Security in the GSM Network

Ammar Yasir Korkusuz

2012

Bogazici University, Electrical-Electronics Engineering Department,

MSc. Student

EE 588 – NETWORK SECURITY

TERM PROJECT

Abstract: GSM is the biggest wireless network in the world. Billions of people are using this technology and only some of them know its structure and security mechanisms. In this paper, GSM and its security mechanisms are discussed with details. Firstly, GSM history and GSM architecture are given. Secondly, GSM security measurements are mentioned. Finally, information about weakness and attacks on GSM network are stated.

Index

1 Introduction 4

2 GSM Overview 4

2.1 GSM History 4

2.2 GSM Architecture 5

2.2.1 Subscriber Identity Module (SIM) Card 7

2.2.2 Mobile Equipment (ME) 7

2.2.3 Base Transceiver Station (BTS) 7

2.2.4 Base Station Controller (BSC) 7

2.2.5 Mobile Switching Center (MSC) 7

2.2.6 Home Location Register (HLR) 7

2.2.7 Visited Location Register (VLR) 7

2.2.8 Authentication Centre (AuC) 8

2.2.9 Equipment Identity Register (EIR) 8

2.3 Subsystems and Working Principles 8

2.3.1 Mobile Station 8

2.3.2 Base Station Subsystem (BSS) 9

2.3.3 Network Subsystem (NSS) 9

2.3.4 Network Management Subsystem (NMS) 10

3 GSM Security Principles 10

3.1 Security Goals & Concerns 10

3.2 Security Mechanisms 11

3.2.1 A3 and A8 Algorithms 12

3.2.2 COMP128 16

3.2.3 A5 Algorithm 16

3.2.4 GPRS Security 19

4 Weakness of GSM Security 19

4.1 Weak sides of the Security Mechanisms ... 19
4.2 History of Cracking Algorithms ... 20
4.3 Popular Attacks Types ... 22
4.3.1 Capturing One or Several Mobile Stations ... 22
4.3.2 Attacks on the Anonymity of GSM Users ... 23
4.3.3 Attacks on the Authentication Algorithm ... 24
4.3.4 Attacks on the Confidentiality of GSM ... 26
4.3.5 Denial of Service (DoS) Attacks ... 30
5 Some Useful Solutions against Attacks ... 31
5.1.1 Using secure algorithms for A3/A8 implementations ... 31
5.1.2 Using secure ciphering algorithms ... 31
5.1.3 End-to-end Security ... 32
6 ACRONYMS ... 32
7 REFERENCES ... 33

1 Introduction

In July 2010, GSM Association announced that GSM has more than 5 billion connections. It doesn't show direct number of user because some people use multiple SIM card. It is still certain that, a lot of people use this system for communication. In GSM, there is one important issue people normally don't think, which is security.

Most of computer users know at least basic concepts of the computer security, such as virus, antivirus, trojan… Besides, more people use at least one cheap anti-virus program for security.

However, people do not even have any idea about GSM security. They blindly trust GSM systems and they do not usually think that there may be an insecure communication. People do not have to know all security mechanisms in technology but they should at least have an idea about weak and strong points in GSM and how opponents can use these weak points against them. [1]

2 GSM Overview

2.1 GSM History

1876 - First telephone was invented by Alexander Bell.

1921 - The first car mounted radio telephone worked.

1946 - First commercial mobile radio-telephone service was started by Bell and AT&T in Saint Louis, USA.

1973 - First handheld cellular phone was released by Motorola.

1978 - First cellular network was setup in Bahrain

1982 - The European Conference of Post and Telecommunications Administrations (CEPT) formed a group called Group Spéciale Mobile (GSM) to develop a European cellular system that would replace the many existing incompatible cellular systems already in place in Europe.

1987 – A milestone was achieved with the signing of the GSM Memorandum of Understanding (MoU) by operators, agreeing to implement cellular networks, based on the

GSM specifications. While it was clear from the start that GSM would be a digital system, it was officially announced in 1987.

1991 - GSM service started. In the same year, GSM was renamed to Global System for Mobile Communications from Group Spéciale Mobile.

Although GSM was initially developed as a European digital communication standard to allow users to use their cellular devices seamlessly across Europe, it soon developed into a standard that would see unprecedented growth globally. [2, 3]

GSM is a lot better system than old analog systems. Key features of GSM can be written as;

- International Roaming - single subscriber number worldwide
- Superior speech quality - better than existing analog cellular technology
- High level of security - user's information is safe and secure
- Universal and Inexpensive Mobile handsets
- Digital Convenience - talk time is doubled per battery life and digital networks can handle higher volume of calls at any one time that analog networks
- New services - such as call waiting, call forwarding, Short Message Service (SMS), GSM
- Packet Radio Service (GPRS)
- Digital compatibility - easily interfaces with existing digital networks like Integrated with Services Digital Network (ISDN)
  [3]

2.2 GSM Architecture

Cellular communication means that there are a lot of different areas, looks like cell, contain communication system devices, such as antennas, base stations… If the base station antenna power is high, it means that it serves large areas. Otherwise, if the antenna power is low, it means that it serves little areas. However there are other parameters which affect the convergence. For example, to achieve a good communication in crowded areas, convergence should be reduced and the channel capacity should be increased.

A lot of adjacent cells create the clusters. Clusters can have different amount of cells and each cell uses different frequency to avoid interference. These cluster structures repeat itself in different communication areas.

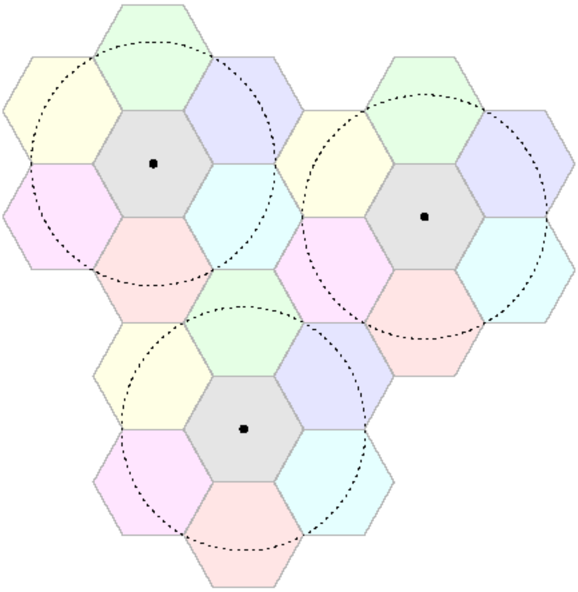


Figure 1: Cell and Cluster Structures

As it can be seen in the figure 1, different cluster cells can use the same frequency since they are far away each other and they don't make any interference.

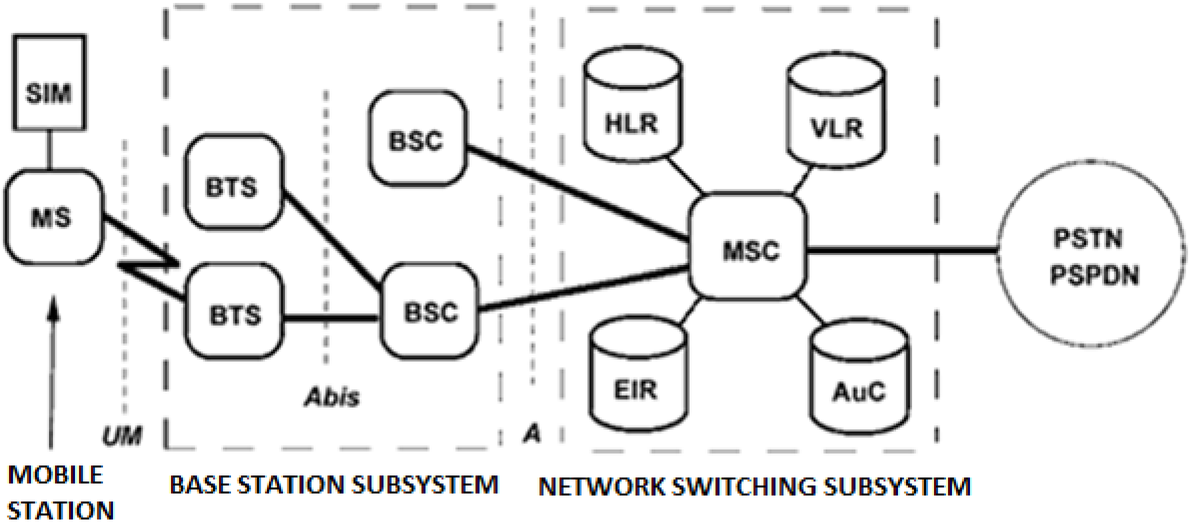


Figure 2: GSM Structure [History GSM]

Figure 2 shows each device in the GSM system. Let's take closer look each of them. [4, 5]

2.2.1 Subscriber Identity Module (SIM) Card

It is operator dependent smart card which contains A3/8 algorithms, IMSI and Ki. There will be god information about SIM card in the security chapter.

