

# SECURITY ASPECTS IN GSM AND ITS FLAWS

Ashish Suri  
ECE Deptt. ,MIET, Jammu  
[ashish.surii@rediffmail.com](mailto:ashish.surii@rediffmail.com)

Vishal Puri  
ECE Deptt. ,MIET, Jammu  
[vishal\\_puri28@yahoo.com](mailto:vishal_puri28@yahoo.com)

Baljit Singh  
ECE Deptt. ,MIET, Jammu  
[baljit\\_singh97@rediffmail.com](mailto:baljit_singh97@rediffmail.com)

Gourav Khajuria  
ECE Deptt. ,MIET, Jammu  
[gouravkhajuria@rediffmail.com](mailto:gouravkhajuria@rediffmail.com)

## Abstract

Mobile communications in the past decade has changed the scenario of communications and is termed as the key services of the digital revolution. A very little is known about how the communication exactly takes place between users accessing the mobile network across the globe. Even less is known about the security measures and protection behind the system. The cell phone is slowly turning into a handheld computer which is capable to do a work of a computer and for that reason only, the security of mobile communication becomes an area of concern. The security of the network has been the area which needs attention as we cannot design a system which can be safe to the external attacks. This paper reviews the security aspects of GSM and its flaws.

## I. Introduction.

General System for Mobile Communications, GSM, is an advanced mobile phone system used around the world. GSM has many benefits over its predecessors in terms of security, capacity, clarity, and area coverage, which aims to provide a secure connection for communication. Since its advent in the early 1980's it has grown into a family of services to provide everything from mobile voice to mobile data communication[1]. Mobile phones are used by hundreds of millions of users each day with the increasing trends and it still remains a fact that landline offers a fixed level of physical security to its users (atleast physical access is required to listen in the phone line), but unlike in mobile phones in a radio link any one can listen the radio transmission if he/ she is having a radio receiver. Therefore it is highly recommended that there should be some means and technological ways so that security is provided to the phone calls and text messages of the users.

## II. GSM Overview

GSM was designed in Europe as a very strong cellular technology that would allow the subscriber to roam

anywhere in the planet where the service is available, regardless of the service provider, by just changing a smartcard in the mobile station. This very specific characteristic has made GSM the most used cellular technology in the world today. In the late 1980s, the groups involved in developing the GSM standard realized that within the given time-frame they could not complete the specifications for the entire range of GSM services and features as originally planned [1]. Because of this, it was decided that GSM would be released in phases with phase consisting of a limited set of services and features. Each new phase builds on the services offered by existing phases.

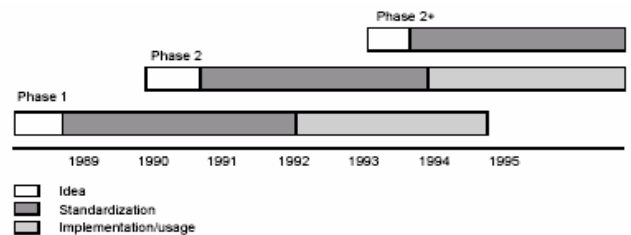


Fig. 1 Phases of GSM [1]

## III. GSM Architecture:

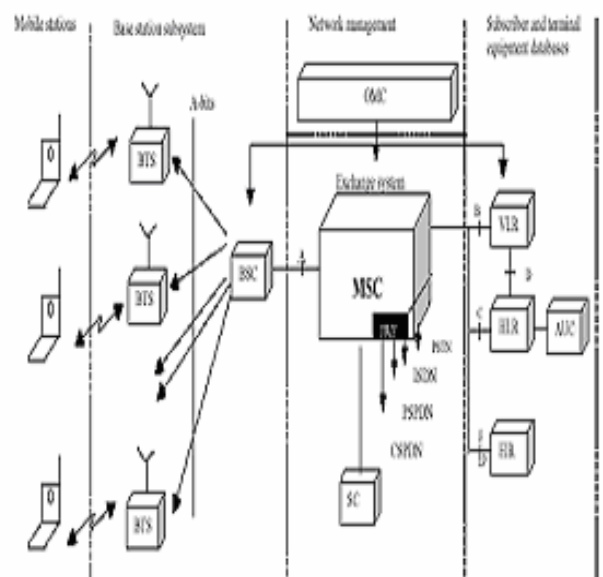


Fig. 2 GSM Network. [2]

