopping its frequency over a given bandwidth several times a second (in the case of Bluetooth 1600 slots [77]). The transmitter and receiver must remain synchronous to be able to communicate with one another. Benefits of this approach include improved privacy, decreased interference, and increased signal capacity.

Conventional fixed frequency radios are designed to transmit and receive on a single channel. This fact makes them vulnerable to techniques such as interception and jamming. Interception is the unauthorised monitoring of radio traffic, while jamming is the deliberate disruption of communication, by operating another transmitter or "jammer" on the same frequency as the radio traffic. Whilst encryption may provide some degree of resistance to the threat of interception, they are ineffective against jammers. Frequency hopping is the only effective countermeasure to these forms of attack.

Most WLANs and Bluetooth devices make use of spread-spectrum technology. This broadband Radio Frequency (RF) technique was developed by

the military for use in reliable and secure communications systems. Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the signal. The transmitter "spreads" the energy, initially concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum. Spectrum modulation techniques present two major advantages namely low power density as the energy is transmitted over a wide band and redundancy as a message is recoverable from more than one frequency in case an error occurs.

A common type of spread-spectrum radio is Frequency Hopping Spread Spectrum (FHSS). FHSS is robust, highly scalable and implemented in Wireless Local Area Networks (WLANs) that meets an international communications standard, for example the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification [81]. FHSS accomplishes the "spreading" by moving the center frequency meaning that the receiver must hop or jump from frequency to frequency at the same time as the transmitter. To an unintended receiver, FHSS appears to be short-duration impulse noise.

Bluetooth is a short-range radio technology that uses spread-spectrum frequency hopping. A piconet is formed when one Bluetooth radio connects to another Bluetooth radio. Both radios then hop together through either 79 or 23 channels depending on the frequency hopping scheme. The Bluetooth radio system supports a large number of piconets by providing each piconet with its own set of random hopping patterns. Occasionally, piconets will end up on the same channel. If this should occur, then the radios will hop to a free channel and re-transmit the data if it were lost in the communication process.

The spreading code is a list of frequencies to be used for the carrier signal; this is known as the hopping sequence. In FHSS, the carrier will hop on a predetermined, pseudo random pattern defined using a pool of 1 MHz sub-channels defined across the entire band. The pseudo random numbers are generated by a deterministic algorithm using an initial seed. In order to predict the sequence knowledge of the algorithm, the seed is needed. Take for example 78 hopping patterns organised in 3 sets of 26 patterns each. Denote frequency as $2432 + b_i$, b_i is the base sequence in range 0 to 78. The k-th sequence is formed from the base sequence as $2432 + (b_i + \mathrm{k}) \bmod 79$. The hopping sequence means that the units should commence working in a frequency, then hop to another, and so on, until the end of the pattern is reached and the cycle commences again.

FHSS was originally conceived as a means to hide a transmission from unwanted listeners during World War II. However, due to the fact that FHSS is based on a predetermined hopping sequence that is not considered secret, it no longer offers any form of inherent security [36]. If the hopping sequence were to remain secret and communicated between the transmitter and receiver in a secure manner it would suffice to say that the communication

is protected from potential eavesdroppers. However due to the nature of WLAN and Bluetooth allowing connection from interested parties by default, the hopping sequence is usually sent in the clear across the network.

If we look a spread spectrum technologies holistically, some of the most important attributes are:

- Secure data communications (if the hop sequence is known to only the communicating parties)
- Anti-jamming capabilities
- Outside interference rejection
- Multiple access capability
- Protect multi-channel interference
- Low probability of intercept (if the hop sequence is known to only the communicating parties)

Frequency-hopping is a means or alternative to encryption techniques to better secure and enhance communication privacy for any narrowband RF.

Although the frequency spectrum in WLAN and Bluetooth is bounded (2.4 GHz band), if regulation allowed, could extend over a wider frequency range resulting in a larger hopping set and cycle repetition.

We now investigate the concept of codec-hopping incorporating concepts learned from frequency-hopping schemes in order to enhance communication channel privacy.

10.6 Codec-Hopping

The concept of codec interchange exists already today, however this is due typically to the various backbone infrastructures found in most communications networks. One example exists in Voice Over IP (VoIP) [93] networks where most clients available tend to use "handshaking" to determine the correct compression algorithm. The Marathon Project [22], a cross-platform VoIP solution, implements dynamic codec hopping depending on available bandwidth. The codec interchange remains unaffected by consistencies in available bandwidth and the codec utilised may be determined by an eavesdropper based on the knowledge of available bandwidth. Another example is a GSM call made to land-line number (GSM to PSTN). In this example two different communications networks namely GSM and PSTN need to carry the call on different infrastructures using different coding techniques. The GSM to PSTN voice call is coded using the GSM codec [56], followed by some G.72x coding at an IP network level and then finally coded using the G.711 (PSTN) codec. This form of codec interchange does not lend itself to

any form of security/privacy enhancement as certain sections in the communications path use specific codecs. An eavesdropper may position himself at a specific point in the communications path, knowing that a specific codec was used, the channel could be exploited. Codec-hopping, alleviates this problem as at any point along the communications path various encoding algorithms are used thus making it difficult for an eavesdropper to reconstruct the original speech in real-time from the communications channel.

Where bandwidth is a limiting factor, strong encryption techniques may not be a plausible option (due to its increased computational overhead) in ensuring secure and private voice communication. As noted earlier, in any ubiquitous communications environment, devices with low computational power may not facilitate encryption techniques. Even if bandwidth is not a limiting factor, these "dumb" devices may not have the ability to encode complex algorithms at high or low bit rates.

Codec-hopping provides an alternative approach to improving security and privacy of real-time communications from eavesdroppers. Codec-hopping may be deployed in conjunction with encryption techniques; however, deployment in a bandwidth constrained communications environment without encryption where encryption may cause delays (latency) not conducive to voice communication.

There are a number of issues to consider when deploying a codec-hopping scheme. From frequency-hopping we identify the following important aspects for a codec-hopping scheme: i) Hop patterns ii) Hop frequency and repeats iii) Use an extended codec set iv) Concealment of the hop set and v) Codec method approach.

10.6.1 Codec Hop patterns

FHSS (802.11–2.4GHz) is restricted to an upper bound and lower bound frequency band; for this reason the number of hopping patterns is limited. Codecs have no such obligations and therefore codecs enjoy the property of unlimited hop patterns, provided there are unlimited codecs available. Thus the codec hop pattern is reliant on the number of codecs (standardised or propriety) available.

10.6.2 Codec Hop frequency and repeat cycles

Take the following example: Assume input speech to be coded is divided into frames of 20ms each. This results in a total of 50 frames/s from the input speech. Therefore the maximum hop frequency reachable is 50 hops/s (assuming we use one codec per frame). It is evident that from this example the maximum number of codec hops is relational to the input speech divide. The input speech can further be divided into frames of varying length depending on the codec used but is not considered here. It is important to note that a value trade-off may occur between the complexity of changing

codecs frequently and the necessity to codec hop frequently (50 hops/s), this however is left for future work.

As in frequency-hopping, the strength of such a scheme is reliant on a large hop set which results in a larger time delay in its repetition. Thus, in order to increase the associated security and perceived privacy the repeat cycles of a codec-hopping scheme should be infrequent.

10.6.3 Using an extended Codec set

It is obvious that as the number of codecs used in a codec-hopping scheme increases so it becomes more difficult for an eavesdropper to listen in and decipher communication on a channel. It becomes apparent that as the number of codecs used increases so the complexity of coding and reconstructing speech increases. This trade-off is not considered in this chapter.

10.6.4 Concealment of the hop set

As in frequency-hopping, in order to protect communication only the transmitter and receiver should know the hop set. The hop set needs to be exchanged between the transmitter and receiver before communication takes place.

10.6.5 Codec method approach

As long as the transmitter and receiver remain are synchronised with each other in terms of the code pattern (hop set), the codec method approach is irrelevant; however one must consider the complexity at both ends is affected due to the use of these different codec method approaches. We may possibly choose, for example, only waveform codecs.

10.7 Codec-Hopping initialisation phase

Before codec-hopping takes place, we identify the following key aspects in the initialisation phase of a codec-hopping voice communication: i) Codec availability ii) Limitations in bit rate iii) Quality of Speech iv) Limitations in the number of codecs used and v) Hop sequence determination and distribution.

These key aspects play an integral role in the initialisation phase of a codec-hopping scheme; therefore we discuss each of the five facets in more detail.

10.7.1 Codec availability

Although fairly obvious, it is essential that codecs used by the transmitter for speech coding are available at the receiver's end for speech reconstruction. Proprietary codecs as opposed to common standardised codecs shared

between transmitters and receivers may further diminish the possibility of a successful eavesdropper attack.

10.7.2 Limitations in bit rate

Limitations in bit rate are a direct result of limitations in available bandwidth. This restriction may further limit the available codes the transmitter and receiver can use.

10.7.3 Quality of Speech

From Section 10.3.1 we recall that Mean Opinion Score (MOS) [85] is a means to rate voice codec quality. Therefore codec-hopping speech quality requirements are best represented by a MOS value. It is important to note that limitations in bit rates may influence the maximum obtainable MOS value (depending on the codecs used), affecting the quality of speech. Perhaps toll quality speech is a requirement, then quality of speech is represented by a MOS value of 4.0.

10.7.4 Limitations in the number of codecs used

In order to achieve a desired level codec-hopping complexity, a minimum limit (lowerbound) on the number of codecs in the hop set is a prerequisite. A codec set for example consisting of two codecs may not be sufficiently complex to alleviate the threat from potential eavesdroppers. By the same token, a restriction on the maximum limit (upperbound) on the number of codecs in the hop set is for example influenced by computational limitations at the transmitter' send.

10.7.5 Hop sequence determination and distribution

A pseudo-random algorithm computes the codec hop sequence. The hopping sequence means that the transmitter should encode using a particular codec, then hop to another, and so on, until the end of the pattern is reached and the cycle commences again. Although not outlined in detail, the secure communication of the hop sequence is achievable using various encryption techniques and is dependent on the device's computational ability.

In initialising codec-hopping, it becomes apparent there is a logical sequence of events; for example we cannot include a codec in the hop sequence if it is not supported by both the transmitter and receiver. Taking such restrictions and formulating them as logical steps, we define an approach to a rule-based initialisation phase setup.

