Vulnerabilities in Existing GSM Technology that causes Exploitation

Madhav M. Ajwalia
Research Student, IT Systems & Network Security,
Gujarat Techlonogical University PG School,
Ahmedabad, Gujarat, India.
madhav_ajwalia@yahoo.co.in

Prof. (Dr.) Nilesh K. Modi
Professor and Head of Department MCA,
S V Institutes of Computer Studies, S V Campus,
Kadi, Gujarat, India.
drnileshmodi@yahoo.com

Abstract — Global System for Mobile communications (GSM system) has become the most popular standard for digital cellular communication for day to day communication in the world. Cellular phones have become a ubiquitous means of communications with over 6 billion users worldwide in 2013, of which 80% are GSM subscribers. It has been over 20 years since GSM was designed, and during this time several security problems have been found. However practical exploits of these weaknesses are complicated because of all the signal processing involved and have not been seen much outside of their use by law enforcement agencies.

Keywords - A3, A5, A8, anonymity, authentication, COMP128, confidentiality, GSM, IMSI, K_c, K_i, RAND, SRES, TMSI

I. INTRODUCTION

Today's third generation GSM is used daily by hundreds of millions of people where different security algorithms and its strength play vital roles. GSM architecture is shown in Figure1. Where each entity has also plays vital role in communication.

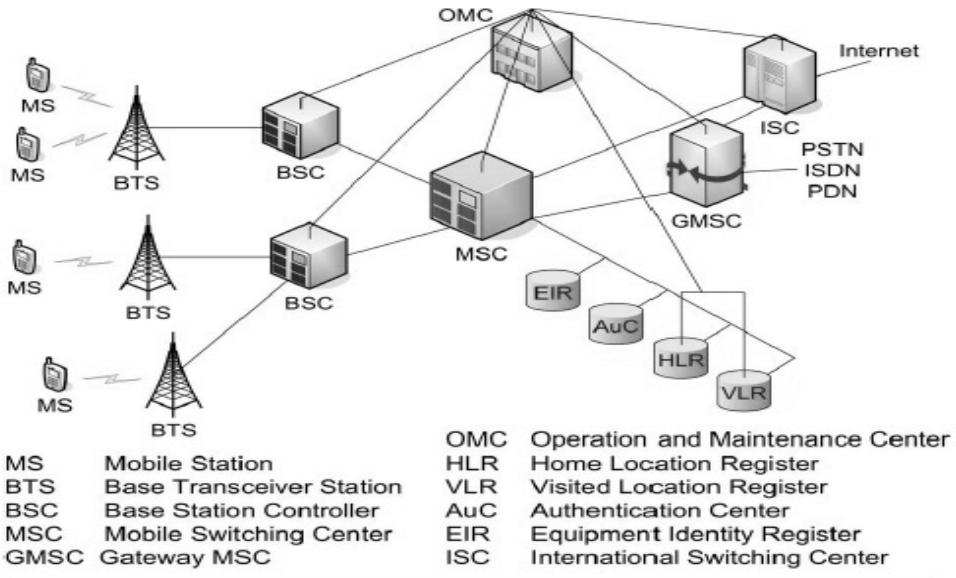

Figure1. GSM Architecture [13]

With Global System for Mobile Communications (GSM) networks, for instance, the network validates the credentials in the Subscriber Identity Module (SIM) card. In cellular networks, there are no provisions to authenticate the network to the user system. It shows that the existing GSM system has many security flaws.

All algorithms used in GSM - A3, A5, and A8, are unpublished. In open systems, it completely violates the design philosophy of the cryptosystem. In an open and heterogeneous system, it will be a dangerous to use an unpublished algorithm which is not verified in public. Moreover they are proved to be cracked.

GSM is one of the widely used mobile systems in the world, found to have some possible vulnerability which is concerned among many researches. Most of them are the weakness in algorithm used in both authentication to mobile user (COMP128) and encryption to communication data (A5/1, A5/2, A5/3) and anonymity (IMSI/TMSI) disclose.

II. WHY SECURITY IS NECESSARY?

The use of radio communications for transmission to the mobile subscribers makes GSM particularly sensitive to misuse of their resources by unauthorized persons using manipulated Mobile Stations, who try to impersonate authorized subscribers and eavesdropping of the various information, which are exchanged on the radio path. If your device is using the GSM network for communication, a hacker can simulate the network, copy your credentials and then use them to gain access to your network without customers ever knowing about it.

