GSM Security Approach towards the Survey and Evaluations of Presents Situation

Pawar Anuradha Bhalerao[1,] Mr. Hemant Verma[2.]

M.E. (EC), SVCOE Indore Department of Electronics Engineering SVCOE, Indore, (M.P), India
Associate Professor, SVCOE Indore Department of Electronics Engineering SVCOE, Indore, (M.P), India

Abstract: *The Global System for Mobile Communications (GSM) is the most widely used cellular technology in the world. Approximately 800 million people around the world are using GSM for different purposes, but mostly for voice communication and SMS. For GSM, like many other widely used systems, security is crucial. The security involves mechanisms used to protect the different shareholders, like subscribers and service providers. The aspects of security that this report covers are mainly anonymity, authentication and confidentiality. The important aspects of the system that need protection are described, along with the implementation of mechanisms used for the protection. It appears that many of the very valuable aspects of GSM can be attacked. The anonymity of a GSM user is compromised resulting in the attacker being able to observe the time, rate, length, sources or destinations of e g calls. Even tracking a subscriber's movements becomes possible. However, a passive attack is not sufficient to perform these attacks. The attacker needs to mount an active attack using equipment offering base station functionality. Authentication is a crucial aspect of a wireless communication system due to the nature of the medium used, i e the radio link that is available to everyone and not only the legitimate entities. Even the authentication mechanisms are attacked. It is possible to clone a subscription either by having physical access to the smart card or over the air interface. Cloning a subscription over the air requires base station functionality.*

Keywords: *Mobile Security, WSN, Cryptography.*

I. Introduction

Security plays a more important part in wireless communication systems than in systems that use wired communication. This is mainly because of the ubiquitous nature of the wireless medium that makes it more susceptible to security attacks than wired communications. In the wireless medium, anyone can listen to whatever is being sent over the network. Also, the presence of communication does not uniquely identify the originator (as it does in the case of a pair of coaxial cables or optical fibers). To make things worse, any tapping or eavesdropping cannot even be detected in a medium as ubiquitous as the wireless medium. Thus security plays a vital role for the successful operation of a mobile communication system. GSM is a 2G system that is used daily by hundreds of millions of people. Can it withstand today's high-tech-equipped hackers?

This document aims to give an introduction to the security mechanisms used to protect GSM2, and present the attacks possible to mount on the system, mainly on the anonymity, authentication and confidentiality aspects of security, along with the resources needed. This will include:

- Describing how the very complex GSM system works. Components used to build the system are introduced and the techniques used to provide the functionality are described. This will answer the question: How does GSM work?
- Introducing the requirements on the security of a wireless communication system along with the mechanisms used by GSM to meet these requirements. This will answer the question: What are the valuable assets of GSM and how are these assets protected?
- GSM was formerly acrony for Groupe Spéciale Mobile (founded 1982). Now is acronym for Global System for Mobile Communication.
- Presenting attacks on GSM security, which include recent cryptanalytical attacks on the cryptographic algorithms protecting the confidentiality of GSM user traffic as well as other types of attacks, especially those making use of weaknesses in the GSM protocols, and examining the resources needed in order to mount these attacks successfully. This will answer the question: How can valuable aspects of GSM be attacked and what resources are needed in order to realise these attacks?
- Drawing conclusions about the suitability of GSM as a communication infrastructure for different user groups. Finally, this will answer the question: Is GSM suitable for providing communication services for users with very valuable information to protect?

II. Background

GSM, like many other large systems with large numbers of users, contains many valuable assets that need protection against misuse and deliberate attacks. This chapter will highlight the valuable assets that, in general, exist in a wireless communication system, and that are crucial to protect for the best of the system's shareholders (subscribers and service providers).