10.8 Rule Based Setup

In the initialisation phase we define the transmitter as T and the receiver as R. The rule based codec-hopping initialisation setup is as follows (refer to Figure 10.1):

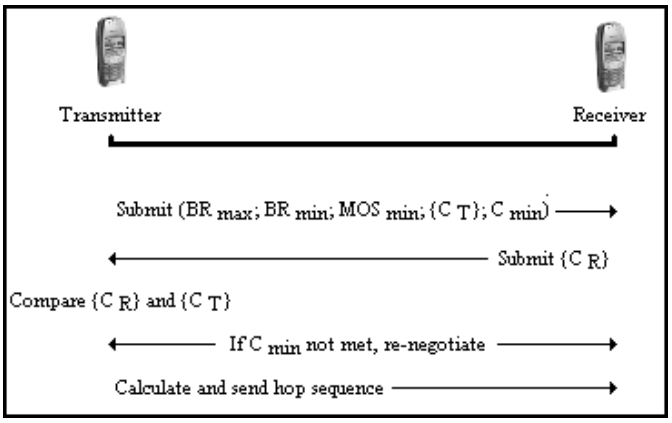

Figure 10.1: Rule Based codec-hopping initialisation phase

Step 1: $T \Rightarrow R$: Submit base requirements

$$(BR_{max}; BR_{min}; MOS_{min}; C_T; C_{min}) \tag{10.1}$$

where BR_{max} and BR_{min} indicate the maximum and minimum bit rate, MOS_{min} the minimum MOS value, C_T the set of available codecs that adheres to the bit rate and MOS requirements of T and C_{min} the minimum number of codecs to be used in the codec-hopping scheme.

Step 2: $R \Rightarrow T$: Submit the codec set

$$C_R \tag{10.2}$$

of available codecs that comply with $T's$ bit rate and MOS requirements.

Step 3: T compares C_T to C_R

$$C_T \cap C_R = C_{TR} \tag{10.3}$$

finding the intersection (C_{TR}), all the common elements from its two arguments. If the cardinality of this intersection is larger or equal to C_{min}, T may proceed in determining a pseudo-random codec hop sequence. If $|C_{TR}|$ is not sufficiently large then $T's$ initial base requirements may need adjustment (return to step 1).

Step 4: $T \Rightarrow R$: Communicate hop sequence securely.

The rule based setup would typically occur in the "ringing" period before voice communication is patched through.

It is important to note that encryption may be used in the secure communication of the hop sequence which unlike voice may not be affected by latency in a bandwidth constrained network. The power and bandwidth constraints limiting the use of encryption during real-time voice communications have less of an impact when used as part of (infrequent) initialisations.

In an insecure communications network where all messages sent over the communications channel can be intercepted by an adversary, two parties not sharing any secret information initially can generate a secure cipher key by each choosing a secret number, applying a one-way transformation to this number and exchanging the results of this transformation (the public keys) over the insecure channel [105]. We briefly discuss the workings of a non-interactive key exchange system.

10.9 Non-Interactive Key Exchange

If a users identity can be assumed to be publicly known, the public keys of an identity-based public-key cryptosystem need not be transmitted [104]. Thus, an identity-based system can be used in a completely non-interactive manner. By building in a trapdoor into the modular exponentiation one-way function this allows a trusted third party to set up a non-interactive public-key distribution system. Maurer et al. [104] proposes a scheme for non-interactive key exchange which differs from [76, 88] in that it does not depend on an additional random information either by the subscriber or the trusted authority.

10.9.1 A Non-Interactive Public Key Distribution System

In non-interactive key exchange, the public key consists entirely of public identifiable information. There are three distinct areas in a non-interactive public key distribution system, namely i) system setup ii) user registration and iii) user communication.

10.9.1.1 System Setup Phase

To setup the system a trusted authority chooses primes p_i such that the numbers $(p_i - 1)/2$ are odd and pairwise relatively prime [103]. The primes p_i are chosen small enough such that computing discrete logarithms modulo each prime is feasible [104]. The trusted authority then computes the product

$$m = p_1 \bullet p_2 \ldots p_r \tag{10.4}$$

of the selected primes, determines as element α of Z_m^* that is primitive in every prime field $GF(p_i)$ and publishes m and α as system parameters [104].

The trusted authority is only required for the initial system setup and for user registration, but does not play a role in the communication phase.

10.9.1.2 User Registration Phase

In joining the system, a user A presents identification information ID_A, together with appropriate proof of identity and receives the secret key S_A corresponding to ID_A. The secret key S_A is computed by the trusted authority as the discrete logarithm of ID_A^2 modulo m to the base α [104]:

$$S_A \equiv log_\alpha(ID_A^2)(\text{mod } m) \tag{10.5}$$

Due to the squaring of ID_A, S_A is guaranteed to exist [105].

10.9.1.3 User Communication Phase

In order for user A to send a message M securely to user B, user A establishes a mutual secure cipher key K_{AB}, which is shared with user B and computed as follows:

$$K_{AB} \equiv (ID_B)^{2s_A}(\text{mod } m) \equiv \alpha^{S_A S_B}(\text{mod } m) \tag{10.6}$$

Any standard conventional symmetric cryptosystem is used to encrypt the message M using the cipher key K_{AB} resulting in ciphertext C. User A then sends the cipher C together with identity ID_A to user B. User B proceeds to decrypt the cipher C by computing:

$$K_{BA} \equiv (ID_A)^{2s_B} \equiv \alpha^{S_B S_A} \equiv K_{AB}(\text{mod } m) \tag{10.7}$$

The cipher C is then decrypted with secret key K_{AB} resulting in the message M.

10.9.2 Using Non-Interactive Public Key Distribution System in GSM

Some may argue that GSM is an insecure communications network. This stems from some of the problems highlighted with GSM security in Section 2.4. Using non-interactive public key exchange distribution systems is a means to enhance security and protect the privacy of the communications channel, independently from the underlying network.

In a mobile communications networks an example of public identifiable information is the mobile number (MSISDN) and the equipment identifier (IMEI) of a particular subscriber. The mobile number is assigned to the subscriber by network operator and is easily distributable by subscribers within the public domain. Likewise, the IMEI is assigned by the handset manufacturer and is retrievable by the subscriber off most handset through the keypad interface.

This public information, used as identifiable information (ID), generates a mutual secure cipher key (K) between the transmitter and receiver. Adding another security layer on top of what GSM currently provides, messages are encrypted using a standard conventional symmetric cryptosystem.

10.10 Privacy Analysis

Although codec-hopping provides a privacy level sufficient for the communications channel in deterring eavesdroppers it still suffers from the fact that the underlying network controls the communications channel. Furthermore, such an implementation does not enforce the linking of the mobile equipment, the subscriber and the communication that is performed. Although authentication is not provided for, the channel privacy is enhanced.

The codec hop pattern is reliant on the extended codec set available to the transmitter and receiver. This in turn has a direct bearing on the repetition cycle, which must be kept to a low frequency. If the hope set is concealed, and the above is adhered to, then we can confidently state that privacy is enhanced.

An identity-based non-interactive public key distribution system is presented that is based on a trusted authority to compute the discrete logarithm of a given number modulo a publicly known composite identifier. While this is infeasible for an adversary not knowing the factorisation. Without interaction with a key distribution center or with the recipient of a given message a user can generate a mutual secure cipher key based solely on the recipients identity and his own secret key and send the message, encrypted with the generated cipher key using a conventional cipher (cryptosystem), over an insecure channel to the recipient.

Due to the lack of confidence in the strength of GSM's cryptographic algorithms, adding another security layer in the form of channel communication protection is what is required. Seeing GSM as an "insecure" network, non-interactive public key exchange is an ideal approach to creating this additional security layer without effecting the underlying network.

10.11 Conclusion

In this chapter we provided two novel solutions to voice channel privacy. The first solution used, in particular, is where bandwidth constraints are a limiting factor. After applying principles learned in frequency-hopping, we introduced the concept of codec-hopping. Codec-hopping is an elegant solution where encryption methods are simply "too expensive" to use in a bandwidth restricted network. We investigated how the codec-hopping sequence is determined and distributed in a manner which is known only to the transmitter and receiver. The second proposal is the use of a non-interactive public key exchange distribution system as an additional security

and privacy protection layer for a communications channel, given an insecure network. This means, a transmitter and receiver can non-interactively establish and update pairwise keys and cipher messages between themselves. Each solution has a specific application but does highlight the use of different methodologies in enhancing communication channel privacy.

Chapter 11

Location Privacy

11.1 Introduction

Location can be defined as the knowledge of the position of an object or an individual. Variations of location-based services offer subscribers the convenience of finding nearby restaurants using their mobile phone, or locating and tracking friends from social networks. In each instance, their precise location is identified and recorded.

Location privacy is a particular type of information privacy. It is defined as the ability to prevent other parties from learning one's current or past location [18]. Usually position is computed and maintained by an external source, such as the underlying network [110]. In a mobile communications network, this is necessary in order to route calls to and from subscribers within the network. Location is determined mathematically by calculating the distance using a time interval approach between an object and a fixed known location point or simply by the entry point of a subscriber to a network. The problem is clear: how is location privacy possible when location information is necessary in connecting communicating parties and while under the control of a service provider?

The custodian of private location information is obliged to protect the individual's personal information. However, if a decision is made by the network service provider to monetise their subscriber's location information, there is little option available for the individual subscriber to prevent such an action nor recoup any compensation for this privacy violation. The only available option for an individual whose privacy has been infringed upon is an attempt to pursue legal action against the perpetrator. In fact, in the generic case, where an individual's private information is divulged by a controlling third party, the individual currently has ***no*** means of reinstating their privacy and has few options for compensation in this regard. On the other hand, if reasonable recourse is an available option, some individuals may feel apathetic towards their private information and content with collecting some economic compensation. In most cases it is assumed that the

vast majority of individuals would opt for privacy assurance over the option of a privacy violation compensated with some economic gain. It is thus our intention to focus on preventing privacy loss and seeing any recourse value as a penalty incurred rather than a reward received.

