Sequenced Release of Privacy Accurate Call Data Record Information in a GSM Forensic Investigation

N.J Croft and M.S Olivier

May 2006

Information and Computer Security Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa
ringtingting@gmail.com

Abstract

The Global System for Mobile Communication (GSM) is a popular mobile communication standard. GSM networks collect personal communication information required for the billing of its subscribers. These communication records, known as Call Data Records (CDRs), may infringe on basic subscriber privacy principles as personal details of performed network events are managed and stored by the serving GSM operator. The dilemma exists, how to achieve subscriber network operator privacy that is accountable, while retaining access to subscriber activities for a forensic investigation without the need for a search warrant. To balance the requirements of protection and forensics against those for privacy, one promising direction is to investigate methods that facilitate key escrow techniques where CDRs are concerned.

This paper discusses, from a technical perspective, the network components involved when conducting a mobile forensic analysis, and how these aspects are influenced by a forensic investigation in a GSM network. It finally shows how a balance is reached between security, privacy and forensics in a GSM network through the release of, by our definition, "privacy accurate" CDR information in a sequential manner. Access to the individual elements that comprise the private CDR information, is based on prior knowledge and proof of defined hypotheses at the outset of the investigation.

Our approach focuses on an accountable CDR Forensic Anonymity Model combined with the theory of compatible keys, forms an integral part of our requirement for the release of *privacy accurate* CDR information during a GSM mobile forensic investigation.

Key words

Privacy, GSM, CDR, Forensic Investigation

1 Introduction

The Global System for Mobile communications (GSM) is a popular digital circuit switched network that provides privacy to its subscribers [4]. The original GSM specification is defined in the European Telecommunications Standards Institute (ETSI) recommendation [10]. For a comprehensive overview of GSM, see [13].

When investigating crimes, it is common for law enforcement officers to investigate mobile phone systems in order to confirm or gather important evidence. People store very private information on their phones, thus making the mobile itself a data goldmine for law enforcement officials. The term "mobile forensics" is however, only sometimes associated with the extraction of data off the mobile device itself. Stored network communication information describing network events, for the sole purpose of billing its subscribers, may also play a critical role in an investigation. This information (which may be the only accessible information to an investigator) may help to place an individual at the scene of a crime or confirm communication between two people prior to criminal act.

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 [1]. [Burmester et al. 2002] further describes "accountable privacy", whose goal is to provide a balance between these competing priorities. We choose to adopt this approach and describe how this is achieved with regards to CDR information and how this is achieved from a technical standpoint.

We introduce the notion of privacy accurate information, which describes a relationship of information in order to maintain privacy. Privacy accurate information is based on the degree of knowledge previously gathered on some related information. If accurate, the privacy-sensitive information is divulged. However, inaccuracy preserves information retaining state and privacy.

Once a decision is made to proceed with a forensic investigation, current techniques do not allow for the accused to return to his/her 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 [2]. By the same token, inherent trust is placed in the forensic investigator when dealing with privacy-sensitive information during the investigation.

The context in which this paper is set deviates from the standard legal requirement of obtaining a search warrant in order for the investigator to proceed with GSM forensic investigation. This is due to the fact that privacy-sensitive CDR information is maintained in a privacy accurate state during the investigation.

Our purpose in this paper is provide a means to conducting a forensic investigation on GSM network data communication records where accountable privacy is the goal, while providing a balance between the competing priorities of security, privacy and forensics. Through the release of individual elements in the CDR, based only on a prior verified hypothesis (made by the forensic investigator), GSM subscriber privacy,

security and state is retained. It is important to note that our approach is based on the initial stages of a GSM forensic investigation where a hypothesis is made by the investigating officer and network CDR information is gathered as supporting evidence.

Our decision to position our work in the GSM context is based on the popularity of GSM coupled with the fact that the work reported on in this paper forms part of a larger privacy and security project [4–9] set in the GSM and next generation wireless communication context. However principles applied here are not restricted to a GSM environment or a call data record context but is generic where any privacy accurate information is relinquished for forensic investigation.