2.1 Requirements for End-User Privacy

A subscriber to a mobile communication system needs protection in the following areas:

2.1.1 Protection of Call-Setup Information

During the call-setup process, the mobile terminal will communicate important call-setup information to the network. Some of the information that could be sent is: calling party number, calling card number, service type requested, etc. This information must be protected and secured from eavesdroppers. [1]

2.1.2 Protection of Speech

All spoken communication and other communication services must be properly encrypted by the cryptographic system, so that it cannot be intercepted by any eavesdropper listening to the radio interface or other interfaces of the system. [1]

2.1.3 Privacy of User-Location

Any leakage of specific signalling information on the network may enable an eavesdropper to approximately locate the position of a subscriber, which will jeopardize the subscriber's privacy. Hence the subscriber must be protected from such attacks on his/her privacy of location. [1]

2.1.4 Privacy of Calling Patterns

Information related to traffic generated by a particular user and his/her calling patterns should not be made available to eavesdroppers. Typical information is: caller-id, frequency of calls to some particular number, etc. [1]

2.1.5 Privacy of User-ID

All mobile communication systems use some sort of user-ID to identify their subscribers. This subscriber identification information (or the user-ID) must be protected from hackers. Transmission of this information in the clear either over the radio interface or over the network must be avoided as far as possible. [1]

2.2 Integrity Protection of Data

In addition to securing the data (system data or traffic data) against eavesdroppers, there must be a provision in the network and the terminal to detect or verify whether the data it receives has been altered or not. This property is called Data Integrity. System and user data that are considered to be sensitive must be protected by using this method. [1]

2.3 Requirements for Preventing Theft of Service or Equipment

Theft of service and equipment is a very serious problem in mobile personal communications. The network subsystem doesn't care whether a call has originated from a legitimate or from a stolen terminal (the mobile equipment/phone) as long as it bills the call to the correct account (the legitimate user cares, though!). There are two kinds of theft that could be possible here, namely the theft of personal equipment and theft of the services offered by the service provider. The cryptographic protection must be designed to make the reuse of stolen terminals as difficult as possible. Further, it should block theft of services made possible by techniques such as cloning. Note that e g cloning can be done both by the hackers using stolen equipment, as well as legitimate users . [1]

The following sections will present important requirements for preventing theft.

2.3.1 Cloning and Clone Resistant Design

Cloning is a serious problem in mobile communication systems. Cloning refers to the ability of an intruder to determine information about a personal terminal and clone, i e create a duplicate copy, of that personal terminal using the information collected. This kind of fraud can be easily accomplished by legitimate users of the network themselves, since they have all the information they need to clone their own personal terminal stored in the Subscriber Identity Module (SIM) in the terminal. In this way, multiple users can use one account by cloning personal equipment. It could even be done by a stranger who wants to use services on the expense of legitimate users or sell the cloned devices. This is where equipment cloning causes problems. The cryptographic protection for the mobile network must incorporate some kind of clone-resistant design. The most obvious requirement for this design is the security of personal equipment information. This security must be provided for the radio-interface, the network databases, and the network interconnections such that personal equipment information is secure from impostors.

Since the terminal can be used by anyone, it is necessary to identify the correct person for billing purposes, i e the user must be identified to the network . This may take the form of a smart-card or a plug-in that plugs into a terminal and is unique to each user. The process by which the network identifies the user is called the authentication process, where information about the identity of the user is transmitted to the network and verified using some cryptographic technique.

2.3.2 Equipment Identifiers

In systems where the account information is separated (both logically and physically) from the terminal, e g GSM, stolen personal equipment and its resale could be an attractive and lucrative business. To avoid this, all personal equipment must have unique identification information that reduces the potential of stolen equipment to be re-used. This may take the form of tamper-resistant identifiers permanently plugged into the terminals. [1]

III. Related Study

This chapter provides a general overview of various types of attacks that can be mounted against computer systems and networks, and cryptographic methods that are commonly used in practice to protect against these attacks. Cryptographic concepts that are relevant for wireless communications, in particular GSM, are emphasised where necessary.

3.1 Security Attacks

Attacks on the security of computer systems and networks are best characterized by viewing the function of the computer system or network to be providing information. The attacker is an entity trying to disturb the normal flow of information in the system (Figure 3.2). Attacks can be categorised as follows:

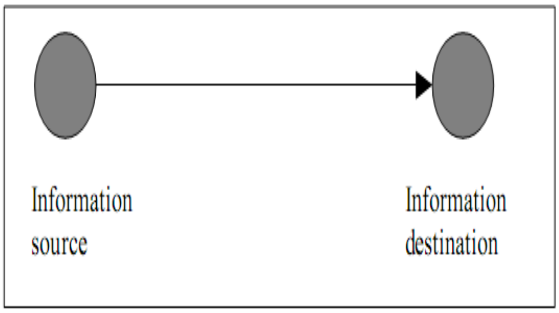

Figure 3.1: Normal Flow of Information.

