Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Vulnerabilities and Attacks in Global System for Mobile Communication (GSM)

Radhika Saini*
Computer Science Engineering Department
Ambedkar Institute of Technology
New Delhi, India
myself_radhika@yahoo.co.in

Mohit Wadhwa
Computer Science Engineering Department
Ambedkar Institute of Technology
New Delhi, India
mohitwadhwa86@gmail.com

Manju Khari
Computer Science Engineering Department
Ambedkar Institute of Technology
New Delhi, India
manjukhari@yahoo.co.in

Abstract: Global System for Mobile Communication (GSM) furnishes users with mobile connectivity via wireless radio link. Such networks are the focus concern for intruders to attack as several vulnerabilities is present in it. Intruder can derive the crucial information about network and its users by exploiting its vulnerability. Therefore it becomes mandatory to secure the network in order to resist attacks. In this paper, such vulnerability is discussed and how these vulnerabilities are exploited to attack the user and network are presented. The defensive methods to resist such vulnerability and attacks are described.

Keywords: Global System for Mobile Communication (GSM); Security; Prevention; Mobile; Attack

I. INTRODUCTION

Now days, everyone is dependent on a cellular phone (called mobile) to get connected to other person. This connectivity among users is wireless in nature. Such communication is furnished by the standards like GSM, CDMA (Code Division Multiple Access) [1] etc. This wireless link is called the Radio Link. All the communication between users takes place through this radio link and in open wireless medium called the Common Air Interface (CAI) [2]. The concept of Global System for Mobile Communication (GSM) was introduced in 1990 by the European country [2]. From then, this standard accepted widely and utilized by several countries.

GSM network consists of several components which are as follows:

Mobile Station (MS) - This is the device which is used by the GSM user and is portable, small, light-weight and hand-held.

Base Transceiver Station (BTS) - It is the cell tower which is located on the roof by the service providers to provide network to its users. A BTS is connected to MS by wireless radio links.

Base Station Controller (BSC) - This controls one or more BTS and is connected to them. This connectivity is through wires.

Mobile Switching Centre (MSC) – A MSC is connected to number of BSC and manages the call routing process.

Authentication Centre (AuC) – Authentication Centre is responsible for authenticating a legitimate user (subscriber) and also provides 128-bit authentication key to user.

Home Location Register (HLR) – This is a database which stores the user's information and its location information. This provides user an IMSI (International Mobile Subscriber Identity) number to identify its user. In other words, the area to which a subscriber belongs is saved in HLR.

Visitor Location Register (VLR) – This database contains the information about subscriber who visited the area of a particular MSC and stores the IMSI number temporarily.

Operation Maintenance Centres (OMC) – The operation of each MS, BTS, BSC and MSC is monitored and maintained by this centre.

Subscriber Identity Module (SIM) – This is a removable 16k or 32k chip (or a small smart card) which a service provider provides to its subscriber. It is used in MS to access the GSM services like calling, messaging etc.

Public Networks – This consists of networks like PSTN (Public Switched Telephone Network), Data Network, ISDN (Integrated Services digital Network) [3] to which MSC is connected.

Below given figure 1 is the architecture of GSM containing all the above described components.

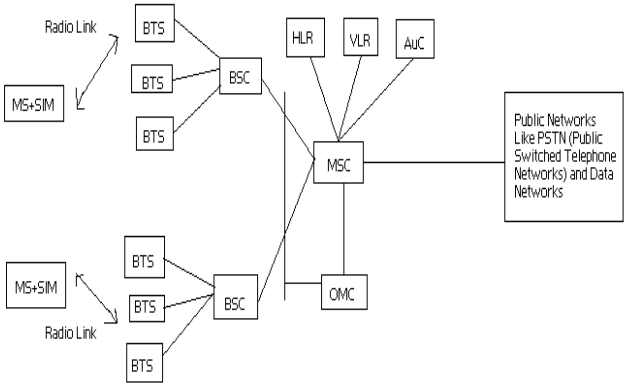

Figure 1- GSM Architecture

GSM communication operates on 900 MHz/1800 MHz standards and uses techniques like FDD (Frequency Division Duplexing) and TDMA (Time Division Multiple Access) [4]. Several generations like 2G (Second Generation), 3G (Third Generation), 4G (Fourth Generation) in GSM has evolved during the past years [5].

Even though the GSM network is utilized by almost every country these days but this standard has some vulnerabilities which are exploited by an intruder to get the access into the network or disturb its operation. The radio link between the MS and BTS is the most crucial point where an intruder takes advantage. Such vulnerabilities are listed in Section II and the way in which this vulnerability is exploited in the form of an attack is described in Section III. The techniques to prevent this vulnerability are discussed in Section IV. Conclusion is given in Section V.

II. VULNERABILITIES IN GSM COMMUNICATION

The GSM standard has some principles of security like subscriber identity confidentiality, use of a SIM as security module, subscriber identity authentication, use of triplets and stream ciphering of user traffic & user control data [17]. An intruder takes an unfair advantage between a legitimate subscriber and the wireless radio link and breaches the security principles of GSM. This breach of principle is due to the vulnerability present in GSM network which are as follows:

A. Wireless Radio Link –

All the communication is taking place through the medium of air. An intruder can easily intercept the communication between two subscribers or between a subscriber and its connected BTS.