This paper is structured as follows: Section 2 provides a brief background on GSM and its various network components. Section 3 covers the evidence available for extraction during a GSM forensic investigation on various GSM networked components. Section 4 describes the theory of compatible keys used later for the sequenced release of privacy accurate GSM CDR information. Section 5 illustrates our CDR Forensics and Privacy Accurate Model. Releasing privacy-sensitive CDR information in a timely and sequential manner maintains a balance between security, privacy and forensics required. Our mechanism, presented in Section 6 together with the use of compatible keys allows for a privacy accurate forensic investigation from network data events. Furthermore, Section 6 allows for returning to an original state present before the initial investigation work (based on a hypothesis) took place. Finally Section 7 concludes this paper.

2 Background

2.1 GSM

The GSM architecture consists of mobile devices and radio towers, or more formally, Mobile Stations (MSs) and Base Transceiver Stations (BTSs) [4]. The Subscriber Information Module (SIM), is a small smart card provided by the GSM network to the mobile subscriber. The SIM plays an important role in identifying a subscriber for usage and billing purposes. The SIM is placed inside a GSM device and stores several key algorithms used in identification and secure communication. The International Mobile Station Equipment Identity (IMEI) uniquely identifies a Mobile Station (MS) internationally (a unique serial number). The IMEI is allocated by the equipment manufacturer and registered by the network operator who stores it in the Equipment Identity Register (EIR). The EIR contains a list of all valid mobile equipment on the network and each MS is identified and authenticated by its IMEI.

BTSs are connected to a Base Station Controller (BSC), which in turn, is connected to a Mobile Switching Centre (MSC). The MSC has an interface to one or more BSCs and to external networks and its main responsibility includes the switching of network events such as calls. The Home Location Register (HLR) is a database which contains information (including location information) on every subscriber in the GSM network. The Visitor Location Register (VLR) is another database which contains information on subscribers visiting its location area. Figure 1 illustrates the

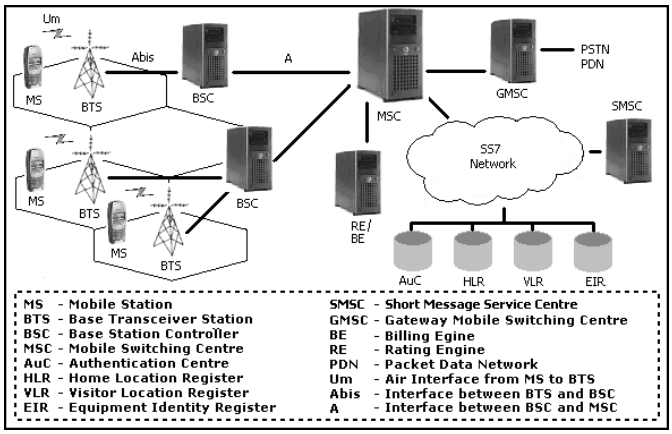

Figure 1: GSM Network Architecture

core components in the GSM network architecture.

The Location Area (LA) is a group of BTSs within a particular region and has its own identifier, known as Location Area Identifier (LAI). The LAI is broadcast by the base station. The MS can determine this information by listening for the LAI and update the information in the HLR/VLR if required. Thus each user, based on location of connection to the serving GSM network, has an associated LAI which is stored at the MS on the SIM card.

The AuC is the subscriber Authentication Centre and contains a shared secret authentication key (K_i) with the MS. In order for a network event to take place the subscriber must be authenticated to its serving network. The Security Information Module (or SIM card) and AuC are both provided with the same unique number known as the International Mobile Subscriber Identity (IMSI) and subscriber authentication key (K_i) for each GSM subscriber. The important aspect of the GSM security protocol is that a subscriber's authentication key, while stored in both the SIM and the AuC, is never transmitted over the network.

Call Data Records (CDRs) are produced every time a user performs a network event (call, SMS, data session etc). The CDRs are produced in the MSC where the network event originates. CDRs are then sent to a Billing Engine (BE) in order to determine associated network cost after which the CDRs are gathered in a centralized database used later for billing subscribers, usually at month end.

Each CDR usually comprises the following:

- Originating number (A-Number)
- Terminating number (B-Number)
- Originating and Terminating IMEI
- Length (duration)
- Type of Service
- Initial serving BTS

CDR elements are usually grouped according to selection criteria. For example, a list can be obtained showing all calls made to and received from a certain mobile device, regardless of which SIM was used. By the same token, the location of the subscribers (to the accuracy of a cell) is captured every time the subscribers partake in a network event. The storage of these call data records is subject to the GSM network operator's data retention policy (which may be influenced by governmental policies).