Our purpose in this chapter is to define a privacy preserving location system which maintains equilibrium between the competing objectives (privacy prevention and profit generation) of the parties. We are concerned with the economic and contract aspects of this relationship, rather than about the technical aspects of location privacy. An equilibrium is expressed in the form of a prohibitive contract which both the subscriber and service provider are bound by and is of no benefit to anyone if violated.

A prohibitive contract describes the constraints necessary in order to prevent the interaction between parties achieving any of their competing objectives. In other words, a prohibitive contract prevents engagement between parties which may lead to a privacy violation. Should the prohibitive contract be compromised by one party, the other party is presented with a mechanism for calculating a suitable recourse value.

Our aim is to define a location privacy prohibitive contract which defines a suitable recourse mechanism, should a violation occur. Furthermore, the goal is to show an overall system outcome resulting from any violations of the prohibitive contracts (between individuals and the service provider) is a desirable one for *all* parties concerned. The objective is thus best represented in the notion of efficiency. Efficiency is an important criteria for evaluating systems and public policies. Efficiency, defines a location privacy system which leaves no one in the system economically strictly better off.

Utilitarianism is the idea that the moral worth of an action is solely determined by its contribution to overall utility, that is, its contribution to happiness or pleasure as summed among all users. Utility, the good to be maximised, has been defined by various thinkers whose classic proponents were Jeremy Bentham [17], John Stuart Mill [107], and Henry Sidgwick [144]. Together these claims imply that an act is morally right if and only if that act causes "the greatest happiness for the greatest number".

11.2 Background

Various approaches have been proposed in gathering user location information. They differ in measurement namely: accuracy, range, units, time and cost. Technologies include Global Positioning Systems (GPS), Radio-Frequency (RF) tags and various other wireless based methods. These systems provide location management operations but rely on privacy-enhancing technologies (PETs) in order to protect the unauthorised misuse of location information.

Bertino et al. [19] proposes privacy-preserving techniques for location-based services. This work was a prelude to a propose a framework for

preserving location privacy in moving-object environments [95]. Their approach is based on the idea of sending to the service provider suitably modified location information.

Some solutions and frameworks have been proposed for handling location privacy and some have investigated the ethical issues surrounding location-based tracking systems [155]. A vast majority are based on the existence of a Trusted Third Party (TTP). IETF Geopriv Workgroup [122] provides a framework for TTPs by introducing a Location Server (LS) to manage subject location. Due to the fact that LS is a centralised storage, user location information is prone to eavesdropping and attacks. Geopriv's goal is to allow the tracking of user location through location (data) objects while maintaining some user controls. Users define rules both on the location server and embedded in the location object which restrict how the data can be redistributed.

Marias et al. [102] propose a new technique in ensuring location privacy through secret sharing techniques where location information is seen as a secret divided into n pieces and all pieces are required to restore the original information. This proposed architecture enables privacy location without relying on the existence of a TTP. Instead it uses "Share the Secret" (STS) servers, which are untrusted entities, to distribute portions of anonymous location information, and authorises other entities to combine these portions and derive the location of a user.

Kesdogan et al. [87] propose the use of temporary pseudonymous identities to protect the identity of subscribers. However, anonymity and pseudonymity are not complete answers to privacy concerns because:

- Anonymity presents a barrier to authentication and personalisation, which are important for a range of applications [80].
- Pseudonymity and anonymity are vulnerable to data mining, since identity can often be inferred from location [18].

Duckham et al. [50] and Ardagna et al. [12] address the location privacy problem through a formal framework using obfuscation, obfuscation-based techniques and negotiation. Obfuscation concerns the practice of deliberately degrading the quality of information in some way, so as to protect the privacy of the individual to whom that information refers. It protects location privacy by artificially inserting into measurements some fake points with the same probability as the real user position. Such techniques may degrade system performance particularly in a network where latency affects the quality of communication. Others like [48, 145] simply take obfuscation a level further and suggest encryption and masking as means to ensuring location privacy.

Zhong et al. [159] introduce three protocols (named *Louis, Lester* and *Pierre*) for solving the nearby-friend problem (a variant of the location pri-

vacy problem). The *Louis* protocol requires a semi-trusted party which does not learn any location information. The Lester protocol does not need a third party, but has the drawback that a user might be able to learn a friends location even if the friend is in an area that is no longer considered nearby by the friend. The Pierre protocol does not have this disadvantage at the cost of not being able to tell the user the precise distance to a nearby friend. Although each of these protocols may have specific application in solving the nearby friend problem, there remains some pertinent privacy issues around friends knowing location information which may be disseminated without the consent of the individual.

Gedik et al. [64], describes a framework which enables each mobile client to specify the minimum level of anonymity it desires and the maximum temporal and spatial tolerances it is willing to accept when requesting for k-anonymity preserving location based services. A release provides k-anonymity protection if the information for each person contained in the release cannot be distinguished from at least k-1 individuals whose information also appears in the release [148].

In all the aforementioned location privacy approaches and frameworks (TTP, location information modification, secret sharing, temporary pseudonym, obfuscation), achieving location privacy has specific application and purpose. Their privacy-enhancing capability, effectiveness and practicality remains open for debate. Should a privacy location violation occur, none of the previously presented techniques allow for a suitable privacy conflict resolution and recourse for the individual should a privacy violation occur. Hence, our approach is to define a privacy preserving location system where equilibrium between the competing objectives (privacy prevention and profit generation) is the goal.

We describe, at the outset, the importance of game theory in understanding techniques available for finding an equilibrium in a system. This forms the basis when establishing a prohibitive contract.

11.2.1 Game Theory

Game Theory [60, 153] is concerned with analyzing the interactions of decision makers with conflicting objectives. Game theory thus studies the choice of optimal behaviour when costs and benefits of each option depend upon the choices of other individuals. In strategic games, individuals choose strategies which will maximise their return, given the strategies that other individuals choose. Although game theory has been the focus of attention in years gone by, there has been a renewed interest in the applications of its principles. One example of this is Mackey et al. [101] who applies game theory to understanding statistical disclosure of events.

Combinatorial game theory (CGT) is a mathematical theory that only studies two-player games which have a position which the players take turns

changing in defined ways or moves to achieve a defined winning condition. CGT does not study games of chance, but restricts itself to games whose position is public to both players, and in which the set of available moves is also public. Applying CGT to a position attempts to determine the optimum sequence of moves for both players until the game ends, and by doing so discover the optimum move in any position. In practice, this process is notoriously difficult unless the game is very simple. CGT should not be confused with game theory which is traditionally used in the theory of economic competition and cooperation; however similar operations and principles apply. CGT is not usually associated in establishing collaboration where private information is concerned, however, given the existence of conflicting objectives between decision makers it is conceivable that CGT is a perfect mechanism to determine the conditions which define a prohibitive contract.

11.2.2 Finding Equilibrium and determining Efficiency

The most important equilibrium concept in game theory is the concept of Nash Equilibrium [111]. A Nash Equilibrium is a strategy profile such that no user may gain by unilateral deviation. Thus Nash Equilibrium is a *stable operating point* as no user has incentive to change strategy. More formally, a Nash Equilibrium is set in game (S, f) where S is a set of strategy profiles and f is the set of payoff profiles. When each player $(i \in \{1, \ldots, n\})$ chooses strategy x_i resulting in a global combined strategy profile $x = (x_1, \ldots, x_n)$ the player i obtains payoff $f_i(x)$. Note the payoff depends on the strategy chosen by player i as well as those chosen by all the other players. A strategy profile is a Nash Equilibrium if no unilateral deviation in strategy by a single player is profitable. Thus a strategy profile $x^* \in S$ is a Nash Equilibrium if:

$$\forall i, x_i \in S_i, x_i \neq x_i^* : f_i(x_i^*, x_{-i}^*) \geq f_i(x_i, x_{-i}^*) \tag{11.1}$$

In other words, by changing strategy, the player will not benefit in any way. We do not use Nash Equilibrium directly but rather apply the principles in finding under what conditions a stable operating point can be found so as to maintain location privacy.

Finding equilibrium, where location privacy is concerned, is comparable to finding suitable constraints such that no party may gain by unilateral deviation. More formally, our goal is to find the constraints under which a stable operating point exists such that the conditions prohibit any party from becoming strictly better off. For our purpose, a privacy equilibrium is finding a balance in the following situation: private information is preserved by the presence of a suitable deterrent (monetary loss) should the custodian divulge the individual subscriber's information, causing a privacy violation. Collectively, such conditions affect the efficiency of the entire location system.

Recall that utilitarianism is often used to gauge levels of "happiness" amongst users, it is also used to represent the total benefit (in monetary terms) to all in a system. We choose utilitarianism as a means to present a numerical example depicting a practical world where apathetic users exist and privacy infringements do occur.

11.3 Finding a Location Privacy Equilibrium

Determining the intrinsic value of private information is a subjective process and evidently hard. This can be attributed to the fact that privacy and privacy violation is dependent on the individual, the degree of violation, time, circumstance and situation.

Private information has a perceived value proportional to the demand for it by others and the amount of anguish it causes the owner should privacy be infringed upon. Information which may be deemed private today may have "less" or even "more" of a privacy implication in the future. Take for example a mobile telephone number which over time, may form part of an individual's identity, used for social and business purposes or alternatively may be used briefly for a specific purpose and then be discarded by the individual. We see private information as information with some inherent value which is influenced by social, economic and environmental factors. This information has the distinct possibility of being relinquished to others without the owner's consent.

Laudon et al. [90] suggests one possibility of valuing private information is through the creation of a National Information Market (NIM). The concept of a NIM is best described as a place where information about individuals is bought and sold at a market clearing price freely arrived at, in which supply for this information is equaled by its demand. Similar to financial markets, an "Exchange" would bring together buyers and sellers of private information for the purpose of transacting at a market clearing price. NIM, in our case, is used as a hypothetical construct, used only as a mechanism to get an associated value. It may be argued that everyone possesses information about themselves that would be of some value under some circumstance, to others, for commercial purpose.

If there is a monetary gain through the sale of private information, the individual currently does not receive any compensation for this *loss*. In many cases, there is an imbalance in the tradeoff of a custodian protecting private information against the desire from benefits derived from relinquishing this information to others. Remember the premise in this chapter is that the individual's primary concern is privacy protection rather than the prospect of the individual deriving benefit from sold private location information.