2.2.2 Mobile Equipment (ME)

It is operator independent communication device. It contains A5 algorithm. It is useless without SIM card. It never sees A3/8 algorithms and Ki.

2.2.3 Base Transceiver Station (BTS)

The Base Transceiver Station belonging to a PLMN serving the MS. Base stations form a patchwork of radio cells over a given geographic coverage area. Base Stations are connected to base station controllers (BSC).

2.2.4 Base Station Controller (BSC)

It is a node controlling a number of BTS, coordinating handovers and performing BS co-ordination not related to switching. The BSC to BTS link is in many cases a point to point microwave link. BSC are also connected to mobile switching centers (MSC) via fixed or microware links.

2.2.5 Mobile Switching Center (MSC)

It is a node controlling a number of BSC. It is center device and has a lot of function in GSM system. It makes switching, authentication, registering and links the nodes each other. It is connected to PSTN.

2.2.6 Home Location Register (HLR)

It is used for recording the most recent known location of all MS belonging to MS's home area. It contains all administrative information about each registered user of a GSM network along with the current location of the MS.

2.2.7 Visited Location Register (VLR)

It is used for recording information about all MS when they are at the "visiting" area. It tracks mobiles that are out of their home network, so that the network will know where to find them.

2.2.8 Authentication Centre (AuC)

It is used by a HLR to generate random challenges (RAND) and to store secret key information (Ki) relating to each of its MS. The AuC can be integrated with other network functions, e.g. with the HLR. The AUC database contains; International Mobile Subscriber Identity (IMSI), Temporary Mobile Subscriber Identity (TMSI), Location Area Identity (LAI), Authentication Key (Ki).

2.2.9 Equipment Identity Register (EIR)

The EIR is a database that keeps tracks of handsets on the network using the IMEI. There is only one EIR per network. It is composed of three lists; the white list, the gray list, and the black list. The black list is a list if IMEIs that are to be denied service by the network for some reason. Reasons include the IMEI being listed as stolen or cloned or if the handset is malfunctioning or doesn't have the technical capabilities to operate on the network. The gray list is a list of IMEIs that are to be monitored for suspicious activity. This could include handsets that are behaving oddly or not performing as the network expects it to. The white list is an unpopulated list. That means if an IMEI is not on the black list or on the gray list, then it is considered good and is "on the white list". [4, 5]

2.3 Subsystems and Working Principles

GSM structure has subsystems, Base Station Subsystem, Network Subsystem and Network Management Subsystem. Moreover, it has 3 interfaces; **UM** interface (air interface), **Abis** interface (between BTS and BSC), **A** interface (between BSC and MSC). [2]

2.3.1 Mobile Station

Every GSM mobile phone has a Subscriber Identity Module (SIM). The SIM provides the mobile phone with a unique identity through the use of the International Mobile Subscriber Identity (IMSI). The SIM is like a key, without which the mobile phone can't function. It is capable of storing personal phone numbers and short messages. It also stores security related information such as the A3 authentication algorithm, the A8 ciphering key generating algorithm, the authentication key (Ki) and IMSI. The mobile station stores the A5 ciphering algorithm. The SIM is removable, which allows users to travel abroad taking with them only their SIM card. They would need to inform their local provider, which countries they would be visiting, and prior to their departure. At their destination, they can simply plug the SIM into a rental cellular phone and make use of the mobile unit. The SIM can be protected with a Personal Identification Number (PIN) chosen by the subscriber. The PIN is stored on the card and if entered incorrectly thrice, the card blocks itself. At this point, you'll have to contact your cellular provider who can unblock your mobile phone, by entering an eight digit Personal Unblocking Key (PUK), which is also stored on the card. [3]

2.3.2 Base Station Subsystem (BSS)

The role of the Base Station Subsystem (BSS) is to connect the user on a mobile phone with other landline or mobile users. The Base Transceiver Station (BTS) is in direct contact with the mobile phones via the air interface and can be thought of as a complex radio modem. The Base Station Controller (BSC) is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manages radio frequencies allocated for the calls through the BTS. [3]

2.3.3 Network Subsystem (NSS)

It is a complete exchange, capable of routing calls from a fixed network via the BSC and BTS to an individual mobile station. The Mobile Services Switching Center (MSC) interconnects the cellular network with the Public Switched Telephone Network (PSTN). The MSC also serves to co-ordinate setting up calls to and from GSM users. The Home Location Register (HLR) stores information of all subscribers belonging to an area served by a MSC. It stores permanent data such as the IMSI, services subscribed by the user, subscriber's number from a public network, Ki and some other temporary data. The HLR has to provide the MSC with all the necessary information when the call is coming from a public network. The Visitor Location Register (VLR) contains relevant information for all mobiles currently served by a MSC. The permanent data stored in the VLR is also stored in the HLR. In addition, it also stores the Temporary Mobile Subscriber Identity (TMSI), which is used for limited intervals to prevent the transmission of the IMSI via the air interface. (See section on GSM Security: Anonymity) The VLR has to support the MSC during call establishment and authentication when the call originates from a mobile station. The Equipment Identity Register (EIR) stores all the International Mobile Equipment Identities (IMEI) of mobile equipment and their rights on the network. The EIR maintains a white, gray and black list. Those on the white list are permitted on the network while those on the black list are blocked from the network. The gray list consists of faulty equipment that may pose a problem on the network but are still permitted to participate on the network. The IMEI reveals the serial number of the mobile station, manufacturer, type approval and country of production. The Authentication Center

(AuC) is a protective database that houses the KI, the A3 authentication algorithm, the A5 ciphering algorithm and the A8 ciphering key generating algorithm. It is responsible for creating the sets of random numbers (RAND), Signed Response (SRES) and the Cipher key (KC), though the created sets are stored in the HLR and VLR. [3]

2.3.4 Network Management Subsystem (NMS)

The Network Management Subsystem (NMS) is the third subsystem of the GSM network in addition to the Network Switching Subsystem (NSS) and Base Station Subsystem (BSS). The purpose of the NMS is to monitor various functions and elements of the network.

The operator workstations are connected to the database and communication servers via a Local Area Network (LAN). The database server stores the management information about the network. The communications server takes care of the data communications between the NMS and the equipment in the GSM network known as “network elements”. These communications are carried over a Data Communications Network (DCN), which connects to the NMS via a router. The DCN is normally implemented using an X.25 Packet Switching Network.

The NMS functions can be divided into three categories; fault management, configuration management and performance management. [6]

3 GSM Security Principles

3.1 Security Goals & Concerns

Security mechanisms should have some features to become efficient. First of all, security concerns can be defined in two side; operator side and customer side.

Operators;

- Should bill the right person
- Should provide systems to avoid fraud
- Should protect their services against attacks

Customers;

- Should have privacy, nobody should be able to detect their identification or their location

- Communication on the air should be encrypted to avoid eavesdropping
- Should be able to change mobile equipment independently

Security mechanisms;

- Shouldn’t add much load to the voice calls or data communication
- Shouldn’t need to increase the channel bandwidth
- Shouldn’t increase the bit error rate
- Shouldn’t bring expensive complexity to the system
- Should be useful and cost efficient
- Should be able to detect suspicious mobile equipment

[7, 8]

3.2 Security Mechanisms

GSM has a lot of security systems to build safe communication. It includes a lot of different types of algorithms and different type of devices.