B. Insecure A3/A5/A8 Algorithm [6] –

GSM standard uses three algorithms. A3 algorithm is used for authenticating the subscriber through a 128-bit authentication key. A5 algorithm is used for encryption and decryption process and A8 algorithm is used for generating random keys. Many intruder attacks these three algorithms to know about the whole procedure. Every service provider keeps these algorithms confidential. But most of the intruder's targets the algorithm of GSM.

C. One-way Authentication-

In GSM network, only a BTS can authenticate a subscriber but a subscriber cannot authenticate a BTS. The problem arises when an intruder compromises a BTS and imposes attack through this BTS on legitimate subscriber.

D. Cloning of SIM Card –

An intruder can clone (or make a copy of a SIM card) by just deriving a 128-bit authentication key from the legitimate subscriber's SIM card. This results in misusing the SIM for fraudulent purpose.

E. Link between BTS and BSC-

The radio link between MS and BTS is in encrypted form but the other links in the GSM architecture like (BTS-BSC link) is not encrypted and can be easily attacked by an intruder.

F. No Integrity of Data-

In GSM standard, the authentication and confidentiality of a subscriber is maintained but there is no security provided for integrity of the data. An intruder can easily change the data with some fake data.

III. ATTACKS ON GSM NETWORK

The vulnerabilities which are described in previous section are exploited by the intruder in order to attack the network. Such attacks are discussed below-

A. Attack on A3/A5/A8 –

Numerous attacks has come into picture which focuses the three algorithm of GSM network. Reverse engineering attempt on algorithm to break them and access the information about a legitimate subscriber. An attack discovered by Ekdahl and Johansson [7] in 2001 which was based on the correlation attack. This attack is based on the ciphers and the key stream bit. Another attack which is the improvement of attack discovered in which does not need any computational time but needs the memory to operate [8].

B. Attack on BTS –

An intruder can easily compromise a BTS by physical access or through radio link. A fake BTS can compromise a legitimate MS and also can send fake or malicious information to MS through radio link. This problem arises because of one-way authentication of MS-BTS as described in previous section.

C. Attack on SIM –

Any intruder can get access to SIM card of a subscriber and can make a clone of a SIM. Cloning of a SIM card requires authentication key. Intruder can achieve this key by trying random methods on the SIM.

D. Denial of Service (DOS) Attack on MS –

A fake BTS or even a compromised MS can send number of fake request in order to make the MS procedure slow or even can keep it busy in other un-useful operation so that it cannot reply or perform any genuine operation. This results in unavailability of a MS so that it denies the services to the subscriber.

E. Man-in-the-Middle Attack –

This attack can be implemented if the intruder can intercept the communication between two legitimate equipments. In this case, intruder can receive the information from one subscriber and change it and then passes it to other in order to disturb the operations. In [9], the intruder portrays as a fake BTS to a victim MS and to behave as a victim to the real network. In this way, intruder tries to connect the MS to fake BTS. The figure 2 given below can explain the scenario in this attack

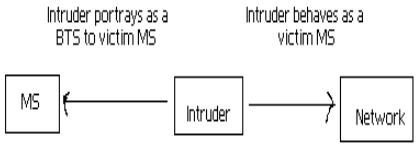

Figure 2 Man-in-the-Middle Attack

F. Attack on Radio Link –

The radio link through which a subscriber communicates can be intercepted by an intruder. Even the communication between the MS-BTS can get trapped by intruder to achieve the information and use for other fraud purpose.

G. Attack on SIM/ME Interface –

As the interface of SIM/ME is not protected; the SIM interface can get connected to other terminal emulator if the SIM is removed from one MS to another while the call is not in progress. This gives chance to intruder to tap the messages on the MS and SIM.

H. Jungle Attack –

Parosh Aziz Abdulla, Jonathan Cederberg, and Lisa Kaati [10] discovered the jungle attack which a graph represents all the possible ways in which an intruder can achieve his goals. In this, a prototype tool has been utilized to construct and analyze the attack.

IV. DEFENSIVE TECHNIQUES FOR GSM ATTACKS

The attacks described above can be prevented by the following discussed methods:

A. Security against One-way Authentication –

A protocol called TESLA is proposed which provides two-way authentication. i.e. MS can also authenticate the BTS or whole network. This protocol helps in reducing the call set up time and the bandwidth utilized during the call connection. Moreover, it reduces the memory overhead in the VLR by the use of concurrent acquisition. Through this way, bilateral authentication of MS-BTS is provided [11].

Another protocol proposed in which the problem of one-time authentication of MS-VLR is removed. The proposed protocol helps the MS in authenticating the VLR. In this protocol, MS joins VLR for the first time and asks for authentication. For subsequent authentication, MS joins the same VLR but at some other time. Through this protocol, efficient authentication is achieved at all the time [12].