The GSM network is divided in 4 sections:

### **Mobile Stations**

The Mobile Stations (MS) contain two major components the Subscriber Identity Module (SIM), which is a removable smart card, and the Mobile Equipment (ME). The user in the GSM Network uses a mobile station to make and receive calls. The Mobile Equipment (ME) is a physical device with unique identifiers, IMEI (International mobile identification number). Each ME or MS has a relationship with its home network and with the visiting network if it is outside [2]. A GSM N/W is shown in Fig.2

### **Base Station Subsystem (BSS)**

The Base Station Subsystem (BSS) consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The MS communicates with the base transceiver station via the radio interference. A BTS performs all the transmission and reception functions relating to the GSM. In some ways the BTS can be considered to be a complex radio modem that takes the up-link radio signal of the MS and converts it into data. The BSC is the connection between the mobile and the Mobile Service Switching Center (MSC)[2]. 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.

### **Network Management [2]**

The central component of the Network Subsystem is the Mobile Services Switching Center. 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. Every BSS is connected to a Mobile Service Switching Centre. The MSC is concerned with the routing of calls to and from the mobile users.

### **Subscriber and Equipment Databases**

Equally important as the quality of service provided are the means of charging and billing subscribers, maintaining accurate subscription records and preventing fraudulent network access. It must also possess some way to track MSs

so that it is able to successfully route incoming calls to them.

**The Home Location Center (HLR)** is the heart of the GSM network and is also known as the memory of the system as it stores information that is specific to each subscriber. Every GSM subscriber will have a record in the HLR.

The **Authentication Center (AuC)** is much related to the HLR. The AuC is solely used to store information that is concerned with GSM security features, i.e. user authentication and radio path encryption. It will contain the subscriber's secret key Ki and the A3 and A8 security algorithms.

The **Visitor Location Register (VLR)** is associated with one or more MSCs and it contains information relating to those subscribers that are currently registered within the MSC area(s) of its associated MSC.

The **Equipment Identity Register (EIR)** database contains mobile equipment identity information which helps to block calls from stolen, unauthorized, or defective mobile stations.

The **Operation and Maintenance (OMC)** provides a central point from which to control and monitor the other network entities (i.e. base stations, switches, database, etc) as well as monitor the quality of service being provided by the network.

## **IV. Security Concern in GSM**

The security in GSM networks is area of research, as the fraudulent measures are on an increase and the network needs to be secure from such kind of attacks. The Security in GSM is broadly divided on the following levels:

- i. Operator's level.
- ii. Customer's level.
- iii. Make a system at least as secure as PSTN.

These three areas look for the following aspects i.e. correct billing to the people, Avoid fraud, Protect Services, Privacy, and Anonymity [3].

### **GSM Security Features**

The GSM Security features describe how the security

can be implemented in the GSM Network. The GSM Network divides the security in the following features.

**Authentication:** GSM Network operator can verify the identity of the subscriber making it infeasible to clone someone else's mobile phone.

**Confidentiality:** GSM Network protects voice, data and sensitive signalling information (e.g. dialled digits) against eavesdropping on the radio path.

**Anonymity:** GSM Network protects against someone tracking the location of the user or identifying calls made to or from the user by eavesdropping on the radio path.

The GSM Security Model implements the above listed features in the following mechanisms

Authentication is achieved by the following processes :

- i. Challenge-response authentication protocol
- ii. Encryption of the radio channel

Confidentiality

- i. Encryption of the Radio Channel

Anonymity

- i. Using Temporary Identities

**Authentication:**

The authentication process can be achieved in a simple way by using a password i.e. Personal Identification Number (PIN). This method is very less secured in GSM Network as an attacker can listen to your PIN can easily break the code. In GSM the Challenge-response authentication protocol is used for the authentication of a subscriber having a Subscriber Identify Module (SIM).