11.3.1 Current Location Privacy Imbalance

Currently, divulgence of private location information is at the sole discretion of the service provider. We use the notation $(individual; service\ provider)$ to indicate the utility of each party. Traditionally in a mobile environment, the individual derives benefit from using the service provider's infrastructure (e.g. making a call). The service provider charges the individual and derives profit. In other words, the utility describes the benefit to each party given a set of circumstances. Generally, an individual is happy to engage in a service, provided the benefit gained is offset against the charges incurred.

If m_i represents the value (in monetary terms) of private information as perceived by i then the utility of the individual should private information be sold or divulged, for some benefit to the service provider, is shown as $-m_i$. Should the service provider SP divulge private location information, the utility for SP is a divulgence payoff, denoted by u.

Should a privacy violation occur, there are a number of legal options available to the individual should SP divulge private information; we briefly discuss two of these. The first is a state-pursued criminal case against SP on behalf of aggrieved individuals. The state prosecutes and fines SP if it is found guilty of a privacy violation. The second is a civil case brought against SP by the individual in order to pursue a degree of compensation for a privacy infringement.

We focus our attention on a civil case, and choose $P(sue)$ to denote the probability i successfully takes legal action against SP for a location privacy infringement. A recourse value, denoted by r, is awarded by the court to the plaintiff should there be sufficient evidence proving a privacy violation. r may include punitive damages, again awarded by the court, as further compensation for losses as a direct result of the privacy violation.

If the costs involved in the individual suing the service provider are greater than the potential recourse value r issued by the court, then the probability of i pursuing any legal action against the service provider diminishes to zero, thus $P(sue) \times r = 0$. In the case where private information is managed correctly, the utility of i and SP is represented as $(\Delta_i; \Delta_{SP})$. In other words, the SP does not gain unilaterally at the individuals expense and the individual does not loose.

If *no* civil case is opened by i against SP, the result is that SP simply gains the divulgence payoff u while i looses his perceived value, m_i. This scenario is indicative of a situation where costs incurred negate any legal option available to i. Thus, there is a clear affinity towards SP divulging i's location information, thus creating an imbalance, as shown in Equation 11.2.

$$(\Delta_i - m_i; \Delta_{SP} + u) \tag{11.2}$$

In summary, the individual wishes to enjoy a service while private loca-

tion information is protected. Should a privacy violation occur, determining and receiving any recourse is an arduous task and the individual has **no** guarantee of being successful. On the other hand, in knowing the service offering is not bound by any privacy contract, SP is confident that if $u > P(sue) \times r$ (the divulgence payoff exceeds the probability of being sued and being forced to pay an "admittance of guilty" fee) then the individual's private location information is "sold" in order to maximise profits.

11.3.2 Privacy, Efficiency and Recourse

A possible solution to solving the privacy imbalance is to create a prohibitive contract outlining the basis for privacy equilibrium including a privacy violation payoff. Recall, a prohibitive contract is seen as the constraints necessary in preventing the interaction between parties trying to achieve their competing objectives. Finding equilibrium is comparable to finding a stable operating point in which no player may gain by unilateral deviation and where the overall location privacy system is considered efficient. In establishing a prohibitive contract, we hope to achieve a desirable equilibrium where the individual maximises privacy confidence while the service provider provides a consistent and private service.

It is interesting to note that SP is subject to lose a degree of trust from i should a privacy infringement occur. However, trust is inconsequential in establishing a prohibitive contract as the strategy profiles are public and the payoff profiles known. Thus, in this case, trust does not form part of any utility.

Take the following scenario; a service provider divulges private location information (causing a privacy violation) where there is a prohibitive contract is in place. In this case, the individual's utility is made up of a privacy loss (expressed as the individual's associated perceived monetary value) and a recourse value gained $(r - m_i)$. The SP's utility is made up of a divulgence value gained and a recourse value lost $(u - r)$.

In the service offering is bound by a prohibitive contract and $r > u$ then there is a clear affinity towards the SP not revealing (selling) i's personal information. In other words, there is a clear affinity towards a stable operating point. Likewise, if $x_i > r$ it is highly unlikely that i will knowingly be enticed to relinquish private information in order to gain recourse value r.

It is clear that constraints are necessary in the establishment of a prohibitive contract. Indeed, if a prohibitive contract is in place, the utility shown for i and SP respectively should private information be divulged is:

$$(\Delta_i + r - m_i; \Delta_{SP} + u - r) \tag{11.3}$$

where m_i symbolises the value that i associates with its private information. m_i, r, and u are considered partial variables, meaning these variables are subjective and influenced by various factors. Finding values for these

partial variables, which tend towards a stable operating point, in many cases is only possible after a violation has occurred. However, the conditional constraints for i and SP in the establishment of a prohibitive contract are $r - m_i < 0$ and $u - r < 0$ respectively. If the prohibitive contract acts as a successful prediction then there exists a sufficient deterrent to act. This is possible if the penalties inflicted are equivalent to the compensation for the loss resulting from a privacy violation. In other words, we tend towards an ideal utility for i and SP, $(\Delta_i; \Delta_{SP})$.

In summary, the service provider is prohibited from divulging private location information while the individual is secure in the knowledge that there is a prohibitive contract safeguarding against the possibility of a privacy violation.

11.3.3 Defining a Privacy Location Prohibitive Contract

We define a prohibitive contract as a strategy profile such that each user is constrained to deviate unilaterally. Thus a prohibitive contract is a *stable operating point* as no user has incentive to change strategy as there is a significant deterrent to do so. More formally, a prohibitive contract is set of strategies with conflicting and competing objectives (S, f) where S is a set of strategy profiles and f is the set of payoff profiles. Strategies in this case are constrained by a recourse value $r^{'}$, where $r^{'}$ is a prediction of the recourse value.

Each player has only one strategy x_i resulting in a global combined strategy profile $x = (x_1, \ldots, x_n)$. In our location privacy example, i's strategy is to protect private information, while SP's strategy is to profit take from the sale of private location information. Thus a strategy profile $x^* \in S$ represents a **prohibitive contract** if:

$$\forall i, x_i \in S_i, x_i \neq x_i^* : f(x_i^*, r_i') \geq f(x_i, r_i') \tag{11.4}$$

By changing strategy, no player will benefit in any way. In other words, a prohibitive contract is used to dissolve conflicting strategies through recourse constraints. Should a player choose to engage (breach the prohibitive contract), how can the efficiency of the system be determined? Under what circumstance can a prediction of the value of $r^{'}$ ensure efficiency?

11.4 A Numerical Example

Our example investigates a communications network where a service provider is responsible for a number of users. In this approach, a service provider and user system interaction is itself modeled as a game. Recall that utilitarian theory is concerned with the greatest benefit to the greatest number. We use this approach to measure the cooperation and for evaluating our location privacy system for efficiency.

Apathetic users presents the service provider the opportunity to benefit directly. Taking this into consideration, an efficiency evaluation method can be used in simulating location privacy systems, given the utility of the service provider and utility of all its users. In other words, finding this balance is best described as finding the association between the divulgence and recourse values given different system scenarios. This utility function evaluates system cooperation in the sense that no player benefits at the other's expense and overall system outcome is considered efficient.

11.4.1 Evaluation

We assume the network service provider values all its users equally and all user's private location information is valued by a NIM. Furthermore, it is assumed that the vast majority of users seek privacy assurance while a small proportion are apathetic towards their private information.

In setting up our numerical example, we choose the most significant factors which may influence a location privacy system. We assign variables influencing our privacy location game as follows:

- u - Divulgence value
- $r^{'}$ - Recourse value
- a - Number of apathetic users where the service provider is likely to sell their information
- b - Number of privacy-seeking users where the service provider is likely to sell their information
- c - Percentage users don't claim the allocated recourse value
- d - Percentage privacy-seeking users defect due to service provider violation
- v - Value of single user to the service provider
- n - Number of users in the system
- α - efficiency value (ideal divulgence to recourse value)

The service provider bases the value of its operation on the number of users and the associated value of each user. The values of a, b, c and d may be determined using sample data from a subset of the population n. The system value is calculated as follows: $SystemValue = v \times n$. In establishing overall system efficiency, the costs incurred must equal incomes received for both the service provider and its users. For the service provider this is expressed using the following equation:

$$\begin{aligned} Income - Expenses &= 0 \\ ((u - r^{'})a) + (ar^{'}c) + ((u - r^{'})b) + (br^{'}c) - (bvd) &= 0 \\ ua - r^{'}a + ar^{'}c + ub - r^{'}b + br^{'}c - bvd &= 0 \end{aligned} \tag{11.5}$$

For the user this may be expressed as the satisfaction in the knowledge that the maximum possible recourse value (determined using utilitarian theory) is received should a privacy violation occur. In addition, it is generally accepted that the service provider does not benefit from infringing upon privacy.

Through elementary mathematical equation manipulation, the divulgence value for our numerical example is calculated as follows:

$$\begin{aligned} 0 &= ua - r^{'}a + ar^{'}c + ub - r^{'}b + br^{'}c - bvd \\ u(a+b) &= r^{'}a - ar^{'}c + r^{'}b - br^{'}c + bvd \\ &\dots \\ u &= r^{'}(1-c) + \frac{bvd}{a+b} \end{aligned} \tag{11.6}$$

We define an efficiency value for our system which is the relationship between the divulgence value and the recourse value. This is used in evaluating a location privacy system's efficiency to maintain balance. In our numerical example, the efficiency value showing the ideal divulgence to recourse ratio is shown below:

$$\alpha = (1-c) + \frac{bvd}{r^{'}(a+b)} \tag{11.7}$$

Both Equation 11.6 and Equation 11.7 directly corresponds to the manipulation of the Equation 11.5 ($Income - Expenses = 0$).

Now that we are able to calculated an efficiency value for our numerical example, let apply this to the following example. Suppose we have a communications environment where there are 1000 (n) users each with a associated value of 10 (v). Assume 10% of the users are apathetic towards their private information and 5% of users who are awarded a recourse value, do not claim the recourse value. Assume the likelihood the service provider is presented with an opportunity to sell private information is 50%. If a privacy-seeking user's information is sold, we assume that 50% of these users will defect to another service provider. This defection is based on insufficient recourse value or due to significant anguish caused by the service provider privacy violation, resulting in the service provider losing system value. We tabulate the values of the given variables and using Equation 11.7 we calculate the efficiency value such that the system best employs the theory of utilitarianism and the end result is an efficient system. From Table 11.1, assuming the recourse value ($r^{'}$) is set to 1, the efficiency value (α) calculated is 5.45.