B. Security against insecure algorithms -

An enhanced version of A5 algorithm is proposed to improve its security against attacks like correlation attack, algebraic attack and linear approximation attack. This algorithm overcomes the weakness due to weak combining function and poor clock-controlled mechanism. The problem of sparseness in A5 is removed by altering the feedback connection [13].

C. Security against BTS-BSC link –

The solution against this problem is to encrypt voice GSM data call CSW (Circuit Switched Data). Packet switching (GPRS, EDGE) can also be used in encrypting the link from BTS to other network part. Diffie-Hellmen Key agreement is used for both the switching methods [14].

D. Security against Users and Network –

An encryption algorithm is proposed which introduces security at user's end. This algorithm encrypts the speech before it enters in the GSM mobile phone. Encryption starts from the microphone of the mobile phone and then transmits this encrypted signal. This signal is decrypted and then sends it to the speaker of the receiving phone [15].

An architecture is proposed for improving the security of GSM users. In this, the subscriber type judgement, network information sharing and authentication procedure are discussed and improved in order to provide security for the present GSM users. This architecture enables the GSM users to upgrade them to access the UMTS (Universal Mobile Telecommunication Systems) network by creating a hybrid network [16].

V. CONCLUSION

In this paper, all the vulnerabilities and the way to exploit those in order to implement attack in the GSM standard has been discussed in Section II and III respectively. And the method which prevents such attacks is described in Section IV. All the methods are robust enough and can resist the attack described in previous section. Moreover, there can be other measures also which can protect the security principles of GSM standards.

The problem in the GSM network and the security solution offered to such problems are discussed above. All these issues and solutions can be summarized which is given below in table I.

TABLE I Summarized Issues in GSM and Solutions

S. No.	Security Provided to	Solution Offered
1.	One-way Authentication	TESLA Protocol [11], Protocol for Subsequent Authentication [12]
2.	Insecure Algorithm	Algorithm by altering feedback Connection [13]
3.	BTS-BSC Link	Circuit Switching, Packet Switching [14]

4.	Users and Network	Speech Encryption at user's end [15] and GSM user's access to a secure network via UMTS [16]

VI. ACKNOWLEDGMENT

We, Radhika Saini and Mohit Wadhwa, would like to thank our college, Ambedkar Institute of Technolgy (situated at New Delhi) for providing us adequate resources to make this paper. We would also like to thank our guide Mrs. Manju Khari for her valuable suggestions and support.

VII. REFERENCES

[1] Tse, D. and Viswanath, P."Fundamentals of Wireless Communication" ISBN: 9780521845274, Cambridge University Press, 2005

[2] S. Rappaport,T. "Wireless Communication – Principles and Practice" Second edition, Pearson Education ISBN 81-203-2381-5, 2005

[3] Integrated Services Digital Network (ISDN) http://www.cisco.com/US/docs/net_mgmt/active_network_abstraction/3.7.1/reference/guide/isdn.html Link visited on March 2011

[4] Multiple Access Techniques- TDMA, FDMA http://www.wtec.org/loyola/wireless/02_04.html Link visited on March 2011

[5] Wireless Generations - 1G, 2G, 3G, 4G, 5G http://hubpages.com/hub/3G-and-4G-Mobile-Services Link visited on March 2011

[6] GSM Algorithms – A3, A5, A8 http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsn_security/gsm_security_algorithms.htm Link visited on March 2011

[7] Ekdahl,P. and Johansson, T. "Another Attack on .A5/11" IEEE 2001

[8] Maximov, A. Johansson, T and Babbage,S. "An Improved Correlation Attack on A5/1" SAC 2004, LNCS 3357, pp. 1–18, 2005 Springer- Verlag Berlin Heidelberg 2005

[9] Meyer,U.and Wetze,S. "On the Impact of Gsm Encryption and Man-in-the-Middle Attacks on the Security of Interoperating Gsm/Umts Networks" IEEE 2004

[10] Abdulla, P. Cederberg, J., and Kaati, L. "Analyzing the Security in the GSM Radio Network Using Attack Jungles" ,Springer, ISoLA Part I, LNCS 6415, pp. 60–74, 2010

[11] Fanian, A. Berenjkoub, M. and Gulliver, T. "A New Mutual Authentication protocol for GSM Networks" IEEE 2009

[12] Chang, C. Lee, J. and Chang,Y. "Efficient Authentication Protocols of GSM" Computer Communication, Elsvier 2005

[13] Ahmad, M. and Izharuddin "Security Enhancements in GSM Cellular Standard" IEEE 2008

[14] Bouska, P. and Drahansky, M. "Communication Security in GSM Networks" International Conference on Security Technology, IEEE 2008

[15] Islam, S. and Ajmal, F. "Developing and Implementing Encryption Algorithm for Addressing GSM Security Issues, IEEE 2009

[16] Lei, Z. Shize, G. Kangfeng, Z. and Zhongxian, L. "Design of a High Security GSM/UMTS Inter-system" 1st International Conference On Information Science and Engineering (ICISE2009), 2009

[17] Pagliusi,P."A Contemporary Foreword on GSM Security" Springer-Verlag Berlin Heidelberg 2002