Security in GSM

Yong LI , Yin CHEN, Tie-Jun MA

1. A Brief Introduction to GSM

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world. According to a press release by the GSM Association recently, there are more than 747.5 million subscribers in over 184 countries today by the time of September 2002, accounting for 71.2% of the World's digital market and 69% of the World's wireless market. The number of subscribers worldwide is expected to surpass one billion by the end of 2003[7].

The name GSM first comes from a group called Group Special Mobile (GSM), which was formed in 1982 by the European Conference of Post and Telecommunications Administrations (CEPT) to develop a pan-European cellular system that would replace the many existing incompatible cellular systems already in place in Europe. But when GSM service started in 1991, the abbreviation "GSM" was renamed to Global System for Mobile Communications from Group Special Mobile. The typical architecture of GSM network was shown in figure 1.

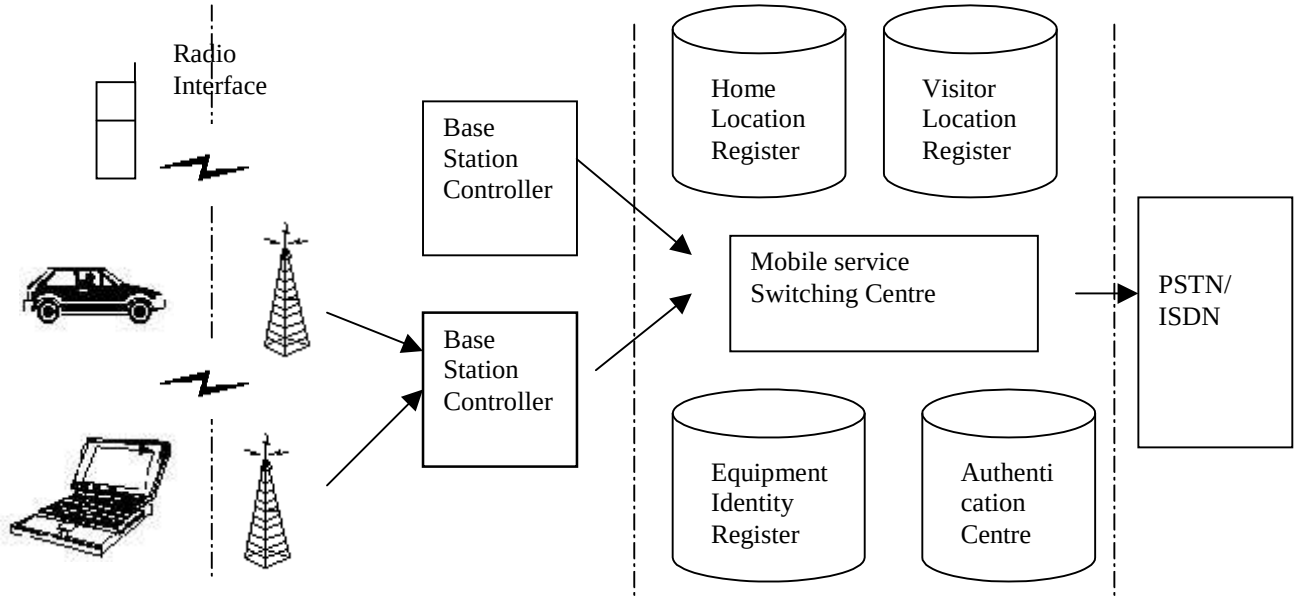

Fig.1. The architecture of GSM

The GSM network can be divided into three parts. The Mobile Station carries the subscriber; the Base Station Subsystem controls the radio link with the Mobile Station; the Network Subsystem, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. Not shown is the Operations and Maintenance center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station

Subsystem communicate across the air interface or radio link. The Base Station Subsystem and the Network Subsystem are also called the fixed network.

1.1 Mobile Station

The mobile station (MS) consists of mobile equipment and a Subscriber Identity Module (SIM) card. The most common mobile equipment is the mobile phone. By inserting the SIM card into a cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services. The mobile equipment uniquely identifies the International Mobile Equipment Identity (IMEI).

The SIM card stores the sensitive information such as the International Mobile Subscriber Identity (IMSI), Ki(a secret key for authentication), and other user information. All this information may be protected by personal identity number(PIN) .

The SIM card itself is a smart card and is in accordance with the smart card standard (ISO 7816-1, -2). The GSM 11.11 has the detailed specification about the SIM card.