α	a	b	c	d	v	n
5.45	50 (1000x10%x50%)	450 (1000x90%x50%)	5%	50%	10	1000

Table 11.1: Numerical Example - Calculating the efficiency value

If the service provider sells information, other than at a value of $u = 5.45r^{'}$, then we have a system imbalance which defies the principles of efficiency. Table 11.2 shows the summed payoff profiles for the service provider and users and the costs incurred by the service provider, given $u = 5.45r^{'}$.

	Apathetic	Privacy-Seeking	Total
User Claim	47.5	427.5	475
SP Claim	225	2025	2250
SP Cost of User Defecting	0	2250	2250

Table 11.2: Case Study - Income and Expenses

The figures show that the maximum possible recourse value is received by the privacy-seeking users offset against the apathetic users, should a privacy violation occur (in our example this occurs 50% of the time). In addition, the sum of the service provider utility and all its users utilities is zero.

11.5 Privacy Analysis

If we consider previous location privacy solutions, all exude preventative measured approaches in protecting private information. However, none consider the scenario where a violation does occur and for the consequences and consideration for recourse thereafter. A privacy preserving location system which maintains equilibrium between the competing objectives of the parties is defined by a prohibitive contract which binds both such that no benefit is gained to anyone if violated. In other words, this approach provides a built-in (possibly pre-determined) safety net governed by a utilitarianistic viewpoint. Privacy is enhanced due to the presence of a deterrent to engage in a privacy violation.

11.6 Conclusion

In this section we defined a privacy preserving location based system which maintains equilibrium between the competing objectives of the parties involved in a service-based environment. Through investigating the current location privacy imbalance, we were able to determine constraints necessary to find a suitable equilibrium. This was expressed in the form of a prohibitive contract which either the subscriber or service provider must not

violate. If the prohibitive contract, is compromised by one party, the other party is immediately presented with a recourse option.

With a prohibitive contract in place, it is evident that no player should ever move. We investigate a possible scenario where the allure of perceived benefit causes a system imbalance. In our example, we model adversaries using numerical data. We adopted the utilitarian paradigm, which provides a means of finding overall system efficiency, where the sum of all utilities is zero. An efficiency function finds the ideal divulgence to recourse ratio for the evaluation of the location privacy system for efficiency.

Chapter 12

Privacy Assurance in Next Generation Private Voice Communications Networks

12.1 Introduction

A Next Generation Network (NGN) is a packet-based network that is able to provide inter alia Telecommunications Services. It is also able to make use of multiple broadband, QoS-enabled transport technologies in which service-related functions are independent from underlying transport-related technologies. It offers users unrestricted access to different service providers and supports generalised mobility that will allow consistent and ubiquitous provision of data and voice services to users. NGNs, however, still face privacy threats similar to that of GSM.

12.2 Privacy Assurance

The original aim of this study was to try and enforce privacy with the aid of technology and to identify novel techniques for privacy assurance. We defined a set of formal mobile voice communications privacy requirements (refer to Section 4.6) as a prelude to ascertaining a set of principles directed specifically at ensuring a private Next Generation Network.

In previous chapters we identified mobile communications privacy controls that enable privacy assurance in current mobile communications networks through the following:

- Privacy by Trust Allocation (Chapter 5) - privacy assurance through the allocation of information to a trusted third party (TTP).
- Privacy by Virtual Assignment (Chapter 6) - privacy assurance through the assignment of virtual identities and identification schemes.

- Privacy by Access Control Segmentation (Chapter 7) - privacy assurance through the segmentation of network information and redefinition of access control.
- Privacy by Domain Extension (Chapter 8) - privacy assurance through controlled extensions in a foreign domain.
- Privacy by Sequential Information Release (Chapter 9) - privacy assurance through controlled forensic ability to gather information sequentially (based on an hypothesis).
- Privacy by Channel Concealment (Chapter 10) - privacy assurance through continual change to or non-interaction with communication medium channels.
- Privacy by Prohibition via Recourse (Chapter 11) - privacy assurance through suitable recourse governed by a prohibitive contract.

This privacy abstraction provides a base set of privacy assurance principles which may be practical and functional in NGNs. What is evident is the emergence of some distinct privacy control mechanisms that constitute a guided and systematic approach to achieving privacy assurance. In many literary works, this referred to as patterns.

12.3 Patterns for Privacy Assurance in NGNs

In computer science in general, there is a strong tendency towards developing standard methodologies for solving certain problems. These are commonly referred to as patterns. A pattern is thus a generic solution to a repeating problem. It is often written using the form: Context. Problem. Solution.

Yoder et al. [158] introduce patterns to the field of information security. However, while they are vital for ensuring the confidentiality, integrity and availability of computing systems, security patterns do not particularly (or necessarily) address the growing privacy issues of individuals.

In a Software Engineering environment, a proposed pattern is only a pattern if it is in use on at least three occasions (rule of three set by Schumacher et al. [141]). Protection against cookies [140] describes different methods for controlling the way in which your web browser manages cookies (e.g. blocking all cookies or only accepting individual cookies). Design patterns are typically used in programming as they allow programmers to structure and reuse code effectively. This generally leads to faster development times and, after a number of iterations, an ultimately higher-quality code.

As our proposed pattern does not yet adhere to the rule of three proposed by Schumacher and others, we refer to it as a "patlet". A patlet is defined as a draft proposal for a pattern and describes the tendency towards a desired result.

These patterns describe how users can protect their privacy by both revealing less about themselves and acquiring more information from the party who is providing the communications medium.

We define the following privacy assurance patlet.

NAME
Should be descriptive of either the technique or methodology used in the solution proposed by the privacy assurance pattern.

CONCISE INTENT DESCRIPTION
A thumbnail or condensed description regarding the intent of the pattern. State which privacy assurance scenario the pattern intends to address.

CONTEXT
The general scenario for use of the privacy assurance pattern. It is imperative that prime usage requirements and critical pitfalls be stated. Lastly, state all requirements and assumptions made in the application/creation of this privacy assurance pattern.

PROBLEM
The problem statement is the core of the privacy assurance pattern, the raison d'être for the privacy assurance pattern itself. Stakeholders and their demands are the driving forces of the solution. Add problems that compound the problem set to be solved by the privacy assurance pattern.

SOLUTION
The solution to the privacy problem at hand, as stated in the Problem section. Include balancing/addressing aforementioned driving forces. Illuminate dealing with pitfalls as mentioned in CONTEXT.

PRIVACY ASSURANCE DIRECTION
Explain in detail how the pattern is applied in practice in order to achieve privacy enhancement. Optionally add known instances of use and their outcomes as references here.

CONSEQUENCES
Discuss benefits vs. drawbacks. Emphasise known shortcomings of the solution. Optionally mention the resolution of possible pitfalls in the application of the pattern.

RELATED PATTERNS
List and discuss related patterns providing a foundation for the proposed privacy pattern.

NGN describes the key architectural evolution in telecommunications, driven by digitisation, packetisation, high-speed transfer and Internet Protocol (IP)-related technology solutions. The telecommunications industry has loosely adopted terminology for this evolution. The first was the move from analogue (1G) to digital (2G) transmission. A 2.5G network - then became known as a mid generation network which mainly introduced improved bandwidth technology in addition to the existing 2G generation. This was followed by multi-media support, spread spectrum transmission (3G) and now 4G, which refers to all IP packet-switched networks, mobile ultra-broadband (gigabit speed) access and multi-carrier transmission. 5G is the dream of having a "REAL" wireless world, an intelligent interconnected network serving the entire world without limits.

Given the above patlet is a draft proposal for privacy assurance in NGN, if we are to assume, there is a progression towards future generation networks, a privacy preserving pattern emerges (having at least three occasions - rule of three). Given this situation, all the mobile voice communications privacy concerns raised in this thesis will undoubtedly persist in NGNs.

12.4 Current and Future Work

In this thesis, I recognised that privacy is not an absolute notion, but rather a highly fluid concept about controlling the dissemination and use of one's personal information. Privacy protection is indeed measured by assessing the appropriate physical, technical and procedural safeguards that are in place to protect the security and integrity of information.

I began by asking the question: Why Privacy is Important? Although it was concluded that it is not possible to clearly define, categorise or measure privacy, one thing is certain - there is a duty to safeguard information so as to quell all fears an individual may have regarding the anguish that the violation of this information may cause. I continue to conduct research and investigate technological solution in preserving privacy where infringements may occur.

The Global System for Mobile Communications (GSM) is a commonly used telecommunications standard. In this thesis, GSM was used as a basis for my evaluation of and recommendations for privacy principles in Next Generation Networks (NGNs). This choice was made partly due to GSMs wide spread use and popularity as well as my fascination with mobile telecommunications and privacy.

The GSM network was segmented into the following areas for privacy consideration:

- Sender and Receiver Privacy
- Numbering Scheme Privacy
- Billing Privacy
- Roaming Privacy
- Legal Privacy
- Communication Channel Privacy
- Location Privacy

which formed the basis of a Private Mobile Voice Communications Architecture, used to constitute a basis for evaluation and recommendations for privacy principles in Next Generation Networks (NGNs). From these areas of privacy concern I adopted a few common privacy enhancing techniques namely anonymity, pseudonymity, unobservability and unlinkability and formulated formal privacy requirement definitions.

In addition, each privacy concern reported on in this thesis formed part of a sub project where the research, reported work and findings were individually submitted to either a relevant journal or conference. Most of the accepted work has been grouped and or inserted verbatim into this thesis and is summarised below:

- Sender and Receiver Privacy - "Using a Trusted Third Party Proxy in achieving GSM Anonymity" [37].
- Numbering Scheme Privacy - appears throughout my work.
- Billing Privacy - "Using compatible keys in achieving subscriber privacy channelling for billing in GSM Networks" [41].
- Roaming Privacy - "On preserving Network and Subscriber Privacy in GSM Roaming" [115].
- Legal Privacy - "Sequenced release of privacy-accurate information in a forensic investigation" [45].
- Communication Channel Privacy - "Codec-Hopping: Secure and Private Voice Communication in Bandwidth Constrained Networks" [39].
- Location Privacy - "Location Privacy: Privacy, Efficiency and Recourse through a Prohibitive Contract" [116].