- **Interruption:**

An asset of a system is either destroyed or it becomes unavailable or unusable (Figure 3.2). This is an attack on availability. The attacker may e g cut a communication line or use jamming to interrupt wireless communications. [5]

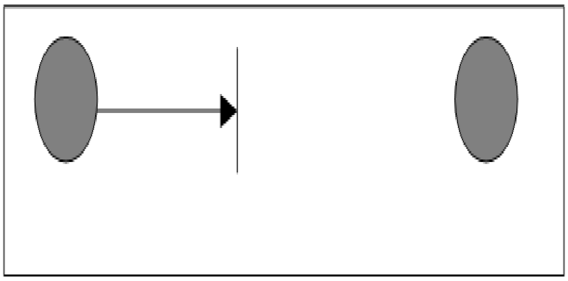

Figure 3.2: Interruption

• Interception:

An unauthorised party gains access to an asset (Figure 3.3). This is an attack on confidentiality. The unauthorised party could be a person or a computer process. Examples include wiretapping/eavesdropping to capture data in a network. [5]

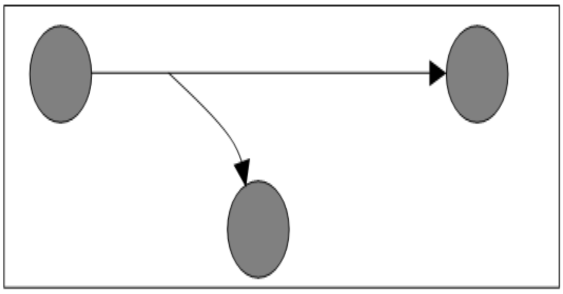

Figure 3.3: Interruption

• Modification:

An unauthorised party not only gains access to but also tampers with an asset (Figure 3.4). This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being
transmitted between communicating entities. [5]

Figure 3.4: Modification

• Fabrication:

An unauthorised party inserts counterfeit objects into the system, or claims to be some other party (Figure 3.5). This is an attack on authenticity. Examples include the insertion of spurious messages (e g signalling messages in the GSM) in a network and the addition of records to a file. [5]

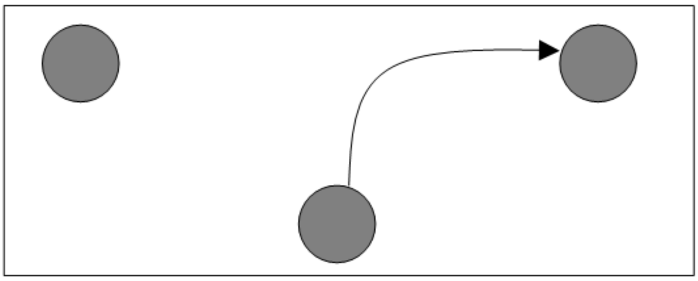

Figure 3.5: Fabrication

3.2 Cryptographic Protection Methods

In traditional cryptography, a message in its original form is known as plaintext or cleartext. The encrypted information is known as ciphertext and the process of producing this ciphertext is known as encryption or enciphering. These two terms will be used interchangeably in this report and will refer to the same process. The reverse process of encryption is called decryption or deciphering. Cryptographic systems tend to involve an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information.

There are three types of cryptographic paradigms:

3.2.1 Secret Key Cryptography

Secret key cryptography involves the use of a single key that is shared by the communicating parties (Figure 3.6). This is the method used in GSM for providing confidentiality. Given a message (plaintext), encryption produces the ciphertext, which is of the same length as the plaintext. Decryption retrieves the plaintext, using the same key used for encryption. This kind of encryption is also called conventional or symmetric cryptography.

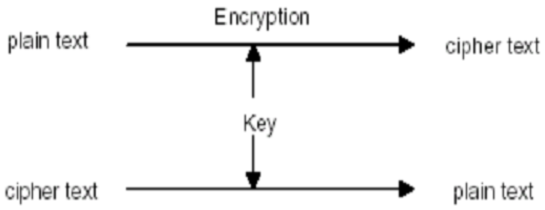

Figure 3.6: A Secrete Key Cryptographic System.