A CDR thus contains privacy-sensitive information relating to subscriber network events. A GSM subscriber relies on the inherent trust of one's serving network [9] where call data records are concerned. The question remains, how may we conduct a forensic investigation without compromising on such privacy-sensitive information when confirming evidence according to an initial hypothesis made. In order to understand the processes involved in conducting a forensics investigation in GSM, we first need to distinguish what would bring about such a need.

3 Forensics in GSM

With GSM a global technology, mobile and or mobile-related crime is set to increasingly impact on future forensic investigations. Such activities include, but are not isolated to: fraud, subscriber impersonation, use of a stolen mobile device, knowingly distributing mobile viruses etc.

Standard guidelines we may adopt form computer forensics include: (i) how to handle the incident, (ii) how to preserve potential evidence, (iii) how to analyze the collected data and information, and (iv) presenting evidence in court [17]. GSM forensic investigations are primarily no different, however the means for the collection, analysis and preservation of potential evidence data may differ slightly. More formally, the steps usually involved in the forensic process are [19]: data acquisition, data authentication, data analysis, evidence documentation where priority and emphasis are placed on accuracy, evidential integrity and security [16].

Forensic evidence available for extraction in GSM environments include [11]:

- Mobile Device(s)
- Network events (Calls, SMS, Data transmission etc)
- Location(s)

We consider each of these independent entities in their entirety.

3.1 On The Mobile Device

The mobile device consists of a number or key elements to a forensic investigator. They include the SIM card, any external flash memory cards and the actual hardware of the mobile device itself (mobile equipment). When a mobile device is found, common forensic protocol suggests to leave the mobile device in whatever state it is in [3]. The mobile device should then be placed in a *faraday* bag, which prevents signals from leaving or being received by the device until such time as the forensic investigation can commence.

3.1.1 Mobile Device: The SIM Card

From Section 2.1, the SIM card uniquely identifies the subscriber and holds various other user-related information. The SIM therefore contains a great deal of value to a forensic investigator. The SIM contains amongst others: International Mobile Subscriber Identity (IMSI), phone book of stored mobile numbers, calendar events, list of dialled, received and missed call numbers, stored and deleted Short Message Service (SMS), etc. [18] provides a detailed forensic analysis of SIM cards and how to extract the above mentioned information from the SIM card itself.

Usually a forensic investigator is most interested in stored SMS messages and dialled, received and missed call numbers. The storage areas on the SIM card for this information may vary phone device manufacturer to manufacturer. Legacy mobile devices are only capable of storage of such items on the SIM card directly. Modern phones however, normally use a combination of SIM, internal memory and external flash memory cards for the storage of SMS messages, dialled, received and missed call numbers etc.

In order for a forensic investigator to obtain evidence from the SIM card the PIN code (obtained from the user), or the PUK code (obtained from the service GSM operator) is required to gain access to the physical card through the operating system.

In some cases, the mobile device may *not* be available in order to conduct an investigation. In such a instance, information about network performed events of a subscriber is only available from the serving GSM operator.

3.2 On the Serving GSM Network

Usually GSM networks provide two types of services for its subscribers, namely a pre and post-paid service offering. Normally a pre-paid subscriber remains anonymous to the serving GSM network. The HLR database (refer to Section 2.1) contains information about each subscriber. Typical post-paid subscriber information captured is as follows:

- Customer name and address
- Billing name and address
- User name and address
- Billing account details
- Mobile Telephone Number
- IMSI
- SIM serial number
- PIN/PUK number
- Subscribed for services (Valued added services)

Currently legal authorities may obtain CDR information from the serving GSM network (usually on presenting the network with a court order). CDR information,

in conjunction with mobile device information (if available), may be used in various types of criminal investigations. The CDR information is usually delivered to the authorities according to pre-determined search criteria. For example, a list of all calls originating from a particular mobile number, or all calls tied to a specific location area (refer to Section 2.1).

The origin and time of the events, as well as who was responsible for the events can be uncertain. It is even possible that an event never occurred but that a digital record was fabricated to misdirect investigators or implicate an innocent person [2]. It is important to note that interconnect fraud may affect the authenticity of certain CDRs generated in the Billing Engine (BE) for foreign network events. Interconnect fraud involves the manipulation, falsification or removal of records by operators to deliberately miscalculate the money owed by one GSM operator to another when its subscribers roam away from their serving GSM network. This may lead to uncertainty when an investigation is conducted on "roaming" call data records. Thus, a mechanism is required to verify the authenticity of CDRs through MS and network mutual authentication [9].

3.3 Location Information

In order for the serving GSM network to route a network event, the serving network always needs to know the location of the mobile users (sender and receiver) [5]. Location information may be useful for instance in a homicide investigation, it is imperative to illustrate that a mobile device was placed in a certain area at a certain date and time. Here the LAI of the sender or receiver extracted from the HLR/VLR may play a pivotal role in proving a suspects presence at a crime scene.

From these available components for extraction in GSM environments, we formulate the requirements for a mobile forensic investigation:

- *Accuracy*: Mobile device (including SIM) are not tampered with. CDRs are unaltered and erroneous CDRs not counted.
- *Democracy*: GSM subscriber must know who the presiding legal authority is.
- *Privacy*: GSM subscriber's private-sensitive CDR information remains anonymous to the serving GSM network and forensic investigator until such time as evidence is obtained and the right to privacy is relinquished.
- *Integrity*: Legal authority able to verify authenticity of CDRs (including location, duration, timeframe and responsible billing engine (BE) etc based on network guarantee)

We now describe relevant hashing techniques combined with some theory of compatible keys. This is used later in the sequenced release of privacy accurate GSM CDR information.

4 Hashing Techniques and The Theory of Compatible Keys

The MD5 [14] and SHA1 [12] algorithms are two popular algorithms for generating cryptographic hash functions. SHA1, considered the successor to MD5, produces 160-bit output while MD5 produces 128-bit output. Hashing algorithm possess two unique characteristics. Firstly, given a hash value, it is difficult to construct new data resulting in the same hash. Secondly, given original data, it is difficult to find other data matching that original datas hash value.

RSA is a public key cryptosystem that offers both encryption and digital signatures (authentication) [15]. RSA is often used on the Internet, since individuals need not send any secret key to others when communication is established.

[Ray et al. 2002] proposed a new protocol for secure multicasting describing the theory of compatible keys based on the RSA algorithm. Although still unproven, [Ray et al. 2002] suggests the protocol is scalable, meaning the encrypted message is independent to the number of consumers subscribing to it. [Ray et al. 2004] further applies the use of compatible keys in a hierarchical implementation where a leaf node has 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. It is important to note the "subscriber" in this instance refers to the user involved in the encryption technique and not the GSM subscriber as the two are unrelated. 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}.

In order to show how we make use of hashing techniques and the theory of compatible keys for the sequenced release of CDR privacy accurate information, we first discuss our CDR forensic model.

5 CDR Forensic Model

We have identified the following elements that constitute the CDR Forensic and Privacy Accurate Model, namely:

- to (receiver)
- from (sender)
- to Location Area Information (LAI) (receiver)
- from Location Area Information (LAI) (sender)
- Communications Type

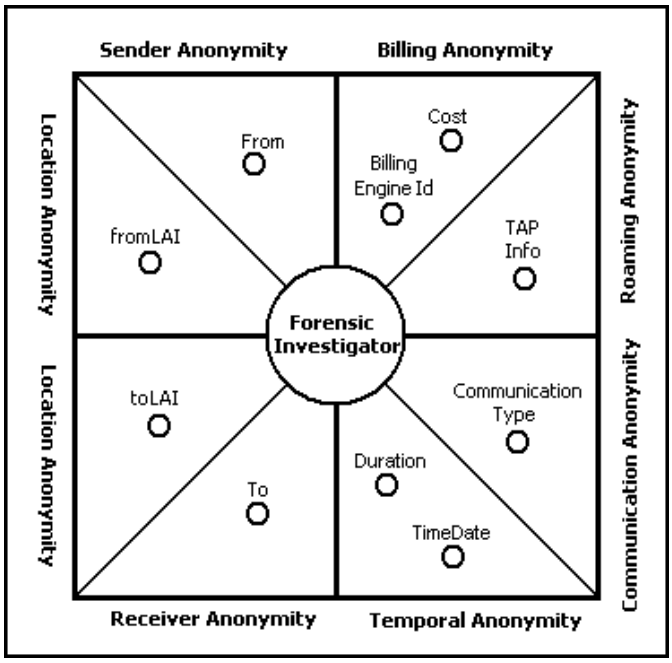

Figure 2: CDR Forensics and Privacy Accurate Model

- Duration
- DateTime
- Billing Engine Identifier
- Cost
- TAP Record (roaming information)

where all elements in the CDR have variable associated privacy and anonymity classification (refer to Figure 2). Classification of anonymity includes: sender anonymity, receiver anonymity, location anonymity, temporal anonymity, communication anonymity, roaming and billing anonymity.

To strike a balance between the need for privacy and security versus forensic ability, Table 1 describers a proposed scale for privacy accurate levels for a forensic investigation. From the lowest level of privacy accurate information (PA_0) to the highest level of privacy accurate information (PA_3), each indicates the level of protection required for striking a balance between privacy, security and associated forensic ability. For example, from privacy accurate level one (PA_1), evidence may allude to any personal information while privacy accurate level two (PA_2) evidence may imply any personal information qualifying in a possible inference being made. The cost element, which forms part of billing information, does not relinquish any personal GSM subscriber information and is placed at the lowest privacy accurate level. On the other hand, information detailing the recipient divulges undeniable personal information with regards to a network event and is subsequently placed at the highest privacy accurate level.

Privacy Accurate Level	Description	Qualification
PA_0	Evidence does not divulge any personal information	Unlinkable
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 1: A Proposed Scale for Privacy Accurate Levels for a Forensic Investigation

We apply these privacy accurate scale measures to the elements found in our CDR Forensics and Privacy Accurate Model (refer to Figure 2). Table 2 describes each element, the relationship to sequenced elements (retrievable elements based on the current privacy accurate level) and assigned privacy accurate level.

CDR element	Sequenced Element (retrievable)	Privacy Accurate Level
to	from; LAIto	PA_3
from	to; LAIfrom	PA_3
LAIto	type; duration; date	PA_2
LAIfrom	type; duration; date	PA_2
type	date; duration; BE_{id}; cost	PA_1
duration	type; date; BE_{id}; cost	PA_1
date	type; duration; BE_{id}; cost	PA_1
BE_{id}	cost	PA_0
cost	BE_{id}	PA_0

Table 2: A Proposed Scale for Privacy Accurate Levels in CDRs

For example, the cost element has a low degree of privacy accuracy PA_0 whereas the to and from elements have the highest degree of privacy accurate information PA_3 as this divulges the sender and recipient of the network event that took place. As the degree of privacy accurate information increases and is divulged, it becomes progressively more difficult to return the suspect to his/her original privacy-preserving state before the investigation began. Once information is known by the forensic investigator, whether for the purpose of the investigation or not, the privacy surrounding this information is lost. Thus, we choose to release the private accurate information in a sequenced manner.

6 Sequenced Release of Privacy Accurate GSM CDR Information

The forensic investigator makes an hypothesis Hyp, based on suspicion, that initially lead to the beginnings of a GSM CDR investigation. The onus is now on the forensic investigator to find sufficient information that correlates with this hypothesis provided by the network operator. The aim is to find enough evidence (through the

hypothesis) to warrant the release of further information based on previously gathered relational information. In this case, by proving a specific element in the CDR an additional "encrypted" element for analysis is released.

An example of hypothesis Hyp, to prove, might be: subscriber A ($from$) makes a call ($type$) from a specific location ($fromLAI$). Let us see how we would be able to prove this hypothesis in a privacy accurate sequenced manner. Recalling Table 2, $type$ has a privacy accurate level of one, $fromLAI$ is set to two and finally, $from$ is set at three.

In order to match the elements the forensic investigator needs to verify, the network operator chooses to hash each element with a hash of itself and the element XORed with the compatible key $k_{PA_{(i+1)}}$ of the next privacy accurate level. Assuming that the *element* exists at a privacy accurate level PA_i, we define the hash of the *element* such that

$$P(element) = \langle hash(element); element \oplus k_{PA_{(i+1)}} \rangle \tag{1}$$

From our example, the hashed *type* element, with an associated privacy accurate level of one (PA_1) is represented as follows

$$P(type) = \langle hash(type); type \oplus k_{PA_2} \rangle \tag{2}$$

as are the other example hashed elements ($P(from)$ and $P(fromLAI)$) with their own privacy accurate levels. The hashing of the elements and assignment of compatible keys, remain the responsibility of the serving GSM network operator. Thus, if the forensic investigator does not posses valid matching element information (based on Hyp), the forensic investigator may not be able to continue with the investigation. This inability to verify the initial hypothesis results in privacy preservation of the CDR information and in turn retains the GSM subscriber's privacy.

From Section 4, we recall that a message M encrypted with compatible keys $k_1 \dots k_i$ is denoted by $[M; k_1 \dots k_i]$. We assign compatible keys to encrypt each element based on its privacy accurate level and the privacy accurate level of its successor(s). A successor refers to all elements on a higher privacy accurate level, denoted as $element \succ PA_i$. Alternatively, a predecessor includes all elements on a lower privacy accurate level, denoted by $element \prec PA_i$

In the forensic CDR context, four compatible keys are assigned, one for each privacy accurate level $PA_0 \dots PA_3$ (refer to Table 1). Thus, we define the encryption of the *element* with privacy level PA_i as

$$E(element) = [P(element); k_{PA_i} \dots k_{PA_n}] \tag{3}$$

where $0 \leq i \leq n \leq 3$. The network operator provides the forensic investigator with all CDR elements in the above format. The forensic investigator may request these encrypted CDRs to be formatted according to his/her initial hypothesis Hyp. Continuing with our example, the *type* element with privacy accurate level PA_1 is encrypted as follows

$$E(type) = [P(type); k_{PA_1} \dots k_{PA_3}] \tag{4}$$

meaning that any of the compatible keys ($k_{PA_1} \dots k_{PA_3}$) are able to decrypt the message M, which in this case, is $P(type)$.

The result alludes to the following property: the higher the privacy accurate level the lower the number of assigned compatible keys when encryption takes place. From our example again, the $from$ element with privacy accurate level PA_3 is only encrypted with compatible key k_{PA_3}. In contrast, the *type* element with privacy accurate level PA_1 is encrypted with compatible keys $PA_1; PA_2; PA_3$.

Based on the CDR information the forensic investigator needs to verify against the received privacy accurate CDR. The forensic investigator first attempts to validate against the element with the lowest degree on the privacy accurate level PA_0. This initial element, for example BE_{id} is provided to the forensic investigator together with the entire encrypted CDR at the outset of the forensic investigation. If an element is successfully hashed (according to a hypothesis made by the forensic investigator), revealing the element itself, the key to move to encrypted elements on the same or a higher degree on the privacy accurate scale are unveiled. This successor key element $k_{PA_{(i+1)}}$, once the hypothesized element information has been confirmed with the $hash(element)$ (refer to Equation 1), is retrievable with the *element* in the following way

$$(element \oplus k_{PA_{(i+1)}}) \oplus \mathbf{element} = k_{PA_{(i+1)}} \tag{5}$$

Informally, if the hypothesized element (with privacy accurate level PA_i) is hashed with the *element* revealing the *element* information again, then we may use the *element* to retrieve the compatible key $k_{PA_{(i+1)}}$. This is achieved through a simple XOR operation shown in Equation 5.

Returning to our example, decrypting $E(type)$ with compatible key k_{PA_0} results in $P(type)$. The hypothesized *element* is hashed and compared to the $hash(type)$ in $P(type)$. If successful, the hypothesized *element* is equal to *type*, *type* may be used to retrieve the next compatible key at a higher privacy accurate level k_{PA_2}.This exposed compatible key k_{PA_2} is now used to decrypt $E(fromLAI)$ revealing $P(fromLAI)$ and so on. If the entire original hypothesis Hyp proves correct, all CDR information is revealed in a complete and accurate sequenced manner to the forensic investigator. However, if any hypothesis for a specific *element* is incorrect, the forensic investigator may not continue with the investigation as the compatible key $k_{PA_{(i+1)}}$ is irretrievable.