Some topics unrelated to the specifics of this thesis were also covered in the fields of security and privacy in Short Message Service (SMS) and Voice over Internet Protocol (VoIP), namely: "Using an approximated one-time pad for securing Short Message Service (SMS)" [40], "A Silent SMS DoS Attack" [44], "A Model for SPAM Prevention in IP Telephone Networks using Anonymous Verifying Authorities" [38].

Future work includes investigating privacy concerns as future generation networks emerge. I hope to devise a formal mobile voice communications network pattern for privacy assurance.

12.5 Conclusion

The aim of privacy assurance was achieved primarily through technical intervention and by applying privacy-preserving principles to each identified area of privacy concern. In following a rigid methodology of evaluation, assessment and technical solution-building composites, I was able to converge towards a mobile communications network with an acceptable privacy-preserving level.

Chapter 5 through to Chapter 11 focused specifically on the individually identified areas of privacy concern within the Private Mobile Voice Communications Architecture. The idea was to return to Chapter 4, and in this chapter ascertain whether privacy principles learnt in subsequent chapters apply to NGN and in the process identify any existential similarities.

The ultimate goal of this thesis was to find ways in which to protect privacy in a mobile voice communications environment, from a technological perspective and in a proactive manner. Using the Global System for Mobile

communications (GSM) as reference, I identified areas of privacy concern and introduced some practical and theoretical mechanisms for privacy assurance. The rationalisation was that if privacy principles were identified (in existing networks) and adhered to (in next generation networks), then we ultimately converge towards a network infrastructure that possesses a desirable level of privacy protection.

In this chapter we define privacy controls enabling privacy assurance in current mobile communications networks. In finding a definitive set of privacy principles, the possibility of exploring patterns emerges as a means to developing standard methodologies for solving privacy concerns in NGNs. I communicate a patlet as a draft proposal for a privacy pattern recognition. This patlet is inclusive of our privacy assurance recommendations. This ultimately fulfils my objective of a comprehensive analytical view of NGNs, specifically where privacy is concerned. Finally I review my current and future work objectives.

Appendix - Acronyms

3GPP 3rd Generation Partnership Project.

AuC Authentication Centre.

BCCH Broadcast Control Channel.

BE Billing Engine.

BSS Base Station Subsystem.

BTS Base Transceiver Station.

CDR Call Data Record.

CLI Caller Line Identity.

CCITT Comité Consultatif International Téléphonique et Télégraphique.

DTMF Dual-Tone Multi Frequency.

ECPA Electronic Communications Privacy Act (ECPA) of 1986 (United States).

ECT Electronic Communications and Transactions Act No. 25 of 2002 (South Africa).

EIR Equipment Identity Register.

EPAL Enterprise Privacy Authorisation Language.

ETSI European Telecommunications Standards Institute.

EU European Union.

FWD Free World Dialup.

GSM Global System for Mobile Communications.

HLR Home Location Register.

IMEI International Mobile Equipment Identity.

IMSI International Mobile Subscriber Identity.

LA Location Area.

LAI Location Area Identifier.

MS Mobile Station.

MSC Mobile Switching Center.

MSISDN Mobile Subscriber ISDN Number.

NGN Next Generation Network.

OSS Operation Subsystem.

OTA Over The Air.

P3P Platform for Privacy Preferences.

PET Privacy-Enhancing Technology.

PKI Public Key Infrastructure.

PSTN Public Switched Telephone Network.

RR Radio Resource.

SIM Subscriber Identity Module.

SMS Short Message Service.

SS7 ITU-T Signalling System Number 7.

TAP Transferred Account Procedure.

ITU-T Telecommunication Standardization Sector.

TTP Trusted Third Party.

UML Unified Modelling Language.

VLR Visitor Location Register.

VoIP Voice over IP.

Appendix - Definitions

Anonymity Anonymity is the state of not being identifiable within a set of subjects, the so-called *anonymity set*.

Pseudonymity A pseudonym usually refers to an artificial or fictitious name, also known as an alias, used by an individual as an alternative to their true identity in order to hide some part of their identity.

Unlinkability Unlinkability is described as two or more items that are no more and no less related than they are related concerning a prior knowledge.

Unobservability Unobservability is the state of items of interest being indistinguishable from any items of interest at all.

Bibliography

[1] 3rd Generation Partnership Project. 3GPP. Web Reference: http://www.3gpp.org. Accessed May 2010.

[2] 3rd Generation Partnership Project. *3GPP TS 23.040, Technical realisation of the Short Message Service (SMS)*, 1999.

[3] 3rd Generation Partnership Project. *3GPP TS 03.48 V8.9.0; Technical Specification Group Terminals; Security mechanisms for the SIM application toolkit*, June 2005.

[4] M. Abe and E. Fujisaki. How to date blind signatures. In *ASIACRYPT '96: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, pages 244–251, London, UK, 1996. Springer-Verlag.

[5] Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948. Universal Declaration of Human Rights. Web Reference: http://www.un.org/en/documents/udhr/index.shtml. Accessed May 2010.

[6] A. Agarwal, V. Shrimali, and M. Lal Das. GSM Security Using Identity-based Cryptography. *Computing Research Repository (CoRR)*, abs/0911.0727, 2009.

[7] G. Aggarwal, T. Feder, K. Kenthapadi, S. Khuller, R. Panigrahy, D. Thomas, and A. Zhu. Achieving anonymity via clustering. In *Proceedings of the twenty-fifth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, PODS '06, pages 153–162, New York, NY, USA, 2006. ACM.

[8] J. Agre, A. Akinyemi, L. Ji, R. Masuoka, and P. Thakkar. A layered architecture for location-based services in wireless ad hoc networks. *Aerospace Conference Proceedings. IEEEAC*, 3:1085–1097, 2002.

[9] P.E. Agre and M. Rotenberg, editors. *Technology and privacy: the new landscape*. MIT Press, Cambridge, MA, USA, 1997.

[10] R. Anderson. A5 - The GSM Encryption Algorithm. http://www.chem.leeds.ac.uk/ICAMS/people/jon/a5.html, June 1994. Accessed October 2006.

[11] T. Anderson and C. DeWolfe. MySpace. Web Reference: www.myspace.com. Accessed May 2010.

[12] C.A Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samariti. Location Privacy Protection through Obfuscation-based Techniques. In *ISSA*, 2007.

[13] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter. Enterprize privacy authorisation langugae (epal 1.2). W3C Member Submission, November 2003.

[14] N. Asokan. *Security Issues in Mobile Computing*. Technical Report. Department of Computer Science, University of Waterloo, April 1995.

[15] L. Austin. Privacy and the question of technology. *Law and Philosophy*, 22(3):119–166, March 2003.

[16] J. Bellamy. *Digital Telephony (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience; 3 edition, 2000.

[17] J Bentham. *An Introduction to the Principles of Morals and Legislation*. Garden City: Doubleday, 1961. Originally published in 1789.

[18] A.R. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2:46–55, Jan-Mar 2003.

[19] E. Bertino. Privacy-preserving techniques for location-based services. *SIGSPATIAL Special*, 1:2–3, July 2009.

[20] G.R. Blakely. Safeguarding cryptographic keys. In *National Computer Conference*. American Federation of Information Processing Societies Proceedings, 1979.

[21] M. Blum, A. de Santis, S. Micali, and G. Persiano. Non-interactive zero-knowledge. *SIAM Journal of Computing*, 20(6):1084–1118, December 1991.

[22] A. Bonin, M. Bonin, R. Iles, and G. Kajmowicz. The Marathon Project - Extensible VoIP with Dynamic Compression. Web Reference: http://andre.bonin.ca/Projects.htm, April 2003. Google Cache, September 2004.

[23] M. Briceno, I. Goldberg, and D. Wagner. An Implementation of the GSM A3A8 Algorithm. Web Reference: http://www.gsm-security.net/papers/a3a8.shtml. Accessed October 2006.

[24] M. Burmester, Y. Desmedt, R. Wright, and A. Yasinsac. Security or Privacy, Must We Choose? Department of Computer Science, Florida State University: Proposition Paper, 2002.

[25] J. Byun, A. Kamra, E. Bertino, and N. Li. Efficient k-anonymization using clustering techniques. In *Proceedings of the 12th international conference on Database systems for advanced applications*, DASFAA'07, pages 188–200, Berlin, Heidelberg, 2007. Springer-Verlag.

[26] R. Cáceres, L. Cox, H. Lim, A. Shakimov, and A. Varshavsky. Virtual individual servers as privacy-preserving proxies for mobile devices. In *MobiHeld '09: Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 37–42, New York, NY, USA, 2009. ACM.

[27] E. Casey. Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, 1(2), 2002.

[28] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981.

[29] D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology - Crypto82*, pages 199–203, Berlin, 1983. Springer-Verlag.

[30] D. Chaum. Demonstrating that a public predicate can be satisfied without revealing any information about how. In A. M. Odlyzko, editor, *Advances in Cryptology — Crypto '86*, volume 263, pages 195–199, Berlin, 1987. Springer-Verlag.

[31] S. Cimato, P. D'Arco, and I. Visconti. Anonymous group communication in mobile networks. In *ICTCS*, pages 316–328, 2003.

[32] R. Clarke. Introduction to dataveillance and information privacy, and definitions of terms. Web Reference: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, 1999. Accessed October 2006.

[33] Comité Consultatif International Téléphonique et Télégraphique (CCITT) Recommendation G.726. General Aspects of Digital

Transmission Systems, Terminal Equipement - 40, 32, 24, 16 kbit/s Adaptove Differential Pulse code Modulation (ADPCM), 1990.

[34] Constitution of the Republic of South Africa Act 108 of 1996. South africa. Web Reference: http://www.info.gov.za/documents/constitution/index.htm. Accessed April 2007.

[35] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The platform for privacy preferences 1.0 (p3p1.0) specification. World Wide Web Consortium Recommendation, April 2002. http://www.w3.org/TR/P3P/, Accessed April 2010.