IV. Problem Statement

Now we have an idea about how radio signals are generated and used to transmit different kinds of information across the air. In this section we will continue to study GSM and take a look at the architecture of the GSM network. This will include a description of the components that build up the system, and how these are interconnected, in addition to introducing the mechanisms used in order to protect the system’s valuable assets, as outlined in Chapter 2.

4.1 An Overview of the GSM Network

A GSM network (Figure 4.1) is comprised of the Mobile Equipment (ME), the Subscriber Identity Module (SIM), the Base Station Transceiver (BTS), the Base Station Controller (BSC), the Transcoding Rate and Adaptation Unit (TRAU), the Mobile Services Switching Center (MSC), the Home Location Register (HLR), the Visitor Location Register (VLR), and the Equipment Identity Register (EIR). Together, they form a Public Land Mobile Network (PLMN). [3] These different components are described below:

4.1.1 The Mobile Station (MS)

The MS is carried by the subscriber. It is made up of the ME, also known as the terminal, and a smart card known as the Subscriber Identity Module (SIM).

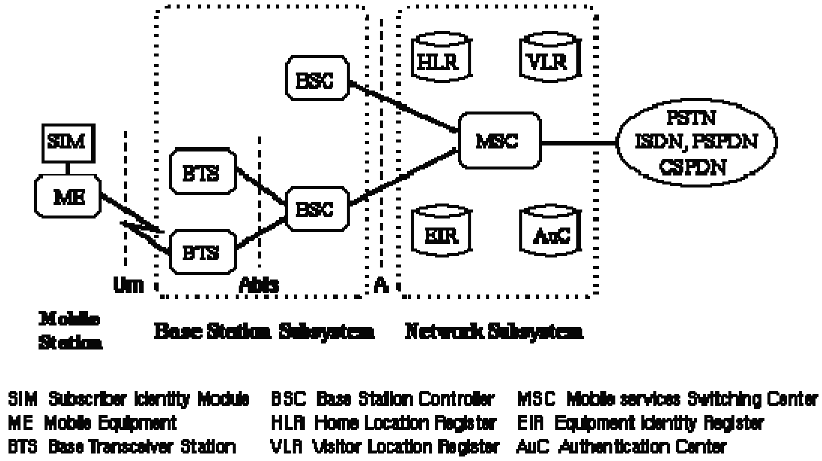
BSC
HLR
VLR
SIM
BTS
MSC
PSTN
ISDN, PSPDN
CSPDN
ME
BSC
BTS
EIR
AuC
Um
Abis
A
Mobile Station
Base Station Subsystem
Network Subsystem
SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile services Switching Center
EIR Equipment Identity Register
AuC Authentication Center

Figure 4.1: An overview of the GSM network [4]

The SIM, which is basically a smart card, determines the directory number and the calls billed to the subscriber. The SIM contains the following subscriber related information:

- The International Mobile Subscriber Identity (IMSI) , which uniquely identifies a subscriber and without which the GSM service is not accessible. IMSI is only used by the network.
- A secret subscriber authentication key Ki and a cryptographic algorithm A3/A8 which provide security functions for authenticating the SIM, and generating session keys.
- Temporary network related data like the Temporary Mobile Subscriber Identity (TMSI), Location Area Identifier (LAI), Kc, forbidden PLMNs, etc.
- Service related data like Language Preference and Advice of Charge.
- Card Holder Verification Information that authenticates the user to the card and provides protection against the use of stolen cards [5]. A Personal Identification Number (PIN) is used. If the wrong PIN is entered three times in a row, the card locks itself, and can only be unlocked by providing a Personal Unblocking Key (PUK).

4.1.2 The Base Transceiver Station (BTS): The BTS controls all of the radio related tasks and provides connectivity between the network and the Mobile Station (MS) via the radio interface.

4.1.3 The Base Station Controller (BSC): The BSC takes care of all the central functions and controls a set of BTSs. The BSC and the controlled BTSs form the Base Station Subsystem (BSS).