The first digital cellular mobile telecommunication system GSM provides security functions [1,2] to guarantee the confidentiality of communications. The purpose of the security functions in GSM is [3,16]:

- keep away from accessing illegal services by intruders who try to impersonate legal and authorized subscribers,
- avoid eavesdropping of the information which are transmitted on the (wireless) radio path,
- authenticate only registered subscriber,
- avoid the usage of duplicate SIMs on the network,
- secure data transmission through the use of any encryption technology.

These lead to the need to implement security functions in GSM in order to protect [3]:

- from the illegal access to the mobile services; and
- the privacy of user-related information on radio paths.

The GSM encryption algorithms are not published along with the GSM standards. Instead, the GSM Association controls the distribution of the algorithm specifications. They do not make the algorithms available for peer review that has received some criticism, from the academic world.

III. SECURITY FEATURES

To implement security policies and to effectively design their security architectures, network managers must understand the security features of the networks they are using. It addresses these goals of security functions by providing user-related security features for *authentication*, *confidentiality* and *anonymity*.

a) Authentication: The first requirement is validation of user for SIM. The user must have to enter a secret PIN to access it. Next requirement is subscriber authentication based on challenge-response scheme. (Figure 2)

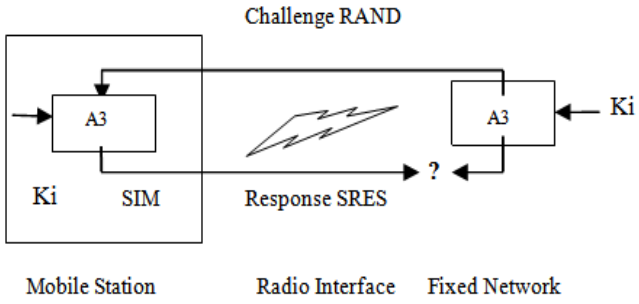

Figure 2. Authentication in GSM

b) Confidentiality: All user related data are encrypted. Encryption is done by algorithm A5 with encryption key Kc. After authentication, BTS and MS apply to encrypt voice, data and signalling. So the data over the air will be secret.

c) Anonymity: All the data are encrypted before transmitted. User identifiers which would reveal permanent identity of user are not used over the air. Instead of that permanent identity IMSI, TMSI is used which is provided by VLR on an update by itself also.

Some Key elements of GSM communication system are:

- **K_i:** The K_i is the 128-bit individual subscriber authentication key which is paired with an IMSI number when SIM is created. Ki is only stored on the SIM card and at the AuC. The Ki will never be transmitted across the network.

- **Kc**: The Kc is the 64-bit ciphering key that is used in the A5 encryption algorithm to encrypt and decrypt the data on the Um interface (between MS and BTS).
- **RAND**: The RAND is a random 128-bit number that is generated by the AuC when the network requests to authenticate a subscriber. It is used to generate the Signed Response (SRES) and Kc cipher key.
- **SRES:** It is computed by A3 algorithm means it is outcome of A3. The inputs are Ki and RAND and 32-bit SRES is generated. When 128-bit Ki and 128-bit RAND are entered into COMP128, it can also generate 32-bit SRES and 54-bit Kc.

IV. SECURITY FUNCTIONS

In GSM, the security system provides three different security functions from the user's point of view:

a) *Anonymity- Temporary Identities:* Each subscriber of the GSM network has a unique international mobile subscriber identity IMSI. Using this unique number, one can easily find which mobile station belongs to which mobile network. So within the network and the radio link between MS and BSS, instead of using IMSI, a temporary mobile subscriber identity (TMSI) is given to each and every subscriber. But the TMSI is stored and accessed in conjunction with the Location Area Identity (LAI). [4] For each LOCATION _UPDATE Request MS receives TMSI significance to that location area. [14]

b) *Authentication- Challenge Response Scheme:* The authentication procedure checks the validity of the subscriber's SIM card and then decides whether the mobile station is allowed on a particular network. The network authenticates the subscriber through the use of a challenge-response method. [5] The procedure is shown in Figure 2.

Firstly, a 128 bit random number (RAND) is transmitted to the mobile station by air interface. The RAND value changes per every access attempt, so an eavesdropper with recordable SRES response will not be able to reuse it later. 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 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. Instead of storing value of SRES at AuC, it ask HLR or VLR as it needed.

c) *Confidentiality- Enciphering:* The enciphering process is carried out between the BSS and the MS. The enciphering algorithm (A5) stored in both the MS, without the SIM, and the BSS. The purpose of the enciphering process is to provide confidentiality of user data. [4] Ciphering is used to protect signaling data and user data (Figure 3).

Figure 3. Ciphering in GSM

V. WEAKNESSES / FRAGILITY OF GSM SYSTEM

This section lists certain weakness in the existing security system.