[36] N.J. Croft. Secure Interoperations of Wireless Technologies. Masters dissertation, University of Pretoria, School of Computer Science, October 2003.

[37] N.J. Croft and M.S. Olivier. Using a Trusted Third Party Proxy in achieving GSM Anonymity. In *South African Telecommunication Network and Applications Conference (SATNAC)*, Stellenbosch, South Africa, September 2004.

[38] N.J. Croft and M.S. Olivier. A Model for SPAM Prevention in IP Telephone Networks using Anonymous Verifying Authorities. In *Fifth South African Security Conference (ISSA)*, Midrand, South Africa, July 2005.

[39] N.J. Croft and M.S. Olivier. Codec-Hopping: Secure and Private Voice Communication in Bandwidth Constrained Networks. In *SecPerU, Workshop on Security an Privacy in Pervasive Ubiquitous Computing*, Santorini, Greece, April 2005.

[40] N.J. Croft and M.S. Olivier. Using an approximated one-time pad for securing Short Message Service (SMS). In *South African Telecommunication Network and Applications Conference (SATNAC)*, Drakensburg, South Africa, September 2005.

[41] N.J. Croft and M.S. Olivier. Using compatible keys in achieving subscriber privacy channelling for billing in GSM Networks. In *International Network Conference (INC)*, Samos, Greece, 2005.

[42] N.J. Croft and M.S. Olivier. Anonymous Mobile Conference Calls. In *South African Telecommunication Network and Applications Conference (SATNAC)*, Stellenbosch, South Africa, September 2006.

[43] N.J. Croft and M.S. Olivier. Sequenced Release of Privacy Accurate Call Data Record Information in a GSM Forensic Investigation. In

Sixth South African Security Conference (ISSA), Sandton, South Africa, July 2006.

[44] N.J. Croft and M.S. Olivier. A Silent SMS DoS Attack. In *South African Telecommunication Network and Applications Conference (SATNAC)*, Maritius, September 2007.

[45] N.J. Croft and M.S. Olivier. Sequenced release of privacy-accurate information in a forensic investigation. *Digital Investigation*, 2010.

[46] D.E. Culler and W. Hong. Wireless sensor networks: Introduction. *Communications of the ACM*, 47(6):30–33, 2004.

[47] G. Danezis, S. Lewis, and R. Anderson. How much is location privacy worth? In *Online Proceedings of the Workshop on the Economics of Information Security Series (WEIS 2005*, 2005.

[48] J. Domingo-Ferrer. Microaggregation for database and location privacy. *Lecture Notes in Computer Science (LNCS) Next Generation Information Technologies and Systems-NGITS'2006*, 4032:106–116, July 2006.

[49] J. Domingo-Ferrer and J. M. Mateo-Sanz. Practical data-oriented microaggregation for statistical disclosure control. *IEEE Trans. on Knowl. and Data Eng.*, 14:189–201, January 2002.

[50] Matt Duckham and Lars Kulik. A formal model of obfuscation and negotiation for location privacy. In Lecture Notes in Computer Science (LNCS), editor, *In Pervasive*, volume 3468, pages 152–170, 2005.

[51] J. Eberspacher, H. Vogel, and C. Bettstetter. *GSM Swithing, Services and Protocols*. Wiley, Second edition, 2001.

[52] Electronic Communications and Transactions Act 25 of 2002. South Africa.

[53] Electronic Communications Privacy Act of 1986 (ECPA) (P. L. 99-508, 100 Stat.1848). United States.

[54] EU Directive on Data Protection Act of 1997. *Directive 97/66/EC of the European Parliament and of the Council*.

[55] European Telecommunications Standard Institute (ETSI). *Recommendation GSM 02.09; Security related network functions*, June 1993. Technical Report.

[56] European Telecommunications Standards Institute (ETSI). *GSM Recommendation 06.10 European digital cellular telecommunications system (Phase 2); Full rate speech transcoding*, September 1994.

[57] European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France. *European Digital Cellular Telecommunications System (Phase 2+): Specification of the SIM application toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) Interface (GSM 11.14)*, 1998.

[58] European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France. *European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11)*, 1998.

[59] F. Fitzek, G. Schulte, and M. Reisslein. System Architecture for Billing of MultiPlayer Games in a Wireless Environment using GSM/UMTS and WLAN Services. *NetGames2002, ACM*, pages 58–64, April 2002.

[60] D. Fudenburg and J. Tirole. *Game Theory.* MIT Press, Cambridge, 1991.

[61] E. Gabber, P.B. Gibbons, D.M. Kristol, Y. Matias, and A. Mayer. Consistent, yet anonymous, web access with LPWA. *Communications of the ACM*, 42(2):42–47, February 1999.

[62] E. Gabber, P.B. Gibbons, D.M. Kristol, Y. Matias, and A. Mayer. On secure and Pseudonymous Client-Relationships with Multiple Servers. *ACM Transactions on Information and System Security*, 2(3):390–415, November 1999.

[63] V.K. Garg. *Principles and applications of GSM.* Prentice Hall PTR, 1999.

[64] B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7:1–18, January 2008.

[65] P. Ginzboorg. Seven Comments on Charging and Billing. *Communications of ACM*, 43(11):89–92, November 2000.

[66] I. Goldberg. Privacy-Enhancing Technologies for the Internet, II: Five Years Later. In *Lecture Notes in Computer Science (LNCS) Privacy Enhancing Technologies*, volume 2482/2003, pages 1–12. Springer Berlin / Heidelberg, August 2003.

[67] I. Goldberg and M. Briceno. GSM Cloning. Web Reference: http://www.echelon.cx/howitworks.html, http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html. Accessed November 2006.

[68] I. Goldberg, D. Wagner, and E.A. Brewer. Privacy-enhancing technologies for the Internet. *IEEE COMPCON '97*, pages 103–109, February 1997.

[69] D. Goldschlag, M. Reed, and P. Syverson. Hiding routing information. In *Workshop on Information Hiding*, Cambridge, UK, May 1996.

[70] D. Goldschlag, M. Reed, and P. Syverson. Onion routing for anonymous and private internet connections. *Communications of the ACM*, 42(2):39–41, 1999.

[71] S. Goldwasswer, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18:186–208, February 1989.

[72] GSM Association. homepage. Web Reference: http://www.gsmworld.com. Accessed May 2010.

[73] GSM Association. Tapping the Potential of Roaming. Web Reference: http://gsmworld.com/technology/roaming/billing-standards/index.htm. Accessed May 2010.

[74] GSM Recommendation 09.02. Mobile Application Part (MAP) Specification. European Telecommunications Standards Institute (ETSI), 1999.

[75] C. Gulcu and G. Tsudik. Mixing email with babel. In *Symposium on Network and Distributed System Security*, San Diego, February 1996.

[76] C. Günther. An identity-based key-exchange protocol. In *EUROCRYPT '89: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 29–37, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[77] J.C. Haartsen, Ericsson Radio, and Systems B. V. The Bluetooth radio system. *IEEE Personal Communications*, 7:28–36, 2000.

[78] R. Hes and J.J. Borking. Privacy enhancing technologies: The path to anonymity. Technical Report A&V 11, Registratiekamer, The Hague, 1998.

[79] Reid Hoffman. LinkedIn. Web Reference: www.linkedin.com. Accessed May 2010.

[80] J.I. Hong and J.A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *2nd International Conference on Mobile Systems, Applications, and Services*, pages 177–189. ACM Press, 2004.

[81] IEEE. ISO/IEC 8802-11, ANSI /IEEE std 802.11. Isbn 0-7381-1658-0, Institute of Electrical and Electronics Engineers, Inc., August 1999.

[82] ISO Standard OSI 9074. *Estelle: A Formal Description Technique Based on an Extended State Transition Model*, 1989.

[83] ISO99 ISO IS 15408. 1999. Web Reference: http://www.commoncriteria.org. Accessed October 2006.

[84] ITU_T Recommendation G.711. Pulse Code Modulation (PCM) of voice frequencies, Geneva, 1972.

[85] ITU_T Recommendation P.800. Methods for subjective determination of transmission quality. Technical report, European Telecommunications Standards Institute (ETSI), 1996.

[86] N.S. Jayant and P. Noll. *Digital Coding of Waveforms: Principles and Applications to Speech and Video*. Prentice Hall Professional Technical Reference, 1990.

[87] D. Kesdogan, P. Reichl, and K. Junghärtchen. Distributed temporary pseudonyms: A new approach for protecting location information in mobile communication networks. In *Fifth European Symposium on Research in Computer Security*, volume 1485, pages 295–312, Louvain-la-Neuve, Belgium, 16–18 1998. Springer-Verlag.

[88] K. Koyama and K. Ohta. Identity-based conference key distribution systems. In *CRYPTO '87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, pages 175–184, London, UK, 1988. Springer-Verlag.

[89] H. Krasnova, T. Hildebrand, and O. Guenther. Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis. In *ICIS 2009 Proceedings*, 2009.

[90] K.C. Laudon. Markets and Privacy. *Communications of the ACM*, 39(9):92–104, September 1996.

[91] C.H Lee, X. Deng, and H. Zhu. Design and security analysis of anonymous group identification protocols. *Public Key Cryptography*, 2274:188–198, 2002.

[92] C.H. Lee, M.S. Hwang, and W.P. Yang. Extension of authentication protocol for GSM. In *IEEE Proceedings-Communications*, volume 150, pages 91–95, April 2003.

[93] M. Leppanen. Voice over IP. Technical report, Department of Computer Science, Helsinki University of Technology, 2001.

[94] T. Lester. The reinvention of privacy. Web Reference: The Atlantic online. http://www.theatlantic.com/issues/2001/03/lester-pt.htm, September 2001. Accessed October 2006.

[95] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar. Location privacy in moving-object environments. *Trans. Data Privacy*, 2:21–46, April 2009.

[96] W.D. Lin and J.K. Jan. A Wireless-based Authentication and Anonymous Channels for Large Scale Area. In *ISCC '01: Proceedings of the Sixth IEEE Symposium on Computers and Communications*, page 36, Washington, DC, USA, 2001. IEEE Computer Society.

[97] Y.B. Lin. Signaling System Number 7. *IEEE Potentials*, pages 5–8, August 1996.