4.1.4 Mobile Services Switching Center (MSC): The MSC controls a large number of BSCs. It is very similar to a digital telephone exchange or a switch and it handles the routing of incoming and outgoing calls and the assignment of user channels on the A-interface.

4.1.5 Home Location Register (HLR): The HLR is a data repository that stores the subscriber specific parameters of a large number of subscribers. The most important parameters of a subscriber, like the Ki and IMSI are stored in the HLR. Every PLMN requires at least one HLR and every user is assigned to one specific HLR.

4.1.6 Authentication Center (AUC): The AuC has as a key component a database of identification and authentication information for each subscriber, and is in most cases an integral part of the HLR. Attributes in this database include the subscriber's IMSI, secret key Ki, LAI, and TMSI The AuC is responsible for generating triplets of values consisting of the RAND, SRES (Signed RESponse), and session key Kc which are stored in the HLR for each subscriber. [1]

4.1.7 Visitor Location Register (VLR): The VLR network element was devised to off-load the HLR of user database related functions. The VLR, like the HLR, contains subscriber information, but only information for those subscribers who roam in the area for which the VLR is responsible. When a subscriber roams away from the network of his/her own service provider, information is forwarded from the subscriber's HLR to the VLR of the serving network, in order to complete the authentication process. When a subscriber moves out of a VLR area, the HLR takes care of the relocation of the subscriber information from the old to the new VLR. A VLR may have several MSCs, but one MSC always uses one VLR. [1]

4.1.8 Equipment Identity Register (EIR): Since the subscriber identity (SIM) and the ME are treated independently by GSM, it is possible to operate any GSM ME with any valid GSM SIM. This makes cellular terminal theft an attractive business and probably starts a possible black market for stolen GSM terminals. To protect against such thefts, the Equipment Identity Register (EIR) was introduced in the GSM system. Every GSM terminal has a unique identifier, called the International Mobile Station Equipment Identity (IMEI), which (according to the GSM organisation) cannot be altered without destroying the terminal. It contains a serial number and a type identifier [6].
The EIR maintains three lists:

- The White list: is composed of all number series of equipment identities that are permitted for use
- The Black list: contains all equipment identities that belong to equipment that need to be barred
- The Grey list: MEs on the grey list are not barred (unless on the black list or not on the white list), but are tracked by the network (for evaluation or other purposes). [1]

Equipment Identification can be done by the network operator by requesting the IMEI from the ME. [6]

V. Proposed Solution

5.1 The Security Implementation – Protecting Valuable Assets

The mechanisms used in GSM to provide anonymity, authentication and confidentiality to shareholders are described in the following subsections.

5.1.1 Anonymity

Anonymity is provided by using temporary identifiers. When a user switches on his/her mobile terminal, the real identity (IMSI) is used to identify the MS to the network and then a temporary identifier Temporary Mobile Subscriber Identity (TMSI) is issued and used for identifying the MS to the network in future sessions. According to the ETSI specification the network should always encrypt TMSI before transmitting it to the MS. A LOCATION UPDATE REQUEST results in the MS receiving a TMSI [4]. The TMSI has significance only within a location area. Outside the location area it has to be combined with the LAI to provide for an unambiguous identity. Usually the TMSI reallocation is performed at least at each change of a location area, as a LOCATION UPDATE REQUEST is issued by the MS to the network (Such choices are left to the network operator). [6] From then on the temporary identifier is used. Only by tracking the user is it possible to determine the temporary identifier being used. [7]

5.1.2 Authentication

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). One of the primary security functions of the SIM is to authenticate the subscriber to the network. This process assures the network that the MS requesting service is a legitimate subscriber and not some intruder. A GSM network verifies the identity of a subscriber through a challenge-response process similar to the mechanism described in 3.2.1. When a MS requests service, the network sends a mathematical challenge to the MS (RAND), which it must answer correctly before being granted access. [7] The challenge sent by the network to the MS consists of a 128 bit number called RAND. It is very important that RAND is unpredictable and has a very slim chance of being repeated, otherwise an attacker could easily make a codebook of (RAND, SRES) pairs and use the information to gain access to services. When the MS receives RAND it passes it into the SIM for processing. The SIM sends RAND and the secret 128-bit key K8 i through the A3 algorithm to produce a 32- bit "signed response". The response, called SRES, is transferred out of the SIM into the terminal, where it is then transmitted to the network. This is the MS's response to the network's challenge. Meanwhile the network (the AuC) has performed the same set of operations (Figure 4.1). Using the same value of RAND and an identical copy of Ki, the network has computed its own value for SRES.