1.2 Base Station Subsystem

The Base Station Subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The Base Transceiver Station houses the radio transceivers that define a cell and handles the Radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTS deployed. The Base Station Controller manages the radio resources for one or more BTS. It handles Radio-channel setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

1.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the public fixed network (PSTN or ISDN), and signalling between functional entities uses the ITU-T Signalling System Number 7 (SS7).

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the Call-routing and (possibly international) roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. There is logically one HLR per GSM network, but it may be implemented as a distributed database.

The Visitor Location Register contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, most manufacturers of switching equipment implement one

VLR together with one MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber' s SIM card, which is used for authentication and ciphering of the radio channel.

2. GSM Security Model

2.1 The Purpose of GSM Security:

The use of radio communications for transmission to the mobile subscribers makes GSM Public Land Mobile Networks (PLMN) particularly sensitive to misuse of their resources by unauthorized persons using manipulated Mobile Stations, who try to impersonate authorised subscribers and eavesdropping of the various information, which are exchanged on the radio path. So the security features in GSM PLMN is implemented to protect:

- The access to the mobile services.
- Any relevant item from being disclosed at the radio path, mainly in order to ensure the privacy of user-related information.

2.2 Security Features of GSM

Several security functions were built into GSM to safeguard subscriber privacy. These include:

- Authentication of the registered subscribers only
- Secure data transfer through the use of encryption
- Subscriber identity protection
- Mobile phones are inoperable without a SIM
- Duplicate SIM are not allowed on the network
- Securely stored Ki. [1]

2.2.1 Authentication of the registered subscribers

International Mobile Subscriber identity (IMSI) authentication is the corroboration by the land-based part of the system that the subscriber identity (IMSI or TMSI), transferred by the mobile subscriber within the identification procedure at the radio path, is the one claimed.The purpose of this authentication security feature is to protect the network against unauthorized use. It enables also theprotection of the GSM PLMN subscribers by denying the possibility for intruders to impersonate authorized users.[1].

The authentication procedure:

- The mobile station send IMSI to the network
- The network received the IMSI and found the correspondent KI of that IMSI.
- The network generated a 128 bit random number (RAND) and sent it to the mobile station over the air interface.
- The MS calculates a SRES with the A3 algorithm using the given Challenge (RAND) and the KI residing in the SIM. [1]

- At the same time, the network calculates the SRES using the same algorithm and the same inputs.
- The MS sends the SRES to the network,
- The network test the SRES for validity.