[98] L. Little, P. Briggs, and L. Coventry. Public space systems: designing for privacy? *International Journal of Human-Computer Studies*, 63(1-2):254–268, 2005.

[99] LOTOS. A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour. ISO Standard OSI 8807, 1989.

[100] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *SAC '99: Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography*, pages 184–199, London, UK, 2000. Springer-Verlag.

[101] E. Mackey. An application of game theory to understanding statistical disclosure events. Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality, December 2009.

[102] G.F. Marias, C. Delakouridis, L. Kazatzopoulos, and P. Georgiadis. Location Privacy Through Secret Sharing Techniques. In *WoWMoM '05: Proceedings of the 6th IEEE International Symposium on a World of WirelessMobile and Multimedia Networks*. IEEE Computer Society, 2005.

[103] U.M. Maurer. Fast generation of secure rsa-moduli with almost maximal diversity. In *EUROCRYPT '89: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 636–647, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[104] U.M. Maurer and Y. Yacobi. Non-interactive public-key cryptography. In *Advances in Cryptology — EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science (LNCS)*, pages 498–507. Springer-Verlag, April 1991.

[105] U.M. Maurer and Y. Yacobi. A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, 9(3):305–316, 1996.

[106] A. Menezes. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

[107] J.S. Mill. *Utilitarianism, edited with an introduction by Roger Crisp*. New York: Oxford University Press, 1998. Originally published in 1861.

[108] R.P. Minch. Privacy issues in location-aware mobile devices. In *37th Hawii International Conference on System Sciences*, volume 5, 2004.

[109] R. Molva, D. Samfat, and N. Asokan. Untraceability in mobile networks. In *International Conference on Mobile Computing and Networking*, pages 26–36, Berkeley, California, United States, 1995. Communications of the ACM.

[110] M. Mouly and M.B. Pautet. *The GSM System for Mobile Communications*. Telecom Publishing, 1992.

[111] J. Nash. Non-cooperative games. *The Annals of Mathematics, Second Series*, 54(2):286–295, September 1951.

[112] National Institute of Standards and Technology, NIST FIPS PUB 180-1. The Secure Hash Algorithm (SHA-1). Technical report, U.S. Department of Commerce, April 1995.

[113] D. Nguyen and K. Truong. PHEmail: designing a privacy honoring email system. In *CHI '03: CHI '03 extended abstracts on Human factors in computing systems*, pages 922–923, New York, NY, USA, 2003. ACM Press.

[114] I. Niven and H.S. Zuckerman. *An Introduction to the Theory of Numbers*. John Wiley and Sons, New York, 1960.

[115] N.J. Croft and M.S. Olivier. On preserving Network and Subscriber Privacy in GSM Roaming. Department of Computer Science, University of Pretoria: Proposition Paper, September 2006.

[116] N.J. Croft and M.S. Olivier. Location Privacy: Privacy, Efficiency and Recourse through a Prohibitive Contract. Transactions in Data Privacy: Submitted, March 2010.

[117] Object Management Group. Unified Modelling Language Specification, ISO/IEC 19501:2005(E), Version 1.4.2. Technical report, OMG, 2005.

[118] M.S. Olivier. A Layered Architecture for Privacy-Enhancing Technologies. In *Third Annual Information Security South Africa Conference (ISSA)*, Sandton, South Africa, July 2003.

[119] D.M. Pedersen. Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19:397–405, 1999.

[120] A. Peinado. Privacy and authentication protocol providing anonymous channels in GSM. *Computer Communications*, 27(17):1709–1715, May 2004.

[121] L. Pesonen. GSM Interception. Technical report, Department of Computer Science and Engineering, Helsinki University of Technology, 1999.

[122] J. Peterson. A presence-based geopriv location object format. Web Reference: http://www.ietf.org/internet-drafts/draft-ietf-geopriv-pidf-lo-03.txt, September 2004. Accessed October 2006.

[123] A. Pfitzmann and M. Khntopp (Hansen). Anonymity, Unobservability, Pseudonymity and Identity Management — A Proposal for Terminology. *Lecture Notes in Computer Science (LNCS)*, 2009:1–9, 2000.

[124] J. Pulver. FWD (formally known as Free World Dialup). Web Reference: http://www.freeworlddialup.com. Accessed April 2007.

[125] R. Safavi-Naini Q. Liu and N.P. Sheppard. Digital rights management for content distribution. In *Conferences in Research and Practice in Information Technology Series*, volume 34, pages 49–58, 2003.

[126] L.R. Rabiner and R.W. Schafer. *Digital Processing of Speech Signals*. Prentice Hall; US Ed edition, 1978.

[127] J. Rachels. Why privacy is important. *Philosophy and Public Affairs*, 4(4):323–333, 1975.

[128] M. Rahnema. Overview of the GSM system and protocol architecture. *IEEE Communications Magazine*, 31(4):92–100, April 1993.

[129] J.R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely. Partitioning attacks: or how to rapidly clone some GSM cards. In *IEEE Symposium on Security and Privacy*, pages 31–41, 2002.

[130] I. Ray and I. Ray. Using Compatible Keys for Secure Multicasting in E-Commerce. In *Proceedings of the 16th International Parallel and Distributed Processing Symposium*, page 327, Washington, DC, USA, April 2002. IEEE Computer Society.

[131] I. Ray, I. Ray, and N. Narasimhamurthi. A cryptographic solution to implement access control in a hierarchy and more. *Symposium on Access Control Models and Technologies SACMAT*, pages 65–73, June 2002.

[132] M.K. Reiter and A.D. Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security (TISSEC)*, 1(1):66–92, 1998.

[133] M.K. Reiter and A.D. Rubin. Anonymous Web transactions with Crowds. *Communications of the ACM*, 42(2):32–48, 1999.

[134] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, Internet Engineering Task Force, April 1992.

[135] R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 2(21):120–126, 1978.

[136] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Trans. on Knowl. and Data Eng.*, 13:1010–1027, November 2001.

[137] A. De Santis, G. Di Crescenzo, and G. Persiano. Communication-efficient anonymous group identification. In *5th ACM Conference on Computer and Communications Security (ACM CCS98)*, volume 3-5, pages 73–82, San Francisco, California, U.S.A., 1998.

[138] B. Schneier. *Applied Cryptography: Protocols, Alorithms and Source Code in C.* Wiley Computer Publishing, John Wiley and Sons, Inc, 1996.

[139] B. Schneier. Schneier on security: A weblog covering security and security technology. Web Reference: http://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html, May 2006. Accessed October 2006.

[140] M. Schumacher. Security patterns and security standards - with selected security patterns for anonymity and privacy. In *Privacy, European Conference on Pattern Languages of Programs (EuroPLoP*, 2003.

[141] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad. *Security Patterns: Integrating Security and Systems Engineering*. John Wiley & Sons, Inc, December 2005.

[142] SDL. Specification and Description Language. Standard Z.100 - Comité Consultatif International Téléphonique et Télégraphique (CCITT), 1992.

[143] A. Shamir. How to share a secret. *Communincations of the ACM*, 22(11):612–613, 1979.

[144] H. Sidgwick. *The Methods of Ethics*. London: Macmillan, seventh edition edition, 1907. First Edition 1874.

[145] A. Solanas and A. Martinez-Balleste. Privacy protection in location-based services through a public-key homomorphism. *Lecture Notes in Computer Science (LNCS) EuroPKI '2007*, 4582:362–368, June 2007.

[146] D.J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477, January 2006.

[147] W.H. Stufflebeam, A.I. Antón, Q. He, and N. Jain. Specifying privacy policies with P3P and EPAL: lessons learned. In *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 35–35, New York, NY, USA, 2004. ACM Press.

[148] L. Sweeney. k-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10:557–570, October 2002.

[149] K.J. Turner. The use of formal methods in communications standards. *Formal Methods for Protocols, IEE Colloquium on*, pages 1–3, February 1991.

[150] V. Vahadharan and Y. Mu. Preserving Privacy in Mobile Communications: A Hybrid Method. *Personal Wireless Communication, IEEE*, pages 532–536, April 1997.

[151] G.W. van Blarkom and J.J. Borking. *PET. Handbook of Privacy and Privacy-Enhancing Technologies*. Olk, J.G.E., 2003.

[152] U. Varshney, A. Snow, M. McGivern, and C. Howard. Voice over ip. *Communications of the ACM*, 45(1):89–96, January 2002.

[153] J. von Neumann and O. Morgenstern. *Theory of Games and Economic Behaviour*. Princeton University Press, Princeton, 1980.

[154] H. Wang, J. Cao, and Y. Zhang. Ticket-based service access scheme for mobile users. In Ed. Michael Oudshoorn, editor, *Conferences in Research and Practice in Information Technology*, volume 4. Twenty-Fifth Australian Computer Science Conference (ACSC2002), 2002.

[155] J.L. Wang and M.C. Loui. Privacy and ethical issues in location-based tracking systems. In *ISTAS '09: Proceedings of the 2009 IEEE International Symposium on Technology and Society*, pages 1–4, Washington, DC, USA, 2009. IEEE Computer Society.

[156] J. Woodwood. Speech coding. Web Reference: http://www-mobile.ecs.soton.ac.uk/speech_codec. Accessed October 2006.

[157] J. Hong X. Jiang and J. Landay. Approximate information flows: Socially-based modelling of privacy in ubiquitous computing. In *UbiComp '02: Proceedings of the 4th international conference on Ubiquitous Computing*, volume 2498, pages 176–193, London, UK, 2002. Springer-Verlag.

[158] J. Yoder and J. Barcalow. Architectural patterns for enabling application security. In *Pattern Languages of Programs*, 1998.

[159] G. Zhong, I. Goldberg, and U. Hengartner. Louis, Lester and Pierre: Three Protocols for Location Privacy. In *Seventh Privacy Enhancing Technologies Symposium (PET 2007)*, Ottawa, Canada, June 2007.

[160] J. Zhou and K. Lam. Undeniable billing in mobile communication. In *International Conference on Mobile Computing and Networking MOBICOM*, pages 284–290, Dallas, Texas, United States, 1998. Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking.

[161] M. Zuckerberg. Facebook. Web Reference: www.facebook.com. Accessed May 2010.