When the network receives SRES from the MS it compares it to its own SRES. If the two values are identical, the network assumes the MS is legitimate and allows service to proceed. If the two values are not the same, the network assumes the 8 The GSM specifications do not specify the length of Ki, thus it is left for the choice of the operator, but usually it is a 128-bit key. SIM does not have the proper secret key Ki and therefore denies service to the MS. [5]

Since the RAND value changes with (almost) every access attempt, an eavesdropper recording the SRES response will not be able to successfully reuse it later. Even if by chance a particular RAND challenge happens to be reused (and an attacker manages to impersonate a legitimate subscriber to the network), a GSM network has the flexibility to authenticate the MS as often as it wishes; perhaps several times throughout the duration of a call. The next challenge the MS (SIM) receives from the network will probably be a new one for the attacker, impossible for him/her to compute the right SRES for [5]. It should be noticed that a cornerstone of the GSM security protocols is that a subscriber's secret key, Ki, remains secret. While stored in both the SIM and the AuC, Ki is never transmitted over the network. Figure 2.5 illustrates the authentication process. A3 and A8 aren't actually algorithms, but simply placeholders [5]. The COMP128 algorithm (Figure 5.1) is almost exclusively used for A3 and A8 throughout the world. This algorithm was designed to be a reference model for GSM implementation but for various reasons has been adopted by almost all GSM providers world-wide. COMP128 was cracked in April 1998 and a new stronger version, COMP128-2 was developed. However, due to the huge amount of cost involved in replacing COMP128 (or maybe ignorance in some cases), it is believed that most operators are still using the old flawed algorithm. [8]

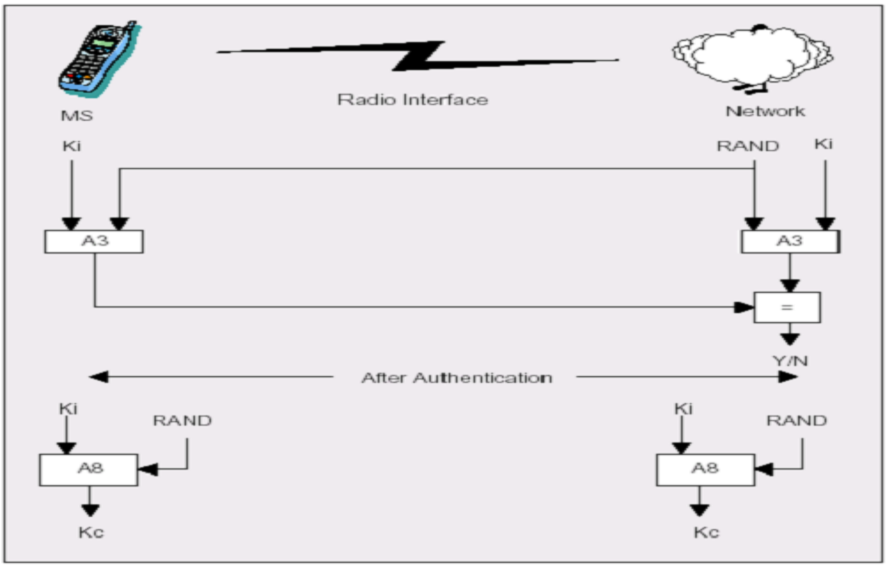

Figure 5.1: Authentication and session key generation in GSM

5.1.3 Confidentiality

The SIM also provides information needed to encrypt the radio connection between the MS and the BTS. More specifically it computes the session key Kc , which is later used in some version of A5 for encrypting the voice or data before transmission on the radio path. The algorithm used for computing the 64 bit Kc , is called A8 and is invoked according to Figure 5.1 [5]. A3/A8 is, as mentioned in the previous section, often realised in practice using the initial design specification given by the GSM MoU, which is a single algorithm called COMP128 (Figure 5.2).