The main security measurements of GSM security can be written in 4 principles;

Authentication of a user; it provides the ability for mobile equipment to prove that it has access to a particular account with the operator.

Ciphering of the data and signaling; it requires that all signaling and user data (such as text messages and speech) are protected against interception by means of ciphering.

Confidentiality of a user identity; it provides IMSI’s (international mobile subscriber identity) security. GSM communication uses IMSI rarely, it uses TMSI (Temporary Mobile Subscriber Identity) to provide more secure communication and to avoid disclosing of user’s identity. This means someone intercepting communications should not be able to learn if a particular mobile user is in the area.

Using SIM as security module; Incase SIM card was taken by opponent, there is still PIN code measurement.

[4, 5, 9]

3.2.1 A3 and A8 Algorithms

A3 and A8 algorithms are A3 and A8 algorithms are symmetric algorithms which the encryption and decryption use the same key. Both of the algorithms are one way function, it means that output can be found if the inputs are known but it is mostly impossible to find inputs incase the output is known. A3 and A8 algorithms are kept and implemented in SIM card. [10, 11]

Many users of GSM will be familiar with the SIM (Subscriber Identity Module) the small smartcard which is inserted into a GSM phone as you can see in the figure 3.

Figure 3: Sample SIM Card

The SIM itself is protected by an optional PIN code. The PIN is entered on the phone’s keypad, and passed to the SIM for verification. If the code does not match with the PIN stored by the SIM, the SIM informs the user that code was invalid, and refuses to perform authentication functions until the correct PIN is entered. To further enhance security, the SIM normally “locks out” the PIN after a number of invalid attempts (normally 3). After this, a PUK (PIN Unlock) code is required to be entered, which must be obtained from the operator. If the PUK is entered incorrectly a number of times (normally 10), the SIM refuses local access to privileged information (and authentication functions) permanently, rendering the SIM useless.

Typical SIM features can be lined as below:

- 8 bit CPU
- 16 K ROM
- 256 bytes RAM
- 4K EEPROM
- Cost: $5-50

On its own, the phone has no association with any particular network. The appropriate account with a network is selected by inserting the SIM into the phone. Therefore the SIM card contains all of the details necessary to obtain access to a particular account. It contains 4 important information; IMSI, Ki, A3 and A8 algorithms. [9]

IMSI (International Mobile Subscriber Identity): Unique number for every subscriber in the world. It includes information about the home network of the subscriber and the country of issue. This information can be read from the SIM provided there is local access to the SIM (normally protected by a simple PIN code). The IMSI is a sequence of up to 15 decimal digits, the first 5 or 6 of which specify the network and country.

Ki: Root encryption key. This is a randomly generated 128-bit number allocated to a particular subscriber that seeds the generation of all keys and challenges used in the GSM system. The Ki is highly protected, and is only known in the SIM and the network's AuC (Authentication Centre). The phone itself never learns of the Ki, and simply feeds the SIM the information it needs to know to perform the authentication or generate ciphering keys. Authentication and key generation is performed in the SIM, which is possible because the SIM is an intelligent device with a microprocessor.

A3 Algorithm: It provides authentication to the user that it has privilege to access the system. The network authenticates the subscriber through the use of a challenge-response method.

Firstly, a 128 bit random number (RAND) is transmitted to the mobile station over the air interface. The RAND is passed to the SIM card, where it is sent through the A3 authentication algorithm together with the KI. The output of the A3 algorithm, the signed response (SRES) is transmitted via the air interface from the mobile station back to the network. On the network, the AuC compares its value of SRES with the value of SRES it has received from the mobile station. If the two values of SRES match, authentication is successful and the subscriber joins the network. The AuC actually doesn't store a copy of SRES but queries the HLR or the VLR for it, as needed. [3]

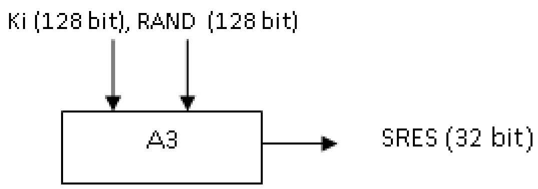


Figure 4: A3 Algorithm

Figure 4 illustrates working principle of A3 algorithm.

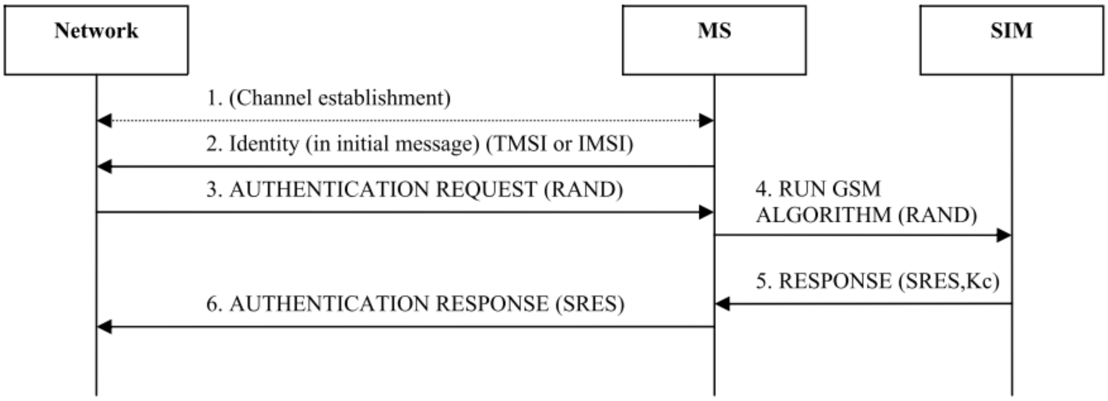

Network
MS
SIM
1. (Channel establishment)
2. Identity (in initial message) (TMSI or IMSI)
3. AUTHENTICATION REQUEST (RAND)
4. RUN GSM ALGORITHM (RAND)
5. RESPONSE (SRES,Kc)
6. AUTHENTICATION RESPONSE (SRES)

Figure 5: A3 Algorithm Request Order

Figure 5 shows the request order between mobile station and operator network in A3 algorithm. This figure can be explained as;

1) Some connection is attempted between the phone and the network.
2) The phone submits its identity. All potential messages used at the start of a connection contain an identity field. Where possible, it avoids sending its IMSI in plaintext (to prevent eavesdroppers knowing the particular subscriber is attempting a connection). Instead, it uses its TMSI (Temporary Mobile Subscriber Identity). This will be discussed later in this article.
3) The network sends the AUTHENTICATION REQUEST message containing the RAND.
4) The phone receives the RAND, and passes it to the SIM, in the RUN GSM ALGORITHM command.
5) The SIM runs the A3 algorithm, and returns the SRES to the phone.

6) The phone transmits the SRES to the network in the AUTHENTICATION RESPONSE message.
7) The network compares the SRES with its own SRES. If they match, the transaction may proceed. Otherwise, the network either decides to repeat the authentication procedure with IMSI if the TMSI was used, or returns an AUTHENTICATION REJECT message.

[9]

A8 Algorithm: GSM makes use of a ciphering key to protect both user data and signaling on the vulnerable air interface. Once the user is authenticated, the RAND (delivered from the network) together with the Ki (from the SIM) is sent through the A8 ciphering key generating algorithm, to produce a ciphering key (Kc). The A8 algorithm is stored on the SIM card. The Kc created by the A8 algorithm, is then used with the A5 ciphering algorithm to encipher or decipher the data. The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data on the air. [3]

Whenever the A3 algorithm runs to generate SRES, the A8 algorithm is run as well The A8 algorithm uses the RAND and Ki as input to generate a 64-bit ciphering key, the Kc, which is then stored in the SIM and readable by the phone. The network also generates the Kc and distributes it to the base station (BTS) handling the connection [9].

Figure 6 shows A8 algorithm working principle;

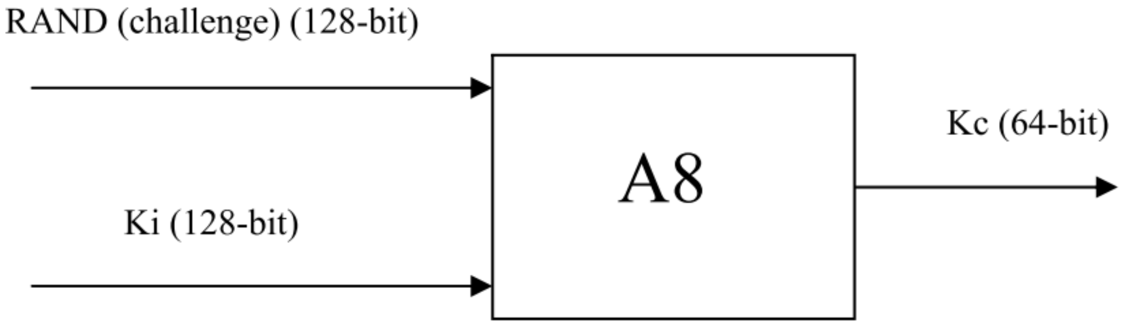


Figure 6: A8 Algorithm

3.2.2 COMP128

COMP128 is hash function which is an implementation of the A3 and A8 algorithms in the GSM standard.

The Algorithm Expert Group was held in 1987 and designed GSM encryption algorithms. They created 2 algorithms; the first one was COMP128 which is to provide authentication and derive the cipher key (A3/8), the second was A5 algorithm. GSM allowed every operator to use its own A3/8 algorithm and the all system support this without transferring between networks, also during roaming. However, most of the operators do not have expertise to make their own A3/8 algorithm design and they use example COMP128 design. [12]

The COMP128 takes the RAND and the Ki as input; it generates 128 bits of output. The first 32 bits of the 128 bits form the SRES response; the last 54 bits of the COMP128 output form the session key, Kc. Note that the key length at this point is 54 bits instead of 64 bits, which is the length of the key given as input to the A5 algorithm. Ten zero-bits are appended to the key generated by the COMP128 algorithm. Thus, the key of 64 bits with the last ten bits zeroed out. This effectively reduces the key space from 64 bits to 54 bits. This is done in all A8 implementations, including those that do not use COMP128 for key generation, and seems to be a deliberate feature of the A8 algorithm implementations. [13]

3.2.3 A5 Algorithm

A5 is a stream cipher which can be implemented very efficiently on hardware. There exist several implementations of this algorithm, the most commonly used ones are A5/0, A5/1 and A5/2 (A5/3 is used in 3G systems). The reason for the different implementations is due to export restrictions of encryption technologies. A5/1 is the strongest version and is used widely in Western Europe and America, while the A5/2 is commonly used in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption. [3, 14]

As a stream cipher, A5 works on a bit by bit basis (and not on blocks, as DES and AES). So, an error in the received cipher text will only result in the corresponding plaintext bit being in error.

None of the algorithms are published by GSM Association. They are all discovered by using reverse engineering methods**.**

A5/1 algorithm uses the structure which can be seen in figure 8. [9]

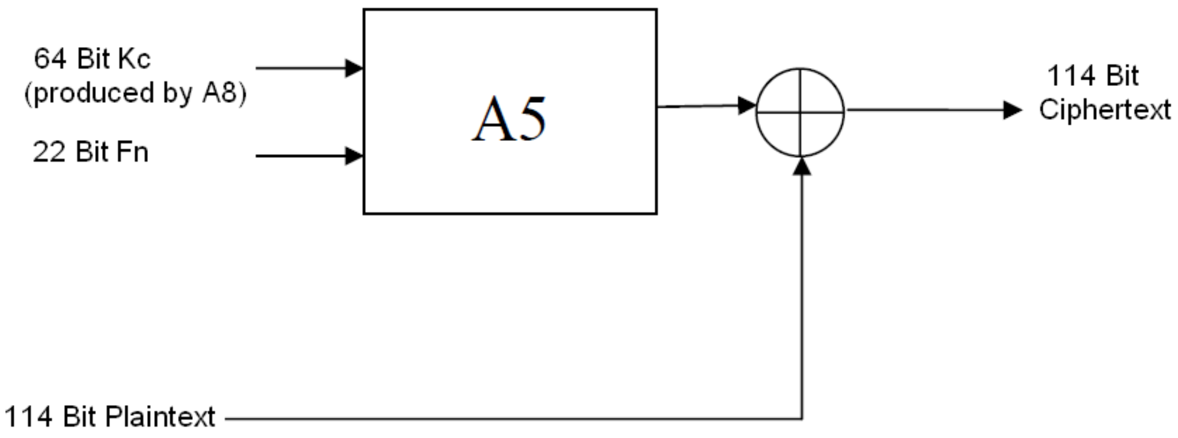


Figure 7: A5 Structure

Kc is the key which was produced by A8 algorithm. Plaintext is the data which is wanted to transmit. Fn is the frame bits which come from **LFSR** (Linear Feedback Shift Register) process.

To understand A5/1 algorithm, **LFSR** (Linear Feedback Shift Register) structure should be introduced firstly.

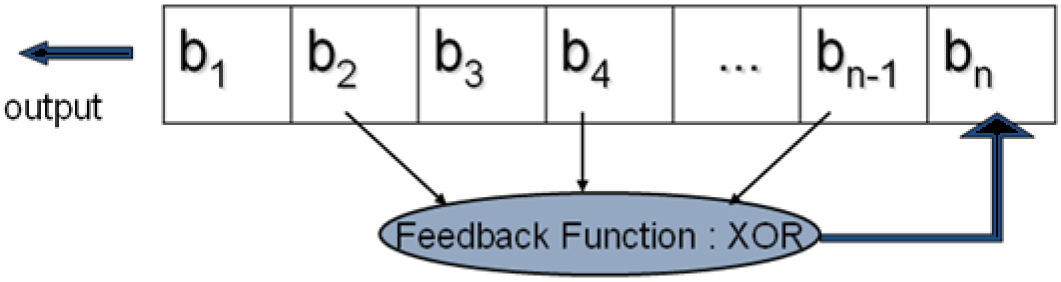


Figure 8: LFSR Structure

As it can be seen in the figure 7, in LFSR structure, there is certain amount of bits which has some special bits (taps). These special taps are XOR ed, all the bits shit one bit left and the result was put to the first bit. [14]

In A5/1 algorithm, LFSR structure uses 3 register bits. These bits are shown in the figure 9.

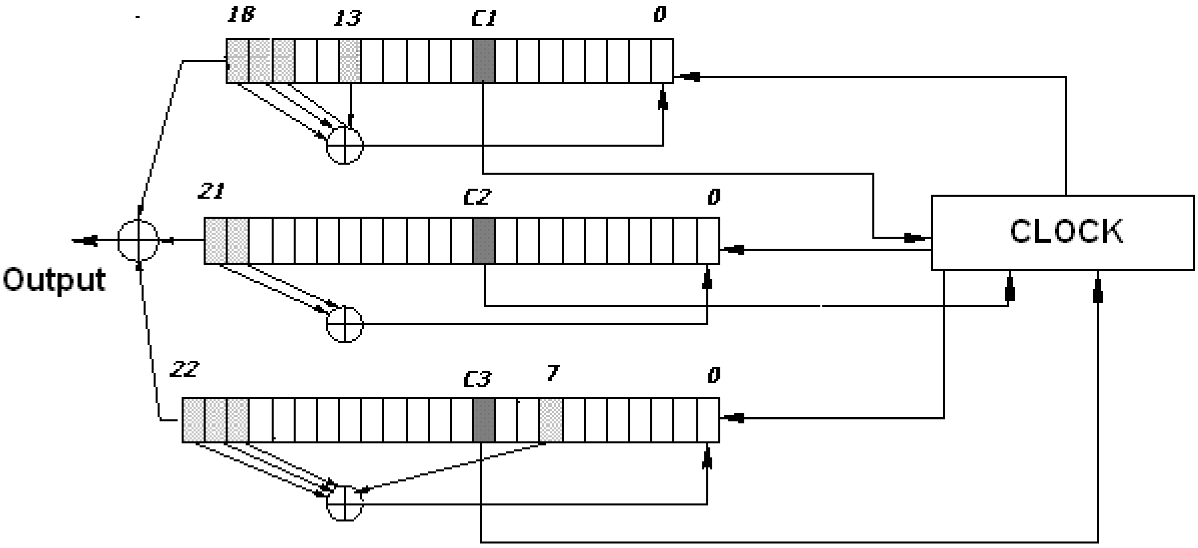


Figure 9: LFSR Structure in A5/1 Algorithm

A5/1 is built from three short linear feedback shift registers (LFSR) of lengths 19, 22, and 23 bits, which are denoted by *R*1, *R*2 and *R*3 respectively. The rightmost bit in each register is labeled as bit zero. The taps of *R*1 are at bit positions 13, 16, 17, 18; the taps of *R*2 are at bit positions 20, 21; and the taps of *R*3 are at bit positions 7, 20, 21, 22. When a register is clocked, its taps are XOR ed together, and the result is stored in the rightmost bit of the left-shifted register. The three registers are clocked in a stop/go fashion using the following majority rule: Each register has a single "clocking" tap (bit 8 for *R*1, bit 10 for *R*2, and bit 10 for for *R*3); each clock cycle, the majority function of the clocking taps is calculated and only those registers whose clocking taps agree with the majority bit are actually clocked. Note that at each step either two or three registers are clocked, and that each register moves with probability 3/4 and stops with probability 1/4.

The process of generating pseudo random bits from the session key Kc and the frame counter Fn is carried out in four steps:

1. The three registers are zeroed, and then clocked for 64 cycles (ignoring the stop/go clock control). During this period each bit of Kc (from least significant bit to most significant bit) is XOR ed in parallel into the lsb's of the three registers.
2. The three registers are clocked for 22 additional cycles (ignoring the stop/go clock control). During this period the successive bits of *Fn* (from lsb to msb)

are again XOR'ed in parallel into the lsb's of the three registers. The contents of the three registers at the end of this step are called the initial state of the frame.

3. The three registers are clocked for 100 additional clock cycles with the stop/go clock control but without producing any outputs.
4. The three registers are clocked for 228 additional clock cycles with the stop/go clock control in order to produce the 228 output bits. At each clock cycle, one output bit is produced as the XOR of the msb's of the three registers. 114 bits of these 228 bits are used in MS-BTS communication and the rest 114 bits are used in BTS-MS communication. [15]

A5/2 is the weak version of A5/1. Different from A5/1, it contains 4 LFSR bits Time complexity of the A5/1 is 2^{54} (if the last 10 bits of the Kc is not zero, then 2^{64}). However, time complexity of A5/2 is 2^{16}. A5/0 is the weakest version between these 3 algorithms. It doesn’t make any encryption. [11]

3.2.4 GPRS Security

The security in GPRS is based on the same mechanisms as of GSM. However, GPRS uses a different encryption key to provide security. To authenticate the customer, the same A3/8 algorithms are used with the same Ki, different RAND. The resulting Kc is different than voice communication key and this Kc is used to encrypt GPRS data. This Kc is refered GPRS-Kc to make it different from voice communication Kc. Similarly, SRES and RAND are referred as GPRS-SRES and GPRS-RAND. GPRS cipher is also referred to GPRS A5 or GEA (GPRS Encryption Algorithm). [16]

4 Weakness of GSM Security

4.1 Weak sides of the Security Mechanisms

GSM doesn’t have perfect security system. Opponents can eavesdrop the channel in real time. The weak sides of GSM Security mechanisms will be discussed in this chapter.

First of all, most of the operators do not have expertise enough to create new A3/8 algorithms. So they use COMP128 function without even changing it. This is big security problem because all the COMP128 function has found by reverse engineering.

The bit size of the algorithms is weak. A5/1 algorithm uses 64 bit Kc in the best case. Most operators use COMP128 which has 54 bit Kc and last 10 bits are always zero. Also A5/2 is weaker than A5/1.

Moreover, authentication query only exists BTS-MS communication. There is no authentication for MS-BTS. It means that, fake base stations can behave like real BTS and MS will answer each SRES request from them. The network does not authenticate itself to a phone. This is the most serious fault in GSM security, which allows a man-in-the-middle attack. This weakness was known for GSM constructors at the time of the GSM design, but it was expected that building a false BTS would be too expensive and it would be difficult to make those attacks cost effective. However, after 20 years the situation changed significantly. Today there are companies that product short range BTS, so an attacker can simply buy a BTS at a reasonable price.

Another serious vulnerability of the GSM is the lack of proper Caller ID or Sender ID verification. In other words, the caller number or SMS sender number could be spoofed. The caller ID and the voice is transmitted in different channels. So, Called ID or SMS ID can be spoofed.

Another weakness attackers can exploit is vulnerability in the IMSI protection mechanism. As mentioned before, networks use TMSI to protect IMSI but if the network somehow loses track of a particular TMSI it must then ask the subscriber their IMSI over a radio link. The connection cannot be ciphered because the network does not know the identity of the user, and thus the IMSI is sent in plain text. The attacker can thus check whether a particular user (IMSI) is in the vicinity. [1]

4.2 History of Cracking Algorithms

In April 1998, the Smartcard Developer Association (SDA) together with two U.C. Berkeley researchers claimed to have cracked the COMP128 algorithm stored on the SIM. By sending large number of challenges to the authorization module, they were able to deduce the K_i within several hours. They also discovered that K_C uses only 54 bits of the 64 bits. The remaining 10 bits are replaced by zeros, which makes the cipher key purposefully weaker. They feel this is due to government interference. A weaker ciphering key, could potentially allow governments to monitor conversations.

The SDA had the SIM in their physical presence when they cracked the algorithm. However they fear “an over the air attack” is not farfetched. Unfortunately, they are unable to confirm their suspicions, as the equipment required to carry out such an attack is illegal in the US. The GSM Alliance responded to the incident, stating even if a SIM could be cloned it would serve no purpose, as the GSM network would only allow only one call from any phone number at any one time. GSM networks are also capable of detecting and shutting down duplicate SIM codes found on multiple phones.

In August 1999, an American group of researchers claimed to have cracked the weaker A5/2 algorithm commonly used in Asia, using a single PC within seconds.

In December 1999, two leading Israeli cryptographers claimed to have cracked the strong A5/1 algorithm responsible for encrypting conversations. They admit the version they cracked may not be the exact version used in GSM handsets, as GSM operators are allowed to make small modifications to the GSM algorithms. The researchers used a digital scanner and a high end PC to crack the code. Within two minutes of intercepting a call with a digital scanner, the researchers were able to listen to the conversation. In the US, digital scanners are illegal. The GSM Alliance of North America has claimed that none of its members use the A5/1 algorithm, opting for more recently developed algorithms.

In May 2002, The IBM Research group discovered a new way to quickly extract the COMP128 keys using side channels. As it can be seen in the figure 10 and figure 11, side channels are the natural features of the devices such as power consumption, electromagnetic radiation, timing, errors… [3, 8]

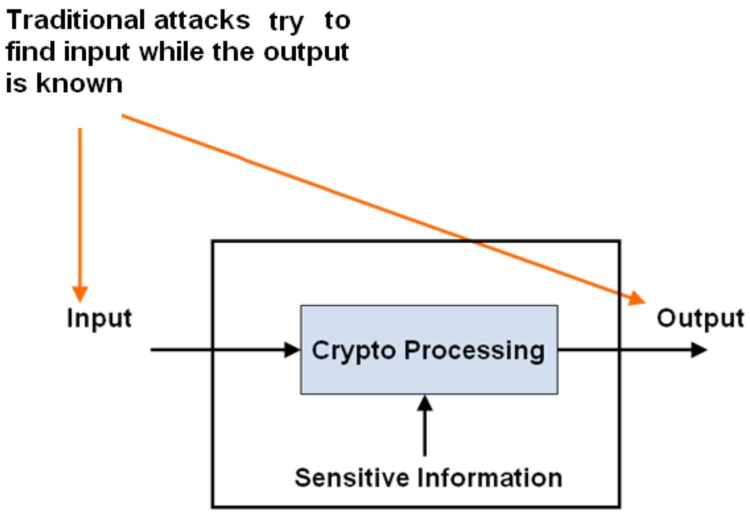

Traditional attacks try to find input while the output is known
Input
Output
Crypto Processing
Sensitive Information

Figure 10: Traditional Attacks

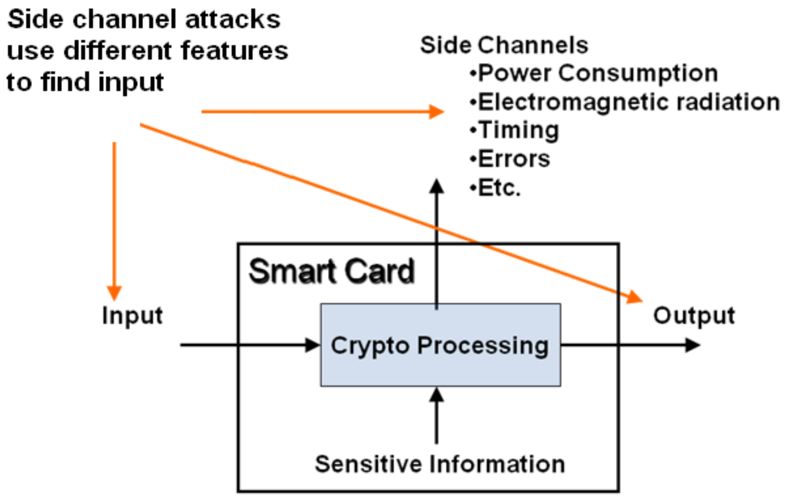


Figure 10: Side Channel Attacks

4.3 Popular Attacks Types

In this chapter, it will be described the significant attacks to the anonymity, authentication and confidentiality.

4.3.1 Capturing One or Several Mobile Stations

In many of the attacks described in this chapter, the attacker needs to pretend the network to the MS or pretending the MS to the network or both in a so called man-in-the middle attack. An attacker impersonating BS and MS to each other can eavesdrop, modify, and erase, order, replay, spoof and relaying signals/user data between two communicating entities. The required equipment is an adjusted and modified BTS and MS bundle. The modified BTS behaves as the identity the network to the MS, while the modified MS impersonates the MS to the network.

This mechanism can be seen in figure 11 below.

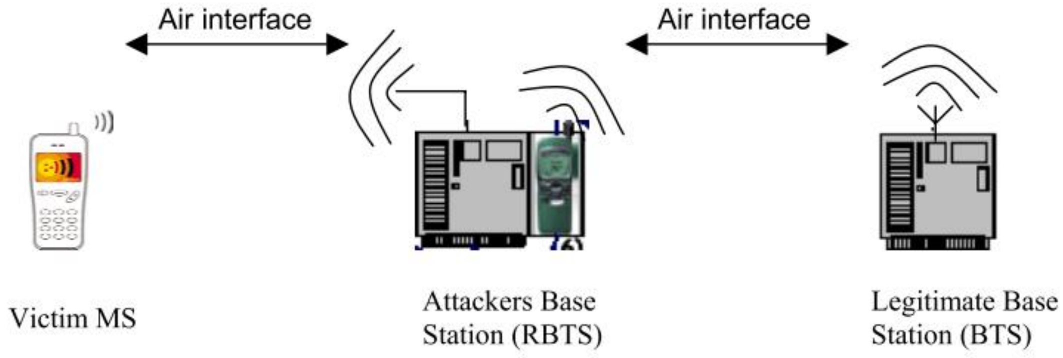


Figure 11: Man-in-Middle mechanism

Before an active attack, the attacker may have to eavesdrop the MS. The attacker may want to learn the information consists of cell identity, network identity, and control channel structure, list of channels in use and details of the access protocol. In this manner, an attacker with a Fake BTS, providing higher power levels than the BTS, between the victim MS and legitimate BTS, forces the MS use the FBTS. The MS captured by the attacker who controls what messages go between the MS and BTS as well as messages flowing in the other direction. After capturing MS identity, the attacker will then use this to provide fabricated messages on behalf of a legitimate subscriber.

4.3.2 Attacks on the Anonymity of GSM Users

The anonymity in GSM is provided by using temporary identifier TMSI, which is like a nickname of subscriber locally. An attacker may want some subscriber's movements and/or pursue call samples and so must have the IMSI and the TMSI of the MS. This information may also be used to attack other security assets than anonymity, for instance eavesdropping on a specific person. If the attacker can get the IMSI of subscriber or associated current TMSI of a specific person then the anonymity of the user is imperiled.

Passive Monitoring:

Every time a MS is powered on, MS is required to introduce itself to the network. This is performed by an IMSI attach. IMSI attach occurs in case of location update. Since the IMSI is not registered in the network and there is not yet any authentication, an encryption cannot be applied. Therefore the IMSI is sent in the clear. An attacker listening to the air traffic can extract the IMSI and associated subscriber's being active.

Passively track GSM users and eavesdropping on the users' permanent identity (IMSI) is possible and easy. This information provides the attacker with a functional IMSI and the knowledge of that the owner of IMSI is in the present area. Passive monitoring is however inefficient and time-consuming since the attacker needs to either wait for MSs to perform IMSI attach when it is powered on or for a database failure to occur in the network, which probably does not happen so frequently.

Active Monitoring:

To track a GSM subscriber, the attacker can make use of the identification procedure. The network may initiate an identification procedure, if the network cannot identify the MS using its TMSI. The identification procedure begins with transmitting an IDENTITY REQUEST message to MS so as to ask it to transmit an identification parameter. The network can request IMSI, IMEI or TMSI. Since GSM does not use message authentication to check message origin on the radio link, an attacker with sufficient base station functionality can use these messages to retrieve the same information as a legitimate base station by deceiving the target MS s.

It should be possible to request from a subscriber (whose IMSI is known by attacker) for his/her TMSI abusing the identification procedure. When the attacker knows the IMSI/TMSI bundle, it is possible to locate a specific subscriber. The attacker simply pages the MS with the specific IMSI/TMSI.

4.3.3 Attacks on the Authentication Algorithm

Many GSM operators use the design specification given in the GSM MoU, COMP128, instead of designing their own algorithm for authentication (A3) and session key generation (A8). The difficulty in starting to create new algorithm is that subscribers who bought SIMs before eventual introduction of a different algorithm, are forced to use their old SIMs with the old algorithm. Other reason to change/revise the algorithm is the cost of changing software in database etc. On the other hand, it is possible to utilize new and more secure versions of COMP128 in new SIMs that are given to new subscribers.

The design of COMP128 was never made public, but the design has been reverse engineered and cryptanalyzed. Today, it is quite easy to find software implementation of

COMP128 by simple search on internet. Since the GSM specification for SIM cards is widely available, all that is needed to clone a SIM card is the 128 bit COMP128 secret key Ki and the IMSI which is coded in the SIM. [17]

By copying Ki and IMSI into an empty SIM (easy to buy from web) the attacker can authenticate himself to the network as the legitimate subscriber and thus call by charging. The attacker can even, instead of using the subscription, use the captured key Ki for decrypting all the calls from and to the subscriber.

Cloning can be done either by physical access to the SIM to be cloned, or over the air. The following subsections will examine the two cases:

Cloning with Physical Access to the SIM Module:

If the attacker has physical access to the SIM module, several attacks can be launched in order to clone the module. Some of these attacks base on using flows in the cryptographic algorithm resided in the smart card, while others use vulnerabilities in the smart card itself.

The most popular attack to SIM modules is the attacks to the cryptographic algorithm (COMP128) itself. It is a chosen-challenge attack and use flows in the hashing function to deduce the secret key Ki. The attacker creates a number of specially-chosen challenges and queries the SIM for each one. The SIM applies COMP128 to its secret key and the chosen challenge, returning a response back. After analyzing the responses, the attacker can determine the Ki. The result of this attack is thus that the attacker gains access to the secret key Ki of the MS. The attack exploits a lack of diffusion, which means that some parts of the output hash depend only on some parts of the input to the algorithm. Mounting this attack requires, apart from having physical access to the target SIM, an off-the-shelf smartcard reader, and a computer to direct the operation. The attack requires one to query the SIM about 150,000 times; an average SIM reader can issue 6.25 queries per second, so the whole attack takes approximately 8 hours. By overclocking the SIM or using a higher frequency oscillator on the SIM card reader the processing time could be reduced considerably. This increases however the risk of failure and damage to the original SIM. [18, 19]

Cloning over the Air:

The attacker can even perform the attack over the air, making use of a fake base station. Apart from this equipment, the attacker needs to know the target IMSI or TMSI. The captured MSs will be immediately forced to make a location update request which is conducted. After the channel allocation is completed the attacker initiates an authentication process. Immediately after the attacker has a challenge-response pair, he/she initiates a new authentication procedure. The MS is required to respond to every challenge made by the GSM network. This process continues until the attacker has got the required number of pairs to be able to initiate the cloning procedure.

It is assumed that the channel establishment stage only has to be done once. The number of frames exchanged between the network and an MS, for one authentication process, are approximately 66 frames. Since the duration of one TDMA frame is 4.610 ms, the duration of the whole signaling sequence is 4.615 ms/frame x 66 frames = 0.30459 s. The time it takes to get the number of challenge-response pairs needed for the attack can be calculated. It is known that the cryptographic attack requires approximately 150 000 challenge-response pairs. This means that the attack takes approximately 45,689 seconds (150 000 challenges x 0.30459 s), that is approximately 13 hours. This means that the MS has to be available to the attacker over the air for the whole time it takes to gather the information. This is quite unrealistic, because people use their mobiles to make calls or receive calls in addition to the fact that such a bombardment with challenges may cause the battery of the MS to run out, which would make the victim suspicious. To get rid of these problems, the attack can be performed in parts; instead of performing a 13-hour attack, the attacker could interrogate the MS for 30 minutes every day. In that way, the battery would not run out and there would be less risk of making the owner or the legitimate network suspicious.

The defense against cloning over the air is to limit the number of times a SIM can be authenticated to a number significantly smaller than 150 000. The SIM locks up if the limit is exceeded. The drawback about this solution is that a new SIM module has to be issued and distributed to the subscriber, which results in costs both for the subscriber and the operator. [12]

4.3.4 Attacks on the Confidentiality of GSM

As mentioned before, the over-the-air privacy of GSM telephone conversations is protected using the A5 stream cipher. This algorithm has two main variants: A5/1 is the “strong” export-limited version used by CEPT-countries, and A5/2 is the “weak” version that has no export limitations. The exact design of both A5/1 and A5/2 was reverse engineered by Briceno from an actual GSM telephone in 1999. [21]

In the following subsections attacks are classified into three: brute-force attacks, crypto analytical attacks, and non-crypto analytical attacks.

Brute-Force Attacks:

The confidentiality of GSM is protected by the secrecy of Kc. Kc is 64 bits although the last 10 bits are set to zero. This reduces the key space from 2^64 to 2^54. A5/2 was developed with assistance from the NSA, and can be broken in real time with a work factor of approximately 2^16. A5/1, the stronger of the two variants, is however susceptible to attacks that can break it with a work factor of 2^40.

Pentium 4 chip has nearly 60 million transistors and the implementation of one set of LFSRs (A5/1) would require about 2000 transistors, 30.000 parallel A5/1 implementations on one chip can be done. If the chip was clocked to 3.2 GHz (a rather ambitious assumption) and each A5/1 implementation would generate one output bit for each clock cycle then it is needed to generate 100+114+114 output bits, hence approximately 10M keys per second per A5/1 implementation can be used. A key space of 2^54 would thus require about 18 hours, using all of the parallel implementations on the chip. If the attack in the average case succeeds after searching half of the key space, the key is found in about 9 hours. Further optimization by giving up on a specific key after the first invalid key stream bit and distributing the computation between multiple chips will decrease the computation time by several magnitudes. This, still in the worst case, means several hours/many minutes of processing and is far away from a real-time attack. Bear in mind that the complexity of the attack is even greater due to the fact that it is quite difficult to determine when the key is found due to the nature of the plaintext. [22, 23]

To conclude, it is too difficult to succeed in a brute-force attack in real-time, but it is fully possible to find a key given a couple of hours. Entities with enough resources (computation power) can probably cut the processing time greatly.

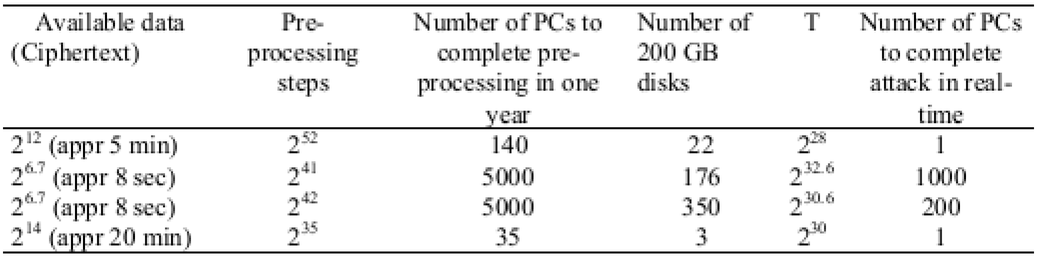
Even though a brute-force attack may not be used as a real-time attack on the A5 algorithm, it could easily be used to find the key used in a specific conversation “offline”. The attacker intercepts and records the interesting conversation and decrypts it at a later time.

Crypto Analytical Attacks:

There exist several crypto analytical attacks against the algorithms protecting different aspects of GSM. The algorithm used by many operators to authenticate subscribers (COMP128) is broken due to flaws in the design of the hash function. The result is the ability of intruders to clone subscriptions either by having physical access to the target SIM or over the air. The most popular attack requires physical access to the SIM to clone and is completed in about 8 hours. It can be speeded up with the risk of damaging the SIM. The most efficient way to clone a GSM smartcard is a partitioning attack proposed by a team from IBM. It requires challenging the target SIM only 8 times in the best case, which means that cloning can be done in minutes or even seconds. The equipment needed to mount this attack (a specially designed smartcard reader and software) is however only available in laboratories yet. Newer versions of COMP128 has been developed and distributed. It is however not known to what extent these stronger versions have been adapted by operators. A guess is that many operators still use the old algorithm due to the costs involved in upgrading. What is known for sure is that users who had COMP128 inside their SIMs when they bought a subscription are still using COMP128.

There exist several crypto analytical propositions on how to attack the encryption algorithms used for confidentiality protection that break these algorithms in real-time. Several attacks against A5/1 and A5/2 exist, although most of them have only theoretical value. Most of the attacks require that the attacker knows portions of the key stream. It is possible to obtain small portions of plaintext because the attacker often knows the structure and content of the signaling messages (especially if the attacker is impersonating the network to the victim MS and is thereby able to query the MS for information) in addition to the fact that channel coding is applied to the data before encryption. An attacker mounting a man-in-the-middle attack may ask the victim subscriber to transmit certain signaling messages (of which the content is known or almost known) after encryption has started. The attacker then has access to the cipher-text in addition to the known portions of the plaintext and can thereby derive portions of the key stream used in the encryption process. It is, however, hard to obtain the amounts of the known plaintext that some of these attacks require. The attack that requires least known plaintext is an attack against A5/2. It requires that the attacker knows the plaintext of two frames approximately six seconds apart from each other and finds the session key in about 10 ms. The known plaintext requirement may be possible to satisfy using the method mentioned earlier, therefore this attack on A5/2 has been used in one of the attacks on confidentiality. It is worth mentioning that it only took a couple of hours to crack A5/2, which illustrates the weaknesses of this algorithm.

The most recent attack on A5/1 is a cipher-text-only attack. This is an impressive attack only requiring knowledge of a small number of encrypted frames, enabling the attacker to listen to the “encrypted” conversation data, in real-time. Further the authors (of [15]) propose a ciphertext-only attack on A5/2 that improves the previous attack on A5/2 to a ciphertext-only attack. The problem of known plaintext is no longer a concern using this attack. This is however an attack requiring huge amounts of computation power. Figure 12 below gives an idea of the computation requirements in the proposed ciphertext-only attack on A5/1. [15]



Available data (Ciphertext)	Pre-processing steps	Number of PCs to complete pre-processing in one year	Number of 200 GB disks	T	Number of PCs to complete attack in real-time
2^{12} (appr 5 min)	2^{52}	140	22	2^{28}	1
$2^{6.7}$ (appr 8 sec)	2^{41}	5000	176	$2^{32.6}$	1000
$2^{6.7}$ (appr 8 sec)	2^{42}	5000	350	$2^{30.6}$	200
2^{14} (appr 20 min)	2^{35}	35	3	2^{30}	1

Figure 12: Three possible tradeoff points in the attacks on A5/1

Since this is a ciphertext only attack, no plaintext is required in order to find the session key in real-time. However, the computation and storage requirements for this attack are very high making it very unlikely that an individual hacker would have the needed resources to mount the attack. The requirements for the ciphertext-only cryptanalysis of A5/2 are however fulfilled by most personal computers of today.

Non-Crypto Analytical Attacks:

It is common knowledge that most GSM mobile phones can communicate with most different base stations and networks. This is possible because all of the different manufacturers follow the specifications and standards of how GSM should function. These specifications are developed by the European Telecommunications Standards Institute (ETSI). It is possible to study the specifications on how the communication between the network and the MS is conducted, and get detailed information on the communication protocols and mechanisms used when a MS is to be authenticated by the network.

The same key Kc is used for the different encryption algorithms A5/1, A5/2, and A5/3. This means that breaking one of this three algorithms and retrieving the session key threatens the confidentiality of the conversation even when the stronger versions of the algorithm are used later.

A base station does not need to authenticate itself to the MS it is communicating with. Furthermore messages are not authenticated and their integrity is not protected.

4.3.5 Denial of Service (DoS) Attacks

DoS attacks can be performed by physically disturbing radio signals or by logical means. These two possibilities will be explained further in the two sections below.

Denial of Service – Physical Intervention

The physical attacks are the most straight forward attacks. The attacker prevents user or signaling traffic from being transmitted on any system interface, whether wired or wireless, by physical means. An example of physical intervention on a wired interface is wire cutting. The attacker could for example cut the wire leaving a base station. An example of physical intervention on a wireless interface is jamming. Having the equipment that jam GSM radio signals is sufficient. The equipment is placed in the area where traffic is to be disturbed and the GSM equipment within the device's range will not function properly. Note that the frequency hopping makes the jamming more difficult than usual.

There are examples of jamming causing problems for GSM operators. Recently a GSM operator in Moldova suffered heavily from jamming activities that effectively caused a drop rate of lost calls of about 7 %. The operator and the authorities had major problems in stopping the attacks. [25]

Denial of Service – Logical Intervention

An attacker can perform DoS attacks by logical means also as the following examples show:

- The attacker spoofs a de-registration request (IMSI-detach) to the network. The network de-registers the subscriber from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for other subscribers. The attacker needs a modified MS and the IMSI of the user to de-register.

- The attacker spoofs a location update request in a different location area from the one in which the subscriber is roaming. The network registers the subscriber in the new location area and the target user will be paged in that new area. The user is subsequently unreachable for mobile terminated services.
- An attacker in possession of a modified base station, transmitting the base channel with higher signal strength will force the MSs in the area to camp on the radio channels of the false base station, making them unreachable for the serving network. [24]

5 Some Useful Solutions against Attacks

Regardless of security improvements in generation networks, it is necessary to provide solutions to improve the security of the currently available 2G systems. Some practical solutions are discussed in the below. [20]

5.1.1 Using secure algorithms for A3/A8 implementations

This can thwart the dangerous SIM card cloning attack. This solution is profitable since the network operators can perform such improvement themselves and without any need to the software and hardware manufacturers or the GSM consortium. However, this solution requires providing and distributing new SIM cards and modifying the software of the HLR. Currently, both COMP128-2 and COMP128-3 algorithms thwart the SIM card cloning and over-the-air cracking of Ki. Since COMP128-3 enhances the effective key length of the session key to further 10 bits, it allows the deployed cryptographic algorithm to have its nominal security. Although it is soon to judge on the real security of COMP128-2 and COMP128-3, they have apparent advantages over the traditional COMP128-1 that its SIM cloning apparatus are available at very low prices.

5.1.2 Using secure ciphering algorithms

Operators can use newer and more secure algorithms such as A5/3 provided that such improvements are allowed by the GSM consortium. The deployed cryptographic algorithms should be implemented on both BTS and mobile phones. Any change to the cryptographic algorithms requires agreement and cooperation of software and hardware manufacturers since they should perform the appropriate changes to their products. Since the cryptographic algorithms should be implemented on the cellular phones, the agreement of mobile phone manufacturers is also required. However, a lonely upgrading of the deployed cryptographic algorithms cannot be so useful. Even though the ciphering algorithms are replaced with the strongest ones, the attacker can simply impersonate the real network and force MS to deactivate the ciphering mode so it is also necessary to modify the authentication protocols.

5.1.3 End-to-end Security

The best, easiest, and most profitable solution is to deploy the end-to-end security or security at the application layer. Most of GSM security vulnerabilities (except SIM cloning and DoS attacks) do not aim ordinary people, and their targets are usually restricted to special groups so it is reasonable and economical that such groups make their communications secure by the end-to-end security. Since the encryption and security establishment is performed at the end-entities, any change to the GSM hardware will not be required. In this way, even if the conversation is eavesdropped by the police or legal organizations, they cannot decrypt the transmitted data without having the true ciphering key, provided that a secure enough cryptographic algorithm is deployed. Therefore, in order to avoid illegal activities, it should be transparent to both GSM operator and service provider.

[20]

6 ACRONYMS

A3: Authentication Algorithm

A5: Ciphering Algorithm

A8: Ciphering Key Generating Algorithm

AUC: Authentication Center

BS: Base Station

DES: Data Encryption Standard

GSM: Group Special Mobile

HLR: Home Location Register

IMSI: International Mobile Subscriber Identity

Kc: Ciphering Key

Ki: Individual Subscriber Authentication Key

LAI: Location Area Identity

LFSR: Linear Feedback Shift Register

MoU: Memorandum of Understanding

MS: Mobile Station

MSC: Mobile Switching Center

OMS: Operation and Maintenance Subsystem

RAND: Random Number

SRES: Signed Response

TMSI: Temporary Mobile Subscriber Identity

VLR: Visitor Location Register

7 REFERENCES

1- Security in the GSM network, Marcin Olawski, 2010

2- GSM Security Overview, wireless telephone history, Yuri Sherman

3- The GSM Standard, SANS Institute, 2001

4- Helsinki University of Technology, GSM Security, Mikko Suominen, 2003

5- A Contemporary Foreword on GSM Security, Paulo S. Pagliusi

6- GSM Architecture Training Document, Nokia Networks, 2002

7- GSM ŞEBEKELERİNDE GÜVENLİK, Nezih Yiğitbaşı, Bogazici University

8- GSM Security Overview, Max Stepanov

9-Security in the GSM system, Jeremy Quirke, 2004

10- GSM SECURITY ANDENCRYPTION, 101seminatopics.com

11- GSM Güvenliğinde Son Durumlar, Fatih Alagöz, Bogazici University

12- Can you clone a GSM Smart Card (SIM)?, Charles Brookson, 2002

13- GSM Interception, Lauri Pesonen, Helsinki University of Technology

14- GSM Security Overview, Gregory Greenman

15- Real Time Cryptanalysis of the Alleged A5/1 on a PC, Alex Biryukov & Adi Shamir, 1999

16- Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication, Elad Barkan & Eli Birham & Nathan Keller, Israel Institute of Technology

17- M Briceno, I Goldberg, D Wagner, GSM Cloning,

18 - J R Rao, P Rohatgi H Scherzer, Partitioning Attack: Or How to Rapidly Clone

19 - Some GSM Cards, IBM Watson Research Center,

20- Solutions to the GSM Security Weaknesses, Mohsen Toorani & Ali A. Beheshti, 2008

21 - [Security Algorithms Group of Experts (SAGE),Report on the specification and evaluation of the GSM cipher algorithm A5/2}.

22 - Intel Corporation, http://www.intel.com

23 - Technical information: GSM System Security Study,

24 - Gadaix E, GSM and 3G Security,

25- http://www.cellular.co.za/news_2003/120903-bizarre_jamming_of_moldova_gsm_n.htm