- Communication traffic and signaling traffic are not protected when connected to fix networks; therefore the GSM network is only secure when connected with at the fixed network.
- The strength of the encryption algorithm depends on the length of the cipher key. Here 54 bits out of 64 bits are used. Creating a longer key than this (64 bits) for GSM is much more complex because it would require the ciphering algorithm to be replaced and the signalling protocols to be upgraded to support the longer key [6] but encryption and authentication mechanisms are very difficult to upgrade. [15]
- The challenge response entity authentication used in the existing security system to verify the authenticity of the mobile station by the network could be vulnerable to reflection attacks. [4] The reason is because the SRES does not contain enough information about either the originator or the receiver.
- In addition to the SIM cards, individual authentication keys of the users are also stored in the GSM authentication centers. Any person who has the rights and capabilities to access to authentication center can obtain the authentication key of a valid subscriber to impersonate that mobile user. [12] An unauthorized person can thus capture and decipher the encrypted traffic on the radio channel between the mobile station and the base station.

- Cause of lack of authentication of VLR/HLR, an intruder can impersonate pseudo-HLR/VLR. Wrong VLR can update wrong data to HLR to misguide management system. And wrong HLR can replace with original one and can take control over system to do everything arbitrary.
- During the inter-domain visits of GSM subscribers, some important authentication parameters, such as the encryption key, are sent from the HLR to the new VLR in the clear. Security of this HLR→VLR (or VLR→VLR) communication depends on the security of the intermediate transport network between these two registers. [7]
- When MS wants to update the location in new VLR and old VLR is unreachable, at that time new VLR will ask MS to directly send its IMSI to new VLR without any protection. [3] Like this, it is possible to get IMSI in the way and can identify MS.
- IMSI is unprotected and during location update procedure it is transmitted across VLRs. The attackers have higher chances of copying subscriber data like IMSI and later on sending a request for the triplet RAND, SRES, Kc using the copied IMSI and can also trace the location of mobile station by keep track of TMSI assigned to the mobile station.
- During the inter network location update the triplet (RAND, SRES, Kc) is sent unprotected to the foreign network. But only the home network can authenticate its subscriber in the foreign network. An attacker can copy the encryption key Kc from the unprotected triplet which passes across the different network and decipher the encrypted voice data of that particular subscription.
- There is no encryption between VLR and VLR/ HLR. An eavesdropper can monitor the physical channel of HLR and eavesdrop MS's location updating information and MS's IMSI and triplet of RAND, SRES, and Kc. [8,17] Using that, he can trace MS's position, use Kc to eavesdrop MS's conversation, and even impersonate MS to access services without the secret key Ki.
- The user's voice data is protected only in the radio link (U_m-interface) between the MS and the BSS. No protection of voice data is provided in the fixed infrastructure of the GSM. This leads to the possibility of eavesdropping of voice data at the fixed infrastructure of the GSM.
- With respect to user authentication, some mobile devices allow for devices to be configured so that a user must enter a PIN before using the device. However, a user can easily disable this mechanism. It also does not satisfy two-factor authentication requirements.
- Security algorithms of the GSM (A3, A5, and A8) are all unpublished, secret algorithms. Researchers have reverse-engineered these algorithms and they have shown that these algorithms have many important security flaws. [7]
- The confidentiality of data over the air depends on the strength of A5 algorithm. If it is feasible to break the algorithm, the opponent will have access to the session key, be able to decrypt, and eavesdropping the call. [8]
- The authentication strength depends on algorithm used, which is COMP128, in A3 and A8. If it is feasible to be break, once opponent has an access to the SIM card, it will become possible to find the secret key and be able to fraud as a legitimate user. [8]
- During the registration phase, a TMSI is assigned to the handset if it has not been seen before. This TMSI is supposed to be always 32 bits long, but a variable length field is used. Indeed, sending a longer TMSI (e.g. 128 bytes) caused the baseband stack to crash. [9]
- To hide the identity of the user, the networks camouflage IMSI with a temporary identification number TMSI. As per international norms, the TMSI should be changed every time a call or SMS is made or received, [10] which are not being done by majority of providers. In the absence of ever changing TMSI, any intruder can get corresponding IMSI and the network can be made to believe that intruder is actual customer and call can be authenticated.
- Wagner and Goldberg announced that they had cracked COMP128. COMP128 had a weakness which would allow complete knowledge of Ki if around 1, 60,000 chosen RAND-SRES pairs could be collected. [11]

The following table summarizes the limitations of operator-hosted security features.