Recall that GSM uses a technique called time division to share the radio channel with up to eight other users (see Section 4.2.1). Each user takes turns using the common radio channel, sending and receiving information only during one of the eight available time slots in every frame. Each frame is very short, lasting onlymabout 4.6 milliseconds, and is identified by a frame number. A GSM conversation uses two frames, one going from the base station to the MS and another going from the MS back to the base station. Each of these frames (time slots) contains 114 bits of user information, which is often digitised and compressed speech. Thus, every 4.6 milliseconds the MS receives 114 bits of information from the base station and transmits another 114 bits to the base station. It is these 228 bits that require encryption to protect it from eavesdroppers.

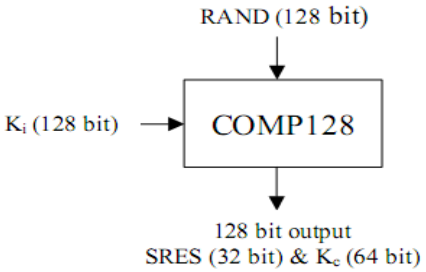

Figure 5.2: A popular A3/A8 implementation (COMP128)

Of the SIM and into the MS, where it is used by a third algorithm (A3 and A8 are the other two) called A5. A5 uses KC and the current, publicly known, frame number to produce a key stream of 228 bits, half of which encrypts the dl and the other half encrypts the ul. For each new frame to be transferred a new 228 bit key stream is produced by the A5 to be used to encrypt (and decrypt) the frame. A5 resides in hardware in the terminal, not in the SIM, and must operate quickly and continuously to generate a fresh set of 228 bits every 4.6 milliseconds. Also, because GSM terminals are designed to operate in different networks, the A5 algorithm must be common to all GSM networks.

There are presently at least two known versions of A5. The first, called A5/1, is only used in countries that are members of CEPT9, provides the strongest level of encryption across the air link (Actually A5/3 is stronger but it is to be used in future networks). Although officially using 64 bit keys, in actual practice the keys are no more than 54 (!) bits long, the last ten bits are forced to be zeros. The second algorithm, A5/2, is considered to be much weaker than A5/1 and is designed for export to countries outside CEPT where presumably there is an interest in easily cracking encrypted conversations.

Since encryption requires additional hardware in each base station, raising the cost and complexity of the network, a third “encryption” option is to employ what’s called A5/0, that is, no encryption at all. The network asks the MS to start encrypting using a certain encryption algorithm each time information will be transmitted on the radio link.

The two algorithms A5/1 and A5/2 will be described in the following subsections:

5.1.4 Preventing Theft of Service or Equipment

As mentioned earlier, in GSM the customer subscription and authentication capability is contained within a smart card (SIM). Any mobile will take on the identity of a subscriber by insertion of a smart card. The mobiles now become attractive items to steal, as they can be used with another SIM card. To prevent this, GSM has specified an International Mobile Equipment Identifier (IMEI). Although at first evaluation to an operator, it may seem as the stolen mobiles have no effect since they do not affect a subscription, there will be problems with an increase in customer facing staff to handle esquires and a possibility that GSM terminals are expensive to insure. [7] An Equipment Identity Register (EIR) exists in each network, with Black, White and Grey Lists (see Section 5.1.8) for stolen or non type approved mobiles, valid mobiles and mobiles that need tracking, respectively. GSM has defined a procedure so that approved, lost or stolen mobile IMEIs can be communicated to all other operators. Type approval authorities issue white list numbers (random ranges of valid IMEIs) to mobile manufacturers, and manufacturers inform the Central Equipment Identity Register (CEIR) when the mobiles are released to market. All operators are able to post their black lists to the CEIR, and in return collect a consolidated list of all operators' black and white lists. [9]

VI. Conclusion

Given the strong belief in the security community that only protocols that can be tested should be trusted (that security should depend on the secrecy of keys and not of algorithms), some believe that it was inevitable that GSM would be attacked for its dependency on the proprietary authentication and confidentiality algorithms. These algorithms are viewed as cryptographically weak by many security analysts and this is proved by the increasing number of propositions for how to break these algorithms. It is a fact that COMP128, the algorithm used for authentication and session key generation, only required a couple of hours to crack (Wagner and Goldberg) and it has been broken for a couple of years, making the process of cloning SIMs using COMP128 trivial and cheap. Another fact is that it only took a couple of hours for the same team to crack A5/2. Their attack only requires a few cycles to crack the algorithm. There are propositions on how to break the algorithms protecting the privacy of GSM conversations as well. Many of these propositions demand however unrealistic portions of known plaintext and/or huge amounts of computation power (especially for the onetime pre-computation part of the attacks). The latest cryptographic attack on A5/1 is however a ciphertext-only attack requiring only a small number of encrypted frames in order to find the session key in real-time. This attack requires however very large amounts of computation power both in the pre-computation stage and in the real-time part of the attack.

