A REVIEW OF SECURITY ISSUES AND MITIGATION MEASURES IN GSM

Gurjeet Kaur*

Pawansupreet Kaur*

Dr. Krishan Kumar Saluja**

ABSTRACT

Under European telecommunication Standards Institute (ETSI), GSM is named as "Global System for Mobile communication". It is a globally accepted standard for digital cellular communication. Global System for Mobile (GSM) is a 2G-3G cellular standard developed to cater voice services and data delivery using digital modulation. Its aim was to replace the analog system. Today many users all over the world use GSM. GSM provides Tele-services i.e telecommunication services that enable voice communication, bearer services i.e Short Messaging Service (SMS), Supplementary Services i.e call related services. Security of GSM is crucial .With the greatest number of users worldwide GSM suffers from various security problems. This paper describes all the existing security mechanisms in GSM and security shortfalls and various attacks on GSM networks which include Authentication, Encryption, Equipment Identification and Subscriber Identity Confidentiality, Denial of service Attacks, Brute force attack, Replay Attack as well as the manifestation of network vulnerabilities including SMS attacks, encryption and signaling attacks and security measures to prevent GSM network from these attacks.

Keywords: *Short message service security, mobile communication, Global System for Mobile Communication.*

*Department of Computer Science, S.B.S.College of Engineering & Technology, Ferozepur, India.

**Associate Professor, Department of Computer Science, S.B.S.College of Engineering & Technology, Ferozepur, India.

I. INTRODUCTION

GSM stands for **G**lobal **S**ystem for **M**obile Communication and is an open, digital cellular technology used for transmitting mobile voice and data services. The GSM emerged from the idea of cell-based mobile radio systems at Bell Laboratories in the early 1970s.The GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard. The GSM standard is the most widely accepted standard and is implemented globally. The GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. The GSM makes use of narrowband TDMA technique for transmitting signals. The GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates. Presently GSM support more than one billion mobile subscribers in more than 210 countries throughout of the world. The GSM provides basic to advanced voice and data services including Roaming service. Roaming is the ability to use your GSM phone number in another GSM network. A GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band [1].GSM is developed by Group Special Mobile (founded 1982) which was an initiative of CEPT (Conference of European Post and Telecommunication).The aim was to replace the incompatible analog system .Presently the responsibility of GSM standardization resides with special mobile group under ETSI (European telecommunication Standards Institute).Full set of specifications phase-I became available in 1990 .Under ETSI, GSM is named as " **G**lobal **S**ystem for **M**obile communication ".[1]Today many providers all over the world use GSM (more than 135countries in Asia, Africa, Europe, Australia, America).More than 1300 million subscribers in world and 45 million subscriber in India.

II. OVERVIEW OF GSM NETWORK ARCHITECTURE

The GSM network is divided in to several functional entities that have specific applications [2]. Figure 1 shows the major components of the GSM network. The GSM Network can be divided in to three major parts: The Mobile Station (MS), the Base Station Subsystem (BSS).

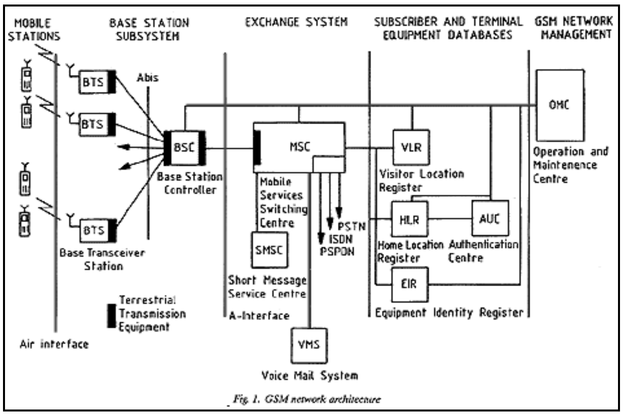


Fig.1GSM Network Architectur

GSM includes MS, BSS, Switching System[3].

A. Mobile Station

The Mobile Station is made up of two entities:

1. Mobile Equipment (ME): Portable, vehicle mounted, hand held device uniquely identified by an **IMEI** (International Mobile Equipment Identity).It is used for Voice and data transmission .

2. Subscriber Identity Module (SIM): Smart card contains the International Mobile Subscriber Identity (**IMSI**).It allows user to send and receive calls and receive other subscribed services. It is protected by a password or PIN. It can be moved from phone to phone – contains key information to activate the phone.

B. Base Station Subsystem

All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

1. Base Station Controller (BSC) The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

2. Base Transceiver Station (BTS) The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

C. The Switching System The switching system (SS) is responsible for performing call processing and subscriber-related functions. The switching system includes the following functional units.

1. Home Location Register (HLR) The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, he or she is registered in the HLR of that operator.

2. Mobile Services Switching Center (MSC) The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling

3. Visitor Location Register (VLR) The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR.

Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

4. