Forensics and the GSM mobile telephone system

Svein Yngvar Willassen, M.Sc,
Senior Investigator, Computer Forensics, Ibas AS

Abstract

The GSM system has become the most popular system for mobile communication in the world. Criminals commonly use GSM phones, and it is therefore a need for forensic investigators to understand which evidence can be obtained from the GSM system. This paper briefly explains the basics of the GSM system. Evidence items that can be obtained from the Mobile Equipment, the SIM and the core network are explored. Tools to extract such evidence from the components of the system exist, but there is a need to develop more sound forensic procedures and tools for extracting such evidence. The paper concludes with a short presentation on the future UMTS system, which largely builds on the design of GSM.

1.0 Introduction

With GSM, systems for mobile communication reached a global scale. In the western world, it seems everyone has their own mobile phone, and GSM has taken more and more of the market. GSM allows users to roam seamlessly between networks, and separate the user identity from the phone equipment. In addition the GSM system provides the functional basis for the 3rd generation mobile system, UMTS.

All these factors make it important for forensic investigators to understand how the GSM system works, and how evidence can be extracted from it. Criminals took the step into the mobile age a long time ago, and information from the mobile system can give the investigator crucial information on the criminal's actions. It is however important that the information contained in the system is retrieved with a forensically sound method. It is equally important that the investigator understands the system in order to be able to explain to the courts how the system works. It is the aim of this paper to give forensic investigators an introduction to the current state of GSM forensics, and highlight some of the issues that will have to be solved in the future.

2.0 History of the GSM system

In the beginning of the 1980s several different systems for mobile communications were developed in Europe. The need for a common system that allowed roaming between countries was early recognized. In 1982 a number of European countries created a new standardization organisation called "Groupe Speciale Mobile" (GSM). The mandate of this group was to develop a standard to be common for the countries that created it. In 1988 the GSM was included in the European Telecommunication Standards Institute (ETSI), and the standards developed by GSM thus became standards for all telecommunication administrations in Europe.

The main work with the GSM took place from 1988 - 1990 and resulted in 12 series of specifications which in great detail specified the inner workings of GSM. In 1990, when phase 1 of the specifications was finished, there were three dominating automatic systems for mobile communications in the world:

- American AMPS from 1984, with networks in the US.
- British TACS from 1985, with network in Britain.
- Nordic NMT from 1981, with networks in the Nordic countries.

Unlike these systems, GSM is a fully digital system, allowing both speech and data services and allowing roaming across networks and countries. These features made GSM a very popular system, not only in European countries but also elsewhere. The term GSM has been chosen as a trademark for the system, meaning "Global System for Mobile communications", whereas the group within ETSI working with the standards has been renamed SMG (Special Mobile Group). Today GSM is the largest system for mobile communications in the world, and exist on all continents.

3.0 Overview of the GSM system

The GSM system is specified in 12 series of specifications. For phase 1, these specifications constitute over 4000 pages. In the following, a short overview of the system will be given.

3.1 Entities of the GSM system

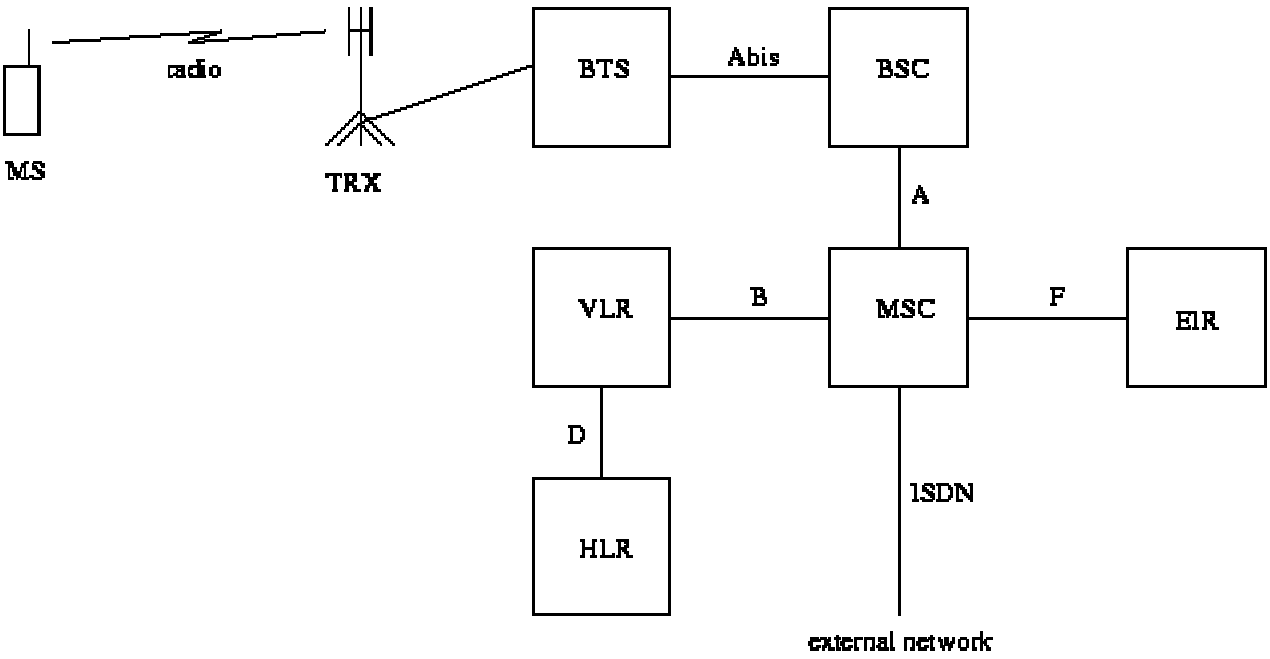

Fig 1 – Entities in the GSM system

The GSM system consists of a number of separate entities [GSM0302]. These are shown in figure 1. The entities are connected through interfaces with their own names according to the specifications, these names are shown on the figure.

3.2 The Mobile Station

The Mobile Station (MS) is the user equipment in GSM. The MS is what the user can see of the GSM system. The station consists of two entities, the Mobile Equipment (the phone itself), and the Subscriber Identity Module (SIM), in form of a smart card contained inside the phone.

Production of Mobile Equipment is done by many different manufacturers, and there will almost always be a wide range of different MEs in a mobile network. Therefore the specifications specify the workings of the ME in great detail. In order to verify the conformal of the specifications by Mobile Stations, equipment must obtain type approval from the standardization body [GSM1110].

The MEs in GSM are independent from networks-providers. The identity of the subscriber is obtained from the SIM that has to be inserted into the MS to make it work. The SIM contains the IMSI (International Mobile Subscriber Identity) which uniquely intentifies the subscriber to the network. It also contains information necessary to encrypt the connections on the radio interface. The ME itself is identified by an IMEI (International Mobile Equipment Identity), which can be obtained by the network upon request. Without the SIM, calls to and from the mobile station is not allowed. The SIM is implemented as a smart card that can exist in two forms; large or small.

3.3 The Base Transciever Station

The Base Transciever Station (BTS) is the entity corresponding to one site communicating with the Mobile Stations. Usually, the BTS will have an antenna with several TRXs (radio transcievers) that each communicate on one radio frequency. The link-level signalling on the radio-channels is interpreted in the BTS, whereas most of the higher-level signalling is forwarded to the BSC and MSC. Speech and data-transmissions from the MS is recoded in the BTS from the special encoding used on the radio interface to the standard 64 kbit/s encoding used in telecommunication networks. Like the radio-interface, the Abis interface between the BTS and the BSC is highly standardized, allowing BTSs and BSCs from different manufacturers in one network.

3.4 The Base Station Controller

Each Base Station Controller (BSC) controls the magnitude of several hundred BTSs. The BSC takes care of a number of different procedures regarding call setup, location update and handover for each MS.

3.5 The Mobile Switching Centre

The Mobile Switching Centre is a normal ISDN-switch with extended functionality to handle mobile subscribers. The basic function of the MSC is to switch speech and data connections between BSCs, other MSCs, other GSM-networks and external non-mobile-networks. The MSC also handles a number of functions associated with mobile subscribers, among others registration, location updating and handover. There will normally exist only a few BSCs per MSC, due to the large number of BTSs connected to the BSC. The MSC and BSCs are connected via the highly standardized A-interface [GSM0808]. However, due to the lack of standardization on Operation and Mangement protocols, network providers usually choose BSCs, MSCs and Location Registers from one manufacturer.

3.6 The Location Registers

With each MSC, there is associated a Visitors Location Register (VLR). The VLR can be associated with one or several MSCs. The VLR stores data about all customers who are roaming withing the location area of that MSC. This data is updated with the location update

procedure initiated from the MS through the MSC, or directly from the subscriber Home Location Register (HLR). The HLR is the home register of the subscriber. Subscribtion information, allowed services, authentication information and localization of the subscriber are at all times stored in the HLR. This information may be obtained by the VLR/MSC when necessary. When the subscriber roams into the location area of another VLR/MSC, the HLR is updated. At mobile terminated calls, the HLR is interrogated to find which MSC the MS is registered with. Because the HLR is a centralized database that need to be accessed during every call setup and data transmission in the GSM network, this entity need to have a very large data transmission capacity.

3.7 The Equipment Identity Register

The Equipment Identity Register (EIR) is an optional register. Its purpose is to register IMEIs of mobile stations in use. By implementing the EIR the network provider can blacklist stolen or malfunctioning MS, so that their use is not allowed by the network.

3.8 GSM Security

GSM provides authentication of users and encryption of the traffic across the air interface. This is accomplished by giving the user and network a shared secret, kalled Ki. This 128-bit number is stored on the SIM-card, and is not directly accessible to the user. Each time the mobile connects to the network, the network authenticates the user by sending a random number (challenge) to the mobile. The SIM then uses an authentication algorithm to compute a authentication token SRES using the random number and Ki. The mobile sends the SRES back to the network which compares the value with an independently computed SRES. At the same time, an encryption key Kc is computed. This key is used for encryption of subsequent traffic across the air interface. Thus, even if an attacker listening to the air traffic could crack the encryption key Kc, the attack would be of little value, since this key changes each time the authentication procedure is performed.

Fig 2 – Subscriber Identity Module (SIM)

4.0 Evidence in the Subscriber Identity Module

The SIM (Shown in figure 2) contains information that can be of value as evidence. First, the SIM itself can have value as evidence. As shown on the picture, the name of the network-provider is usually printed on the SIM, along with a unique identification number that can be

used to get information from the provider, such as the subscriber name and address and phone number associated with the SIM. Phone records can also be retrieved from this number as discussed below.

4.1 Access to the SIM

A PIN-code (Personal Identification Number) is usually required to access the SIM. This number is a four-digit code that must be entered to gain access. Since the phone cannot be used without access to the SIM, this number must be entered whenever the phone is turned on. If the user fails to enter a valid PIN through three attempts, the card becomes blocked, and the user must instead enter a 8-digit code called PUK to reopen it. If the user fails to enter the correct PUK during ten attempts, the card becomes permanently blocked and cannot be reopened.

PIN-codes for a card can be changed and deactivated by the user. The PUK-codes are fixed and cannot be changed. Since the PUK-code is fixed, the network operator usually keeps track of the PUK-codes for all its users. Therefore, the investigator can almost always gain access to a SIM-card by asking the network operator for the PUK code. It might, however, be more efficient to ask the owner of the phone to provide correct PIN or PUK-codes. During searches, the PUK code might also be recovered, since phone owners usually keep the PUK code in writing in case they forget the PIN.

4.2 Forensic analysis of SIM cards

The SIM card is a smart card, containing a processor and non-volatile memory. In GSM, the SIM card is used as a storage device for subscriber related data. The only purpose of the processor is to implement the access mechanism and security features. The physical and logical properties of the access mechanism are defined in GSM specifications. [GSM1111]

The SIM card can be accessed by mounting the card in a standard smart-card reader. To access the card logically software is needed that implement the GSM SIM access mechanism. The contents of the SIM card is organized as a series of files containing binary data that can be downloaded once the user has authenticated himself with a PIN or PUK code.

The best forensic procedure would be to image the entire contents by downloading the entire memory of the SIM and compute a hash value of this memory. There is currently no tool available to do this. There are however tools available to download binary contents of individual files and store them as individual files. Examples of such tools are Sim Manager Pro (previously Sim-Surf Profi) [SIMMAN], ChipIt [CHIPIT], PDUSpy [PDUSPY] and SIM-Scan [SIMSCAN]. There are also available administrative tools, which will synchronize data such as text messages between a SIM card and a computer. Such tools should be avoided in forensic analysis, since the contents of the card will be contaminated. The currently most popular tools in law enforcement communities is the tool Cards4Labs [C4L], developed by Netherlands Forensic Institute, available to law enforcement only. This tool does not store a digital copy of the SIM-files on the computer, but rather produces a text report on most of the content on the SIM card.

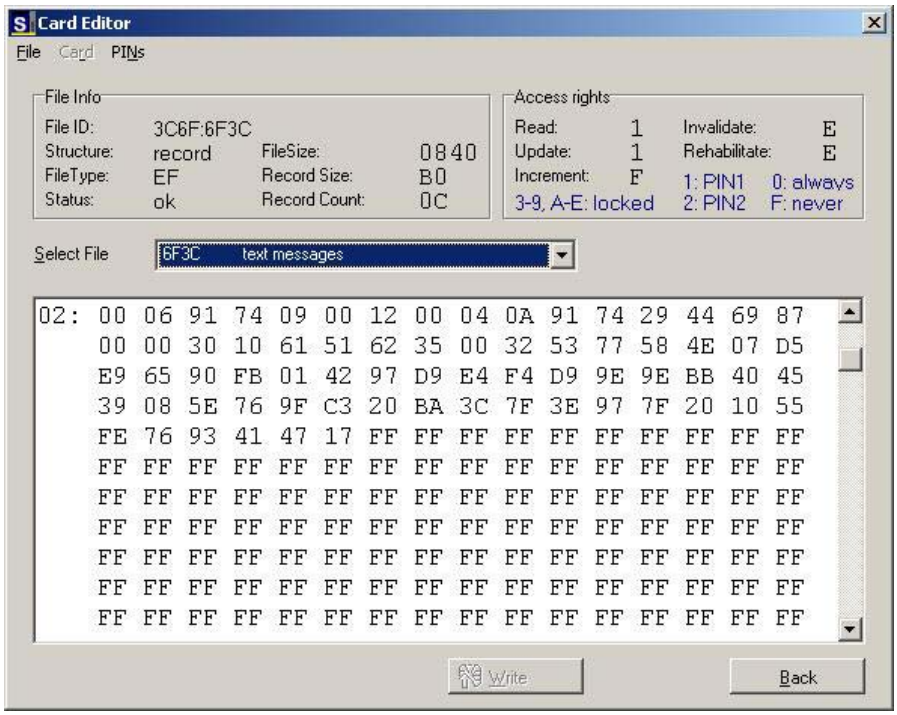

Fig 3 – Reading a file as hex values with Sim-Surf Profi

4.3 The files on the SIM-card

The evidence on the SIM card is stored in the following files:

Phase	Phase ID	1 byte
SST	SIM Service table	5 bytes
ICCID	Serial Number	10 bytes
LP	Preferred languages	variable
SPN	Service Provider name	17 bytes
MSISDN	Subscriber phone number	variable
AND	Short Dial Number	variable
FDN	Fixed Numbers	variable
LND	Last Dialled numbers	variable
EXT1	Dialling Extension 1	variable
EXT2	Dialling Extension 2	variable
GID1	Groups 1	variable
GID2	Groups 2	variable
SMS	Text Messages	n * 176 bytes
SMSP	Text Message parameters	variable
SMSS	Text message status	variable
CBMI	Preferred network messages	variable
PUCT	Charges per unit	5 bytes
ACM	Charge counter	3 bytes
ACMmax	Charge limit	3 bytes
HPLMNSP	HPLMN search period	variable
PLMNsel	PLMN selector	variable
FPLMN	Forbidden PLMNs	12 bytes
CCP	Capability configuration parameter	14 bytes

ACC	Access control class	2 bytes
IMSI	IMSI	9 bytes
LOCI	Location information	11 bytes
BCCH	Broadcast control channels	16 bytes
Kc	Ciphering key	
AD	Administrative data	variable

All of the stored data can potentially have evidentiary value. However, most of the files refer to network internals that the user never see, and therefore does not represent evidence on the usage of the telephone as such. We therefore limit the discussion here to the files that typical represent relevant evidence on phone usage. For further reference, please refer to [GSM1111].

4.4 Location information, serial number, IMSI, MSISDN

The LOCI-file byte 5-9 contains among other information the Location Area Identifier (LAI) where the mobile is currently located. This value will be retained in the SIM card when the mobile is shut off. Thus, it is possible for an investigator to determine in which Location Area the mobile was located when it last was operating. The network operator can assist the investigator in identifying which area the identifier corresponds to. It should be noted that a location area can contain hundreds or even thousands of cells. Which cell the mobile was last camping it is not stored in the SIM card.

The serial number, IMSI and MSISDN all provide a unique identification of the customer. The serial number, which is possible to obtain without providing PIN, identifies the SIM itself. The IMSI is the customer identification, whereas the MSISDN is the phone number to the mobile.

4.5 Text messages

The Short Message Service (SMS) became a very popular service in GSM during the last years of the 90s. The service basically lets a user type in a short text message on the phone and send it to another user via a central Short Message Service Centre (SMSC). The SIM provides storage space for text messages. Most SIM-cards have 12 slots for text-messages. In addition, most modern phones also let the user store text messages in memory in the ME. It's up to the ME software and user configuration which memory is used first, and which messages are stored. A common configuration is that all incoming messages are stored by default, and outgoing messages are stored only at the user's explicit request. Most MEs use the SIM memory first, before utilizing ME internal memory.

Each of the SMS slots on the SIM have the following layout:

Byte

1	Status	[GSM1111]
2-176	TPDU	[GSM0340]

The status byte can take the following values:

%00000000	Unused
%00000001	Mobile terminated message, read

%00000011	Mobile terminated message, not read
%00000101	Mobile originated message, sent
%00000111	Mobile originated message, not sent

When a user deletes a message, only the status byte is set to 0. Thus; deleted text-messages can be recovered except for the status byte as long as the slot has not been overwritten by a new message. Recovery is done simply by interpreting byte 2-176 of the stored message. Cards4Labs does this by default.

The TPDU consists of the following elements:

- The ISDN number of the service center
- The ISDN number of the sender (or recipient, depending on status) of the message
- Date and time (in seconds) the message was received by the service center, referring to the clock on the service center.
- Phonebook number
- The message itself

Phonebook number refers to how the user get the message presented. A ME can for instance define phonebook 1 as “Inbox”, phonebook 2 as “Outbox” etc.

The message itself can be coded in different codes. The original and still most common code scheme is 7-bit packed. In this scheme, the message is coded in a GSM-specific 7-bit character set, which is converted into a bit-stream. The bit-stream is then split into bytes to fit on the SIM card. As a result, the text cannot be read directly from the data using a normal hex editor. Programs such as Cards4Labs and Sim-Surf Profi will decode all the contents of the TPDU.

When a new message is written to an available slot, the part of the slot that is not taken up by the message is filled with hex value FF. Thus, it is not possible to find remnants of previous messages in “slack-space” in the text-message slots.

4.6 Short Dial Numbers

To aid the user in remembering numbers, most phones have an ability to store commonly dialled phone numbers. Most SIM-cards have around 100 slots for storing short dial numbers. On GSM phones older than around 1999 this was the only mechanism for storing numbers. On most modern phones, the phone also have it’s own memory and the user can choose to use one of the memories or both.

In the SIM, short numbers are stored in a binary encoded format, containing a name and a number in each slot. Programs such as Cards4Labs and Sim-Surf Profi will decode the format. When a short-number is deleted, the information in the slot is overwritten with hex value FF. Thus, it is not possible (or at least not feasible) to recover deleted short dial numbers. The slots will normally be allocated in sequence, so identifying empty slots between used slots will normally indicate that a stored number has been deleted.

4.7 Last Numbers Dialled

The SIM also has the ability to store the numbers last dialled. Most cards have only 5 slots for this. The numbers are stored in a binary encoded format that can be interpreted by programs such as previously mentioned Cards4Labs and Sim-Surf Profi. Most phones does not use this feature however, and store a calling log on phone memory instead. Investigators should therefore also investigate the phone for calling logs.

4.8 Attacks on the SIM module

It is important for the investigator to understand that the Subscriber Identity Module can be attacked by crafty criminals. In a forensic context, the most obvious attack method is removal of evidence. Since the files on the GSM card can be accessed in raw, an attacker can remove evidence by overwriting storage space. For instance, a person knowing that deleted text messages are still accessible on the card, could use the card editor in Sim-Surf Profi to overwrite the messages with other information.

Of more interest to a criminal would be to attack the SIM to impersonate another subscriber. If this could be done, a criminal would be able to make calls on other subscriber's accounts, and impersonate other subscribers, as their caller identification would show up at the called party. In the GSM system, the subscriber identity is only stored on the SIM, so the protection against impersonation only rely on the SIM security features. The only information that identifies a user is the user IMSI and the secret encryption key Ki. Both are stored on the SIM and in the HLR in the network. As we have seen, the IMSI can be read directly from the SIM card if the user knows the PIN or PUK code. IMSI of other valid subscribers could also be obtained by listening to unencrypted network traffic on the air interface, since the IMSI will be transferred unencrypted across the air interface whenever a mobile registers with a new network. (This happens a lot at certain locations, such as international airports.)

But how can the criminal obtain the encryption key Ki? Since the Ki is stored only internally in the SIM card it is not accessible directly, but only through usage of the encryption algorithms stored on the card. However, since the user of a SIM card can feed the algorithm with known numbers, the Ki can be found if the algorithms contain weaknesses that allow such analysis. Such an attack is commonly known as a chosen-plaintext attack. The algorithms in GSM do indeed have such a weakness. A tool to extract Ki from a SIM has been implemented in the program Sim-Scan, available on the Internet [SIMSCAN]. Both IMSI and Ki can therefore be obtained by anyone with access to a SIM-card and knowledge of PIN or PUK.

The next step for the criminal is to produce a new SIM-card with the IMSI and Ki implemented. This cannot be done on SIM-cards in use, since IMSI is locked through the SIM access mechanism, and Ki is only internally stored. The attacker therefore needs to get hold of a fresh card without any subscriber information. These cards can be ordered from the same source where network providers get their cards. The card must then be programmed with a special tool for programming of fresh cards. Such a tool is distributed together with the Sim-Scan package. An attacker could also get hold of a generic smart card and smart card programmer, and then program the card to act as a SIM.

The conclusion is that impersonation of other GSM subscribers is indeed possible for anyone who can get hold of a subscriber card and corresponding PIN/PUK.

Fig 4 - Mobile Equipment (ME)

5.0 Evidence in the Mobile Equipment

Specifications specify many functional requirements to the Mobile Equipment in the GSM system when it comes to the interface with the network and the SIM. As long as these requirements are met, it's up to the manufacturer to decide which other functions to implement on the ME, such as storage of different types of information. It therefore exist a long range of different phones on the market, each with it's own capabilities of information storage and each with it's own potential as digital evidence. A study of all GSM mobile phones in a forensic context is therefore infeasible. This paper will focus on general principles and information that is commonly stored on different types of equipment.

5.1 Access to the phone

Since access to the SIM is needed to use the phone, all phones ask for the SIM PIN code when the phone is turned on, unless the PIN has been deactivated. Many phones also have the ability to ask for a separate access code for access to the phone memory. This feature is rarely used, since the user then will have to enter two access codes whenever the phone is turned on. In principle, the investigator will not have any means to get hold of the phone access code if it is activated. It is believed however, that most phones have an ability to circumvent the code by using special hardware/cables and software to access the contents of the phone.

5.2 Forensic analysis of GSM phones

Most, if not all, mobile phones implement information storage by means of one or several on-board flash memory chip(s). This memory contains all information stored on the phone as well as phone-internal software. The most forensically sound procedure for analysis of phones would therefore be to find a way to digitally image the contents of the phone memory chips, and analyse the contents off-line. Since most phones provides a way for the manufacturer to access the contents and upgrading the software, this procedure can actually be done for most phones. The procedure would however require knowledge of the programming interface of the phone, information that manufacturers usually keep for themselves. Tools for accessing the phone memory directly (called "flashers") are available on the Internet for many phones.

(Phones from Nokia, Ericsson, Siemens and Motorola amongst others) These flashers seem to be unauthorized by the phone manufacturers. Using such tools for forensic imaging would therefore in the author's opinion seem questionable, but might be the only way to retrieve information that could have relevance as evidence.

Most phones can be connected to a computer for data transfer. Connection can be done by means of a special cable from the manufacturer, or by using wireless interfaces such as IrDa or BlueTooth. The information on the phone can then be accessed by using special software from the manufacturer. Such software will commonly let the user download information contained within the phone, such as text messages, short numbers, dialled numbers, received calls, and configuration parameters. The contents of the memory will not be directly accessible using such tools.

A third method of forensic analysis of a mobile phone is simply to use they keypad of the phone to access the stored information, and photograph it as it comes on screen. Most information stored on the phones can be accessed using the phone menu system. The IMEI is on most phones available by typing *#06#. As this method is cumbersome and the analyst risks to change the information on the phone, it should be avoided if possible.

The author has observed that some phones tie information stored on the phone to the subscriber identity on the SIM-card. This is probably meant as a security feature to prevent access to sensitive information by unauthorized users. As an example, Nokia phones store logs of outgoing and incoming calls in the phone. If a user removes the SIM card and insert another card, these logs will be cleared. Investigators should therefore be cautious with removing the card from the phone before relevant information has been secured.

5.3 Phone contents

The following contents of modern mobile phones can have value as evidence:

- IMEI
- Short Dial Numbers
- Text Messages
- Settings (languge, date/time, tone/volume etc)
- Stored Audio Recordings
- Stored Computer Files
- Logged incoming calls and dialled numbers
- Stored Executable Progams
- Stored Calendar Events
- GPRS, WAP and Internet settings

Most of this information is available through cable and manufacturer specific software. However, direct analysis of the memory could potentially reveal other hidden information, such as deleted text messages. Such analysis has to the authors knowledge not yet been performed.

5.4 Attacks on the phone

The before mentioned tools for direct access to the phone memory, so called flashers, also allow anyone to freely modify the contents of the phone, including phone software. Such

modification is usually done to remove access constraints in the phone. The most common access constraint one would want to remove is a Service Provider lock (commonly called SP-lock). A SP-locked phone is locked to SIM cards from a certain service provider. Such locked phones are often sold together with cheap subscriptions or prepaid subscriptions, to lock the customer to a certain service provider.

Another change one would want to do is to change the IMEI code of a phone. This is necessary to use stolen phones, since stolen phone IMEIs will be blacklisted in the EIR. The ability to change IMEI could also make it more difficult to trace the usage of specific phones. It is therefore desirable to find a way to detect that the IMEI of a phone has been changed. The obvious method to do this is to compare the internally stored IMEI with the IMEI printed on the phone (commonly located under the battery). To detect changes of IMEI and other changes to a mobile phone it could be useful to find a way to detect electronically if a phone has been "flashed". This could be an area of further research within mobile phone forensics.

6.0 Electronic evidence in the network

GSM networks contain information that can be of value as evidence. The most valuable information is arguably the Call Data Record database of the network operator. This database contains information on each and every call made in the mobile network.

6.1 Subscriber database

The network provider maintains it's own subscriber database. The database usually contains the following information about each customer:

- Customer name and address
- Billing name and address (if other than customer)
- User name and address (if other than customer)
- Billing account details
- Telephone Number (MSISDN)
- IMSI
- SIM serial number (as printed on the SIM-card)
- PIN/PUK for the SIM
- Services allowed

Some providers allow prepaid subscriptions, where the customers are not identified by name. Such subscriptions cannot be tied to a person unless a SIM card with the subscription was seized from a specific person. Given the SIM-card number, the network operator can always identify the associated IMSI and MSISDN, and then provide access codes and call details for that card.

6.2 Call Data Records

Call Data Records (CDRs) are produced every time a user makes a call or send a text message. The CDRs are produces in the switch (MSC) where the call or message originates. CDRs are then gathered in a centralized database and used for billing and other purposes.

Each CDR contains the following:

- Originating MSISDN (A-Number)
- Terminating MSISDN (B-Number)
- Originating and terminating IMEI
- Length
- Type of Service
- Initial serving Base Station (BTS) (not subsequent BTSs after handover)

CDRs can be filtered on any of the above parameters. This means that one can not only obtain a list of all calls made to/from a certain SIM, but also to/from a certain phone, regardless of which SIM was used. By looking at the serving BTS, the location of the subscriber can be pinpointed to the accuracy of a cell at any time the subscribers sends or receives a call or a text message. Such information certainly has great evidentiary value.

6.3 Subscriber location

As long as a subscriber is logged on to the network, it is stored in the HLR which Location Area the subscriber is currently located in. The network operator can however pinpoint the subscriber to a certain cell at any time by activating *subscriber trace* in the network. More accurate location than one cell (the coverage of one base station) was not initially supported in GSM [WIL98]. Governmental requirements have later demanded the implementation of a location service in GSM Phase 2 and 2+. Such a location service has now been implemented in many GSM networks. The location service works by performing triangulation of a mobile between different base stations, by using field strength measurements reported from the phone to the network. The location can then be pinpointed to a more accurate level, ranging from a few hundred meters down to tenths of meters, depending on the conditions. The location service can be invoked from the mobile at the users request. It can also be invoked from the network, for instance when the user calls an emergency call centre. The network operator can use the location service to locate a customer at any time.

An interesting situation is if it is possible to locate where a phone was shut off. This is often the situation during searches for missing persons. When a phone is turned off it deregisters with the HLR before it shuts down to avoid incoming calls to page the mobile in the entire location area. This means that it is impossible to tell which location area or cell a phone was shut down in after the shutdown. However, if the phone loses its power source, it will not deregister in the HLR since it has no power to communicate. As a result, the last location area of the phone will be available in the HLR a period of time after the phone lost its power. This situation can also be detected by people trying to call the missing subscriber. The reason is that since the mobile is not deregistered in the HLR, the network will try to page the mobile in the entire location area. The caller will therefore experience 15-20 seconds of silence before the caller gets the message that the phone cannot be reached. This property can be useful to detect if missing persons have fallen in water or been implicated in violent crashes, since the mobile will lose its power source in such situations.

6.4 Attack on the network

For a long time, it was believed that the GSM system was immune to transmission interception on the air interface due to the digital encoding and encryption. This has however shown to be wrong. The transmission protocol on the air interface has flaws in the lack of mutual authentication and the lack of mandatory encryption. The protocol specifies that the network can order the MS to turn on or off encryption.

Mobile calls can therefore be intercepted by launching a man-in-the-middle attack in the following way:
The attacker constructs a device that act as a Mobile Station on one side, and as a Base Station on the other side. The Base Station side acts as a normal base station within the network whose customers the attacker want to intercept. Customers of this operator who are closer to the attacker than a normal base station (in terms of radio field strength) will now try to register with the attacker's base station. The attacker now acts as a Mobile Station and forwards the traffic to a normal base station of the provider network. Since the traffic is just forwarded, neither network nor MS will notice anything abnormal. Now, when subscriber Alice wants to use her mobile to call Bob, the call will go through the attackers device. The attacker now poses as network and order Alice's MS to use unencrypted communication. The attacker then encrypts the data, and sends it to the network encrypted. Since Alice herself normally will not notice that the communication is unencrypted, the attacker can now listen in to the conversation, without anyone knowing.

Equipment to perform this type of attack has indeed been reported sold in the black market, although very expensive. It should be noted that it is possible to discover such attacks by constructing phone software that warns the user when the communication is unencrypted. (The MS cannot deny unencrypted communication, since that would not conform to GSM specifications.)

7.0 The Future – UMTS

Within the next ten years, the UMTS (Universal Mobile Telephone System) is expected to become the dominant mobile system all over the world. UMTS has been specified by 3GPP (3rd Generation Partnership Project), and heavily builds on the principles set forth in GSM. Some features of the UMTS of interest for the forensic examiner will be discussed in the following.

7.1 UMTS network structure

UMTS contains similar network elements as GSM for circuit switched calls. As in GSM, the core of the network is the MSC, and location registers HLR and VLR. Base Stations (BS) are controlled by network elements called RNCs (Radio Network Controllers). In addition to the circuit switching elements, UMTS will have a parallel network structure for packet switching. This consists of interconnected routers, where IP will be used as the transmission technology. The two different network structures are called CS (Connection Switched) Domain and PS (Packet Switched) Domain. In the future, as more and more of traditional circuit switched transmission will be realized through packet switching (such as Voice over IP), it is expected that the PS Domain will dominate, with Ipv6 as the transmission protocol.

7.2 UMTS radio interface

The biggest difference between GSM and UMTS is the new radio interface, called UTRAN. The frequency/time division multiplexing scheme used in GSM has been abandoned for a code division multiplexing scheme called WCDMA. For the end user this technology will give better throughput rates (in theory up to 960 kbit/s) and more stable connections. The interference on other electronic equipment in GSM due to the time multiplexing will also disappear. However, since the radio interface is very different, the network providers will

have to build a lot of new base stations, a very expensive operation. UMTS will therefore coexist with GSM, and mobile terminals will be able to use both systems.

The security scheme in UMTS is similar to GSM, with a shared secret hidden on the USIM providing authentication and encryption between the mobile terminal and the network. The cryptographic algorithms have been changed to known algorithms without shown weaknesses. In addition, the protocol has been changed to include mutual authentication, and inability to turn off encryption as was shown to be a problem in GSM. The protocol also includes cryptographic signature of the signalling traffic before the encrypted connection has been established to disallow an attacker to intervene at this stage.

Only time will show if these security measures are enough to keep an entire world of attackers at bay.

7.3 UMTS terminals

UMTS does not lay any specific demands on the terminal. It can therefore be expected that there will be a whole range of different terminals with even more diversity than today. The UMTS Subscriber Identity Module (USIM) will be an extended version of todays SIM. As the GSM SIM, the USIM will be implemented as a smart card. The USIM can contain several "profiles", for use by different users or different terminals. These profiles contain the information on today's SIM, such as IMSI and MSISDN. In addition, the USIM will be able to contain executable applications, and other user data.

7.4 Location services

In GSM, location service was added at a late stage in the specification process, long after the core networks were up and running. In UMTS, location service has been implemented from the start. The location service gives both the user and network the ability to obtain the position of the phone. UMTS allows for location service using field strength triangulation, but also specifies network assisted GPS as a solution. This would require GPS receivers in each and every phone, but would give higher positioning accuracy when the phone is outdoors.

8.0 Conclusion

Since GSM is the worlds largest system for mobile communication today and also lay the foundation for the future UMTS, it is important to recognize the need to study the methods and tools for forensic analysis of the GSM system. Where current investigation is done with tools not specifically designed for forensics (except Cards4Labs), the future will hopefully see tools that let an investigator image and analyse contents of phones and SIM-cards in a forensically sound way. Further research is also needed into analysis of information stored on phones and SIM-cards.

It is clear that the GSM system contains large amounts of information valuable to the investigator. Most of the information is available today and can be retrieved and have a great potential to be used as evidence.

9.0 References

[MOULY92] Mouly, M. "*The GSM System for Mobile Communications*" Palasieu, France, 1992.

[GSM0302] *Network Architechture*, ETS 300 522 (GSM 03.02), ETSI recommendation, 1996

[GSM1110] *Mobile Station (MS) conformance specification*, ETS 300 607-1 (GSM 11.10), ETSI recommendation, 1997

[GSM0808] *BSS-MSC layer 3 specification*, ETS 300 590 (GSM 08.08), ETSI recommendation, 1996.

[GSM1111] *Specification of the SIM – ME interface,* ETS TS GSM 11.11, ETSI recommendation, 1996

[GSM0340] *Technical realization of the Short Message Service (SMS),* ETS TS GSM 03.40, ETSI recommendation, 1996

[SIMMAN] *Sim-Manager Pro*, Software package, Commercial http://www.txsystems.com/

[CHIPIT] *Chip-It*, Software package, Freeware http://mobileoffice.co.za/download_chipit_sim_editor.htm

[PDUSPY] *PDU-Spy*, Software package, Freeware http://www.nobbi.com/download.htm

[SIMSCAN] *Sim-Scan*, Software package, Freeware http://users.net.yu/~dejan/

[C4L] *Cards4Labs*, Software package, Law Enforcement only http://www.forensischinstituut.nl/

[WIL98] Willassen S., "*Mobile Station Location in GSM*", 1998. http://www.willassen.no/msl/

[KAR01] Kaaranen H. et al, "*UMTS Networks*" Helsinki, Finland, 2001.

About the Author

Svein Yngvar Willassen graduated from the Norwegian University of Science and Technology in 1998 with a M.Sc in Telematics with focus on GSM systems and information security. He has since been employed as a special investigator at the Norwegian Police Computer Crime Centre, where he worked with computer forensics and investigation of

computer intrusion. During this period Willassen contributed to the Interpol Computer Crime Manual, as well as work in the International Organization on Computer Evidence. Since August 2002, he has worked with computer forensics in the computer forensics and data recovery company Ibas AS. Contact: svein@willassen.no.