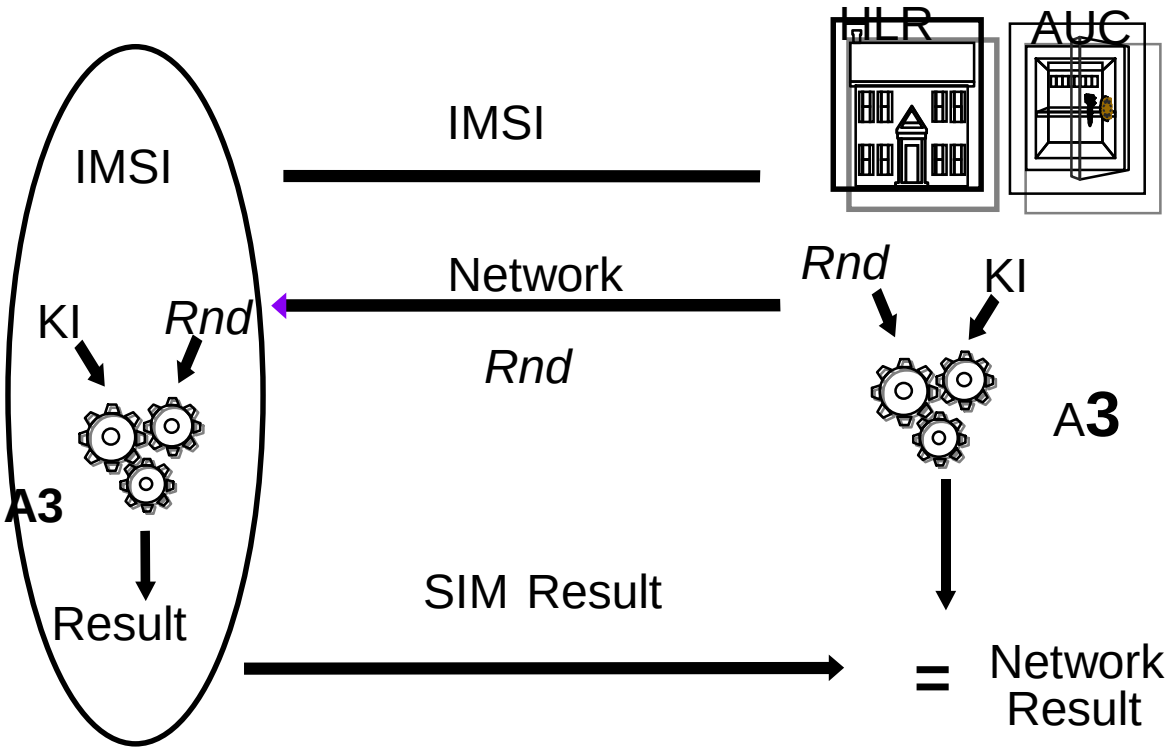

Fig.2. Authentication procedure

The authentication is based on a shared secret KI between the subscriber' s home network' s HLR and the subscriber' s SIM. This KI was generated and write to the SIM card at a safe place when the SIM card is personalised, and a copy of the key is put to the HLR.

When a new GSM subscriber turns on his phone for the first time, its IMSI is transmitted to the AuC on the network. After which, a Temporary Mobile Subscriber Identity (TMSI) is assigned to the subscriber. The IMSI is rarely transmitted after this point unless it is absolutely necessary. This prevents a potential eavesdropper from identifying a GSM user by their IMSI. The user continues to use the same TMSI, depending on the how often, location updates occur. Every time a location update occurs, the network assigns a new TMSI to the mobile phone. The TMSI is stored along with the IMSI in the network. The mobile station uses the TMSI to report to the network or during call initiation. Similarly, the network uses the TMSI, to communicate with the mobile station. The Visitor Location Register (VLR) performs the assignment, the administration and the update of the TMSI. When it is switched off, the mobile station stores the TMSI on the SIM card to make sure it is available when it is switched on again.

2.2.2 Encryption of the data

a. Generation of the cipher key KC

GSM makes use of a ciphering key to protect both user data and signal 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.

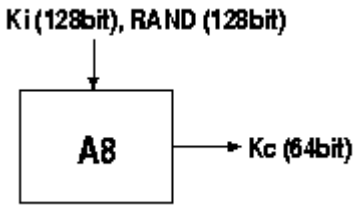

Fig. 3. Generation of the Session Key.

Note that the session key is generated in the SIM card of the Mobil Station. And the network can use the same set of Ki, RAND and the same algorithm to generate the same key to decrypt the data.

Allmost all the GSM operators use one algorithm(called COMP128) for both authentication and generation of Kc. As will be discussed below.

Encryption of the data

Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data. Each frame in the over-the-air traffic is encrypted with a different key-stream. The A5 algorithm used to encrypt the data is initialised with the KC and the number of the frame to be encrypted, thus generating a different keystream for every frame. The same KC is used as long as the MSC does not authenticate the MS again, in which case a new KC is generated. In practice, the same KC may be in use for days. The MS authentication is an optional procedure in the beginning of a call, but it is usually not performed. So it is very common the KC will not change during calls. When it is switched off, the mobile station stores the TMSI on the SIM card to make sure it is available when it is switched on again.

The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data on the fly.

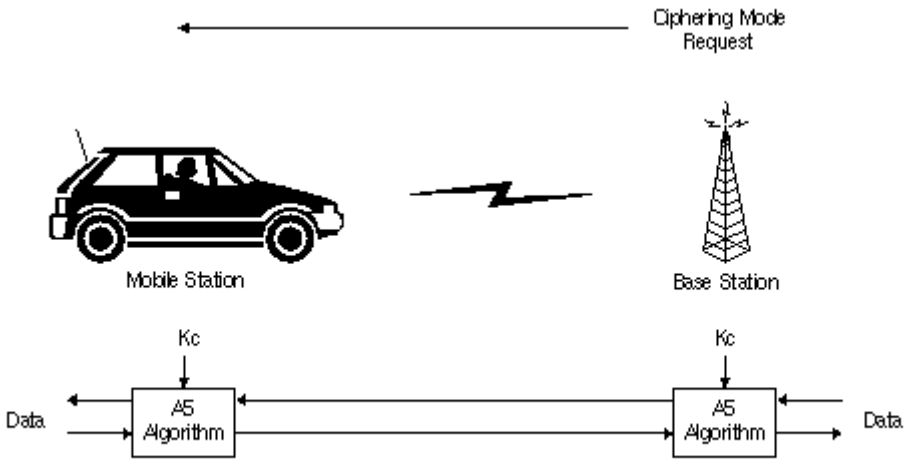

Fig.4. Ciphering of the voice data

2.2.3 Other secuity features

Subscriber identity protection

The IMSI(International Mobile Subscriber Identity) is stored in the SIM card. To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

Smart card

The smart card is like a micro computer which has memory, cpu and operating system. By programming the rom, it can store the sensive data with very high security leve. So it provides a good way to store the Ki and IMSI and other sensitive user data.