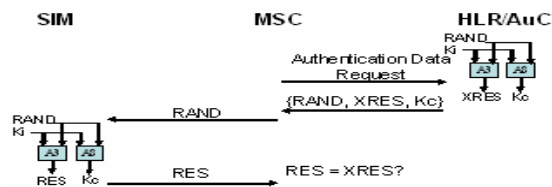


Fig 3: Authentication Protocol.[4]

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 the protection of the GSM subscribers by denying the possibility for intruders to impersonate authorized users. The authentication is done by the procedure shown in Fig 3. i.e. The mobile station sends IMSI to the network. The network receives the IMSI and finds the correspondent Ki of that IMSI. The network generates a 128 bit random number (RAND) and sends 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. At the same time, the network calculates the SRES using the same algorithm and the same inputs [4]. The MS sends the SRES to the network, the network tests the SRES for validity. The authentication is based on a shared secret key Ki between the subscriber's home network's HLR and the subscriber's SIM. This Ki was generated and written in the SIM card at a safe place when the SIM card is personalized, and a copy of the key is put to the HLR.

**Anonymity**

The Anonymity of the subscriber on the radio access link in the GSM Network can be achieved by allocating Temporary Mobile Subscriber Identity (TMSIs) instead of permanent identities i.e. International Mobile Subscriber Identity which helps to protect against tracking a user's location and obtaining information about a user's calling pattern. When a user first arrives on a network he uses his IMSI to identify himself and when the network has switched on encryption it assigns a temporary identity TMSI 1 to the user, next accesses the network he uses TMSI 1 to identify himself and the network assigns TMSI 2 once an encrypted channel has been established.

**Confidentiality**

The Confidentiality of a subscriber in the GSM network is achieved by using the encryption techniques prescribed by the GSM designers. The encryption of data on the radio path is encrypted between the Mobile Equipment and the Base Transceiver Station which protects user traffic

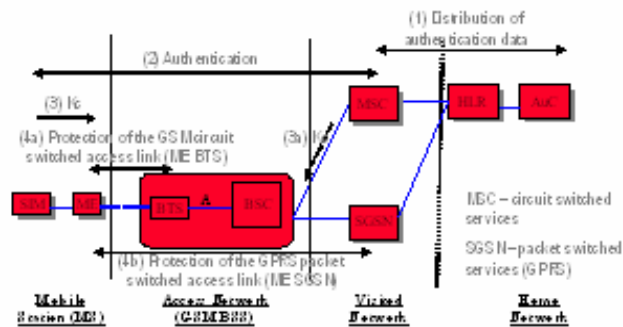


Fig 4: Radio Link Security [5].

and sensitive signalling data against eavesdropping and extends the influence of authentication to the entire duration of the call. It uses the encryption key ( $K_c$ ) derived during authentication for encryption. Encryption is performed by applying a stream cipher called A5 to the GSM TDMA frames, the choice being influenced by speech coder, error propagation, delay and handover.

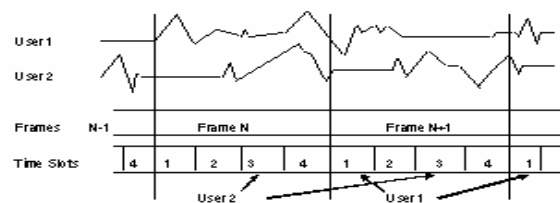


Fig 5 TDMA frame Structure for two Users [5].

From Fig 5, it can be seen that for each TDMA frame, A5 generates consecutive sequences of 114 bits for encrypting/decrypting in the transmit/receive time slots. Encryption and Decryption is performed by applying the 114 bit key stream sequences to the contents of each frame using a bit-wise XOR operation. A5 generates the key stream as a function of the cipher key and the frame number, so that the cipher is re-synchronised to every frame. The TDMA frame number repeats after about 3.5 hours, hence the keystream starts to repeat after 3.5 hours new cipher keys can be established to avoid keystream repeat. The encryption mechanism follows the sequence of the procedure i.e. The BTS instructs ME to start ciphering using the *cipher* command, at same time BTS starts decrypting. ME starts encrypting and decrypting when it receives the *cipher* command and BTS starts encrypting when *cipher* command

is acknowledged by the ME. The GSM uses the following encryption algorithms. Currently defined algorithms which are in use are A5/1, A5/2 and A5/3. The A5 algorithms are standardised so that mobiles and networks can interoperate globally. At present all GSM phones currently support A5/1 and A5/2. Most networks use A5/1, some use A5/2. A5/1 and A5/2 specifications have restricted distribution but the details of the algorithms have been discovered and some cryptanalysis has been published.