Looking at the history of the cryptographic protection of GSM the picture becomes clear. Although it is obvious that secret algorithms make it harder to break the protection in the short run, it often fails in the long run. Designers of security reason that before cryptanalysing the algorithm the potential attacker has to know the algorithm, which will make the task much harder. This kind of reasoning fails; history shows that COMP128, A5/1 and A5/2 was reverseengineered and cracked in a short period of time by individual researchers, for some reasons. Firstly, the public crypto community is not given a chance to examine the algorithm to find eventual flaws. Secondly, some entities may have interest in deliberately build in flaws in the algorithms to make it easy for them to crack when they need to. Limiting the key bits to 54 instead of 64 may be an indicator of this. This reasons will make the device in [8] possible to build even in the future, meaning that authorities and other entities that can buy and use the device will be able to perform illegal tracking, eavesdropping etc, violating the personal integrity of the concerned users of the system. Note that law enforcement agencies are able to perform this actions in a legal way asking for permission to perform tracking and/or eavesdropping. Not having access to the resources required to break the cryptographic algorithms protecting GSM does not however mean that GSM is secure. Certain flaws in the protocols that are used to manage the system make it possible for people with relatively modest resources to listen to GSM conversations in real-time without breaking the encryption algorithms. An attacker with access to a modified base station (easy to buy a used one) can mount active attacks on the system enabling the attacker to break the anonymity and confidentiality aspects of GSM and even clone SIMs using the radio link.

VII. Future Work

The author of this report has presented some attacks on the second generation GSM that are believed to be possible in presence of the needed resources. However, the presentation has omitted the details of how things are done and the attacks have not been verified through practical experiments. A future work could go deeper into:

- examining which functionality needs to be implemented in a base station in order to be able to mount an active attack on a MS, e g to be able to mount a man-in-the-middle attack. Of course an estimation of how much a device that can act like a (limited) base station costs may be interesting knowledge. Of course it is essential to examine also whether such a device can operate according to the outlined attacks without making operators and authorities suspicious.
- performing practical experiments using equipment hosting base station functionality in conjunction with mobile station functionality to examine to what extent theory hold in practice.
- look into what work is needed to make the attacks presented in this report impossible or at least harder to mount. What is the situation in the UMTS systems?

Reference

[1]. Vijaya C, Security, Authentication and access control for mobile communications, http://www.ittc.ku.edu/~rvc/documents/865/865_securityreport.pdf

[2]. Trappe W, Washington L C, Introduction to Cryptography with coding theory, Prentice Hall 2001

[3]. GSM 01.02, European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2+) (GSM), General description of a GSM Public Land Mobile Network (PLMN), 1997, http://www.etsi.org

[4]. Javier Gozalvez Sempere, An Overview of the GSM System, http://www.comms.eee.strath.ac.uk/~gozalvez/gsm/gsm.html, March 5, 2000

[5]. GSM 02.17 (ETS 300 509): European Telecommunications Standards Institute (ETSI), European digital cellular telecommunication system (Phase 2); Subscriber identity modules (SIM), Functional characteristics, http://www.etsi.org

[6]. GSM 02.16, European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase2); International Mobile station Equipment Identities (IMEI), http://www.etsi.org

[7]. Brookson C, Security and Cryptography Applications to Radio Systems, IEE Colloquium on GSM security: a description of the reasons for security and the techniques 1994

[8]. Wagner D, Cellphone Security, http://www.cs.berkeley.edu/~daw/talks/SAC02.ppt

[9]. GSM 03.20 (TS 100 929), European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2+); Security related network functions, http://www.etsi.org