TABLE 1. SECURITY MECHANISMS AND LIMITATIONS

Security Mechanism	How it works	Limitation
Device Authentication	Authenticates device of network to allow network access	Only 3G networks employ bi-directional authentication. Seamless 2G/3G handover makes it difficult to know network type.
User Authentication	User must enter PIN to use device	User can disable features, and does not satisfy two-factor authentication requirements.
Encryption of Radio Link	Encryption of the radio link from user device to a node in network.	Data decrypted within operator network and may travel in the clear within operator network.
Back-end Connection Security	Private circuits and network VPNs to protect Internet traversal	Requires custom arrangement with additional service charges. Private circuits such as frame relay do not encrypt data.
Protection for Alternate Network Access	Potential extension of encryption to other network types.	Only available in isolated cases for networks under the particular operator's control.

VI. SOLUTIONS

Regardless of security improvements in the upper generation networks, it is necessary to provide solutions to improve the security of the currently available 2G systems. Because of the security mechanisms of the upper generation are similar to that of the GSM.

Use secure algorithms for A3/A8 implementations. COMP128 is thwart by SIM card cloning and Ki cracking over the air. A more regular change requires for the session key, which gives the attacker less known data.

Use secure encryption algorithm. A system should have to upgrade other security features and the encryption algorithm from A5 to another stronger encryption algorithm like triple DES. Sometime intruder will force to deactivate encryption mode. Thats why ciphering should be implemented on mobile phone.

Deploy end-to-end security. Most of security flaws like SIM cloning and DOS attack are targeted to group of user instead of the particular ordinary people. Make secure the traffic between mobile devices and network such that it prevents the attacker to eavesdrop and modify the conversation. Make regular changes of the TMSI at each transaction such that, it is harder to follow a specific mobile phone's location. Randomization of control message padding requires which reduces the known text in the messages. It was already specified [18] but should required implementation with high priority.

One interesting solution is; on latest mobile phones the user could install additional encryption software to encrypt calls. It requires this software at both node of communication.

VII. CONCLUSIONS

Since the digital mobile cellular communication systems are the infrastructure of the future personal communication services, the security is essential. In the case of security about legitimate user, network operators are primarily concerned with authentication mechanisms and encryption, designed to ensure that only legitimate devices connect to the network. According the requirements, we indicate that the security functions of GSM are not enough. GSM security system becomes vulnerable and be more possible to attack. In order to satisfy the security requirements, today's mobile communication systems, like as GSM, need more upgrading.

REFERENCES

[1] "GSM 03.20: Security Related Network Functions," European Telecommunications Standards Institute
[2] "GSM 02.09: Security Aspects," European Telecommunications Standards Institute
[3] Shiuh-Pyng, Shieh Chern-Tang, Lin Jung-Tao Hsueh, Secure Communication in Global Systems for Mobile Telecommunications, Department of Computer Science and Information Engineering National Chiao Tung University, Hsinchu, Taiwan
[4] Chenthurvasan Duraiappan, yuliang Zheng, University of Wollongong, Enhancing Security in GSM
[5] Security Requirements for Wireless Networking, Rysavy Research,
[6] UMTS Security, K. Boman, G. Horn, P. Howard and V. Niemi, Electronics and Communication Engineering Journal

[7] Basar Kasim, hacettepe Uni., Turkey, Levent Ertaul, Depart. maths and CS, Hayward, CA, USA, GSM Security
[8] Pacharawit Topark-Ngarm, Panupat Poocharoen, GSM Security vulnerability
[9] Ralf-Philipp Weinmann, University of Luxembourg, Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks
[10] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim, Location Leaks on the GSM Air Interface, University of Minnesota Holloway, University of London, Egham, Surrey TW20 0EX, UK
[11] Paulo S. Pagliusi, A Contemporary Foreword on GSM Security, Paulo S. Pagliusi, Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
[12] Basar Kasim, hacettepe Uni., Turkey, Levent Ertaul, Depart. maths and CS, Hayward, CA, USA, GSM Security
[13] Mohsen Toorani, Ali A. Beheshti, Solutions to the GSM Security Weakness, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies
[14] Paul Yousef, GSM-Security:a Survey and Evaluation of the Current Situation, LiTH-IS-EX-3559-2004
[15] Valer BOCAN, Vladimir CREŢU, Threats and Countermeasures in GSM Networks, JOURNAL OF NETWORKS, VOL. 1, NO. 6, pp-18-27, NOVEMBER/DECEMBER 2006
[16] SANS Institute InfoSec Reading Room, The GSM Standard (An overview of its security), SANS Institute 2001
[17] Shiuh-Pyng Shieh Chern-Tang Lin Jung-Tao Hsueh, Secure Communication in Global Systems for Mobile Telecommunications, Department of Computer Science and Information Engineering
[18] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996