A5/3 is new algorithm expected to be phased out over the next few years.

## V. Precincts in GSM Security

Security problems in GSM stem by and large from design limitations on what is protected. The designs only provides access security and the communications. Signalling in the fixed network portion aren't protected by the attacks. The design does not address active attacks, whereby network elements may be impersonated. The design goal was only to be as secure as the fixed networks to which GSM systems connect. The other precinct is that lack in acknowledging limitations. The terminal is an unsecured environment, so trust in the terminal identity is misplaced by the designers and also disabling encryption does not just remove confidentiality protection, it also increases risk of radio channel hijack. The standards don't address everything and operators must themselves secure the systems that are used to manage subscriber authentication key.

## VI. Explicit problems in GSM

### Ciphering Algorithms

The use of COMP 128 as the A3/A8 algorithm by some operators but it is susceptible to collision attack and the key can be determined if the responses of about 160,000 subscribers are known to the attacker, later improved to about 500,000. The GSM cipher A5/1 is becoming helpless to exhaustive search on its key and towards the advances in cryptanalysis. The GSM cipher A5/2 which the cryptanalysis leaked and broken in August 1999[6]. A5/2 now offers virtually no protection against passive

eavesdropping

A5/2 is now so weak that the cipher key can be exposed in near real time using a very small amount of known plaintext.

### **False Base Station**

The false base station can be created by knowing IMSI Number. IMSI catching is the concept by which it forces the mobile to reveal its IMSI. The other method is intercepting mobile-originated calls by disabling encryption as the encryption is controlled by network and the user generally is unaware if it is not on and the false base station masquerades as network with encryption switched off. The third method was intercepting mobile-originated calls by forcing use of a known cipher key.

## **VII. Measure to GSM Security Precincts**

The GSM Standard is not a stagnant standard as it is being updated every year and new technologies are being incorporated. In India we are having only the 2.5 G specifications which include EDGE, GPRS and HSCSD. The UMTS is designed to conquer the security flaws in the GSM. 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 [7]. This would effectively disable the attacker from cloning SIM-cards, the most dangerous attack. There is now a new algorithms available called COMP128-2. The operator can employ a new A5 implementation with strong encryption too. A new version of A5 i.e. A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm. The third solution would be to encrypt the traffic on the operator's backbone network between the network components [8]. This would disable the attacker from wire tapping the backbone network. The co-operation of the hardware manufacturers would still be required for the implementation of such kind of encryption techniques.

## **VII. Conclusion**

The strong demand for GSM is continuing. Today, GSM is used by billions of people worldwide and the strong growth is expected to be maintained. GSM architecture reveals a highly complex and hierarchical system. 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 kind of attacks targeted at different parts of an operator's network. The paper discusses the security aspects of the GSM network has made the designer to think new technologies, which has made the security attacks less harmful in the GSM Network. This paper is basically a review of all the basic aspects involved in GSM.

### **References:**

- [1] Brookson, Charles. "GSM (and PCN) Security and Encryption." August 2001.
- [2] Li, Yong, Chen, Yin, and Ma, Tie-Jun. "Security in GSM". February 2002.
- [3] Wei Zhang, GSM security issues, [11.15.2000].
- [4] Tuan Huynh and Hoang Nguyen, "Overview of GSM and GSM Security", June 06, 2003.
- [5] Max Stepanov, " GSM Features and Security" ,July 2004.
- [6] P. HOWARD, .GSM and 3G Security, Lecture Notes, Royal Hollowly, University of London, 19 Nov 2001.  
<http://www.isg.rhbnc.ac.uk/msc/teaching/is3/is3.shtml>.
- [7] <http://www.3gpp.org/ftp/specs/latest>
- [8] Dr. S. Muhammad Siddique, Muhammad Amir, "GSM Security Issues and Challenges", 2006.
- [9] [www.motorola.com/trainingmaterial/cp02](http://www.motorola.com/trainingmaterial/cp02)