The formal privacy accurate element encryption process is defined by the following equation:

$$EPA_i = [P^*(element); k_{PA_i} \dots k_{PA_n}] \tag{6}$$

where

$$P^*(element) = \{P(element) | element \preceq PA_i\} \tag{7}$$

Informally, n is equal to the maximum number of defined privacy accurate levels and $P^*(element)$ indicates *any one* of the element(s) whose privacy accurate level is less than or equal to its predecessor.

Note the assumption in the equation for EPA_i that it is possible to serialize a set and encrypt it. Also note the implication that once the hypothesis has been confirmed for a single element on a given privacy accurate level, all other elements on

that level can be exposed. However, a hypothesis is necessary to expose any elements on the higher level.

Such an approach provides for a sequenced access control to private CDR information. By the same token, if the hypothesis proved incorrect, access to privacy-sensitive information is restricted thus retaining the desired level of subscriber privacy. The mechanism used above strikes a balance between privacy, security and forensic ability. However, such an approach is not limited to the GSM context and may be applicable where any privacy-preserving forensic investigation takes place.

7 Conclusion

In this paper we provided a means to conducting a forensic investigation on GSM network data communication records where accountable privacy is the goal, while providing a balance between the competing priorities of security, privacy and forensics. Through the release of individual elements in the CDR, based only on a prior verified hypothesis, the GSM subscriber privacy, security and state is preservable. Thus effectively eliminating the need for a search warrant on CDR information in order for an investigator to proceed with the forensic investigation.

We illustrated a CDR forensics and privacy accurate model which provided the basis for the sequenced release of private GSM CDR information. We utilized the theory of compatible keys in necessitating the hierarchical release of private information in a GSM CDR forensics investigation. This fulfils the goal to return a GSM subscriber (suspect) to privacy-preserving state if insufficient supporting evidence is not forthcoming. The forensic investigator is able to override (based on a hypothesis) any anonymity classification in order to extract the relevant privacy accurate CDR information in a sequenced manner. Future work will include an analysis on key strength and pitfalls in an elements with limited information such as *type* which may include the set SMS, MMS, Call only.

References

[1] 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.

[2] E. Casey. Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, 1(2), 2002.

[3] Computer Security Division, National Institute of Standards and Technology, NIST FIPS PUB 800-72. Guidelines on PDA Forensics. Technical report, U.S. Department of Commerce, November 2004.

[4] N.J. Croft. Secure Interoperations of Wireless Technologies. Masters dissertation, University of Pretoria, School of Computer Science, October 2003.

[5] 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, September 2004.

[6] 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.

[7] N.J Croft and M.S Olivier. On Preserving Network and Subscriber Privacy in GSM Roaming. *VLDB Privacy-Preserving Data Management*, September 2005. Submitted.

[8] 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, September 2005.

[9] N.J. Croft and M.S. Olivier. Using compatible keys in achieving subscriber privacy channelling for billing in GSM Networks. In S. Furnell, P. Dowland, and G. Kormentzas, editors, *Proceedings of the Fifth International Network Conference*, pages 245–252, 2005.

[10] European telecommunications Standard Institute, ETSI. *Recommendation GSM 02.09; Security related network functions*, June 1993. Tech. Rep.

[11] A.J. Goode. *Forensic extraction of electronic evidence from GSM mobile phones*. The Forensic Science Service, 2003.

[12] 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.

[13] M. Rahnema. Overview of the GSM Systems and Protocol Architecture. *IEEE Communications Magazine*, April 1993.

[14] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, Internet Engineering Task Force, April 1992.

[15] 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.

[16] M.M. Saud. *An Overview of Disk Imaging Tool in Computer Forensics*. SANS Institute, 2001.

[17] Y. Wang, J. Cannady, and J. Rosenbluth. Foundations of computer forensics: A technology for the fight against computer crime. *Computer Forensics: Computer Law & Security Report*, 21:119–127, 2005.

[18] S.Y. Willassen. Forensics and the GSM mobile telephone system. *International Journal of Digital Evidence*, 2(1), 2003.

[19] H.B. Wolfe. Evidence analysis. *Computers & Security*, 22(4):289–291, 2003.