2.3 The Algorithms

A3: The MS Authentication Algorithm

The A3 is the authentication algorithm in the GSM security model. The A3 algorithm gets the RAND from the MSC and the secret key KI from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the KI secret are 128 bits long.

A3 algorithm can be typed as a one-way hash function. Generally, one-way hash functions produce a fixed-length output given an arbitrary input. Secure one-way hash functions are designed such that it is computationally unfeasible to determine the input given the hash value, or to determine two unique inputs that hash to the same value.

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM

Consortium. Other algorithms have been named as well, but almost every operator uses the COMP128 except a couple of exceptions. The COMP128 takes the RAND and the Ki as input, but it generates 128 bits of output, instead of the 32-bit SRES. The first 32 bits of the 128 bits form the SRES response.

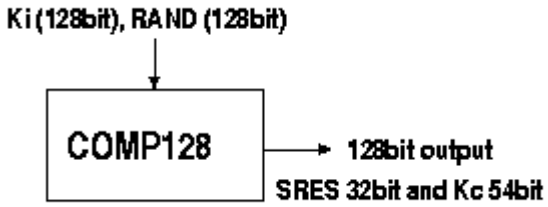

Figure 5 COMP128

A8, The ciphering Key Generation Algorithm

The A8 algorithm is the session key generation algorithm in the GSM security model. The A8 algorithm takes the two 128-bit inputs and generates a 64-bit output from them. This output is the 64-bit session key KC. As stated above, COMP128 is used for both the A3 and A8 algorithms in most GSM networks. The COMP128 generates both the SRES response and the session key, KC, on one run. The last 54 bits of the COMP128 output form the session key, Kc, until the MS is authenticated again. 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, we have a 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. Both the A3 and A8 algorithms are stored in the SIM in order to prevent people from tampering with them. This means that the operator can decide which algorithms to use independently from hardware manufacturers and other network operators. The authentication works in other countries as well, because the local network asks the HLR of the subscriber' s home network for the five triples. Thus, the local network does not have to know anything about the A3 and A8 algorithms used.

A patched version of COMP128 is now available (called COMP128-2), although it remains unpublished[4].

A5, the stream-ciphering algorithm

The A5 algorithm is used to encrypt over-the-air transmissions. There are now three different possibilities for GSM, A5/0(unencrypted), and use of the A5/1 algorithm or the A5/2 algorithm to secure the data. This arose because the GSM standard was designed for Western Europe, and export regulations did not allow the use of the original technology outside Europe. The uses of the algorithms in the network operator' s infrastructure are controlled by the GSM Memorandum of Understanding Group (MoU) according to the formula below:

- The present A5/1 algorithm can be used by countries, which are members of CEPT.

- The algorithm A5/2 is intended for any operators in countries that do not fall into the above category.

Generally, the A5 algorithms after A5/1 have been named A5/x. Most of the A5/x algorithms are considerably weaker than the A5/1, which has the time complexity of 2^54 at most as, shown above. The estimated time complexity of A5/2 is as low as 2^16. This encryption is used in the USA. The other A5 implementations have not leaked. Thus, there are no real facts about them, just guesses and assumptions.

Latest news: The A5/3 Algorithm has been developed:(The following is abridged from a press of www.etsi.org).

A new security algorithm, known as A5/3, will provide users of GSM mobile phones with an even higher level of protection against eavesdropping than they have already. A5/3 has been developed by a joint working party between the GSM Association Security Group and the 3rd Generation Partnership Project (3GPP™), for use in GSM™ systems. A5/3 is based on the Kasumi algorithm, specified by 3GPP for use in 3rd Generation mobile systems as the core of confidentiality and integrity algorithms.

3. Problems with GSM Security

3.1 The limitation and problems with GSM security

Problems with GSM security

- Security by obscurity. which means that all of the algorithms used are not available to the public. Most security analysts believe any system that is not subject to the scrutiny of the world's best minds can't be as secure.
- Only provides access security. All communication between the Mobile Station and the Base Transceiver Station are encrypted. But all communications and signalling is generally transmitted in plain text in the fixed network.
- Difficult to upgrade the cryptographic mechanisms
- Lack of user visibility (e.g. doesn't know if encrypted or not)
- The flaw of the algorithms.

3.2 Some possible method of attacks.

History
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.

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.

The most dangerous attach is retrieving the key from the SIM. The Smartcard Developer Association and the ISAAC security research group discovered a flaw in the COMP128 algorithm that effectively enabled them to retrieve the secret key, KI, from a SIM. The attack was performed on a SIM they had physical access to, but the same attack is applicable when launched over-the-air as well. The attack is based on a chosen-challenge attack that works, because the COMP128 algorithm is broken in such a way that it reveals information about the KI when the appropriate RANDs are given as arguments to the A8 algorithm. The SIM was accessed through a Smartcard reader connected to a PC. The PC made about 150.000 challenges to the SIM and the SIM generated the SRES and the session key, KC, based on the challenge and the secret key. The secret key could be deduced from the SRES responses through differential cryptanalysis. The Smartcard reader used in implementing the attack could make 6.25 queries per second to the SIM card. So the attack required about eight hours to conduct. [4]

In May 2002, the IBM Research team discovered a new way to quickly extract the COMP128 keys in SIM cards using side channels in spite of existing protections. The COMP128 algorithm requires the lookup of large tables, which can only be achieved in a complicated way on simple devices such as SIM cards leaking a lot of sensitive information into the side channels. The attack can be easily accomplished by making the card perform the algorithm just seven times with the unknown key. A hacker, who has possession of a SIM card for a minute, can easily extract the full 128-bit key.

3.3. Possible improvement

Security could be improved in some areas with relatively simple measures. One solution is to use another cryptographically secure algorithm for A3. This would require issuing new SIM-cards to all subscribers and updating HLR software. This would effectively disable the attacker from cloning SIM-cards, the most dangerous attack, which is discussed above. This solution is easy to be implemented because the network operators can make the changes themselves and do not need the support of hardware or software manufacturers or the GSM Consortium. There is now a new algorithms available called COMP128-2.[4]

The operator can employ a new A5 implementation with strong encryption too. A new A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm[7]. This improvement would require the co-operation of the hardware and software manufacturers because they will have to release new versions of their software and hardware that would comprise with the new algorithm.

Third solution would be to encrypt the traffic on the operator's backbone network between the network components. This would disable the attacker from wiretapping the backbone network. This solution could probably also be implemented without the blessings of the GSM Consortium, but the co-operation of the hardware manufacturers would still be required.

4. Conclusion

Although the GSM network was designed to be a secure mobile system and it did provide strong subscriber authentication and over-the-air transmission encryption, it is now vulnerable to some

attacks targeted at different parts of an operator' s networkOne of the main reasons is that some of the algorithms and specifications were leaked out and studied and some critical errors were found. The A5 algorithm used for encrypting the over-the-air transmission channel is vulnerable against known-plain-text and divide-and-conquer attacks and the intentionally reduced key space is small enough to make a brute-force attack feasible as well. The COMP128 algorithm used in most GSM networks as the A3/A8 algorithm has been proved to have some flaw either.

Even if security algorithms were not broken, the GSM architecture would still be vulnerable to attacks from inside which means the attack targeting the operator' s backbone network or HLR.

However, the security can be improved in some areas with relatively simple measures.

5. Acronyms

A3
Authentication Algorithm
A5
Ciphering Algorithm
A8
Ciphering Key Generating Algorithm
AUC
Authentication Centre
BS
Base Station
CEPT
European Conference of Post and Telecommunication Administrations
ETSI
European Telecommunications Standards Institute
GSM
Group Special Mobile
HLR
Home Location Register
IMSI
International Mobile Subscriber Identity
KC
Ciphering Key
KI
Individual Subscriber Authentication Key
MS
Mobile Station
MSC
Mobile Switching Center
RAND
Random Number
SRES
Signed Response
TMSI
Temporary Mobile Subscriber Identity
VLR
Visitor Location Register

6. References

[1] European Telecommunications Standards Institute, Recommendation GSM 02.09, "Security Aspects".

[2] European Telecommunications Standards Institute, Recommendation GSM 02.17, "Subscriber Identity Module".

[3] European Telecommunications Standards Institute, Recommendation GSM 03.20, "Security Related Network Functions".

[4] Internet Security, Applications, Authentication and Cryptography, University of California, Berkeley. “GSM Cloning” http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

[5] David Margrave, “GSM Security and Encryption”, http://spyhard.narod.ru/phreak/gsm-secur.html.

[6]Lauri Pesonen, “GSM Interception”, http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/a5/Netsec/netsec.html.

[7] GSM Association. www.gsmworld.com.

[8] Josyula R Rao, Pankaj Rohatgi, Helmut Scherzer and Stefan Tinguely “Partitioning Attacks: Or how to rapidly clone some GSM cards”, IEEE Symposium on Security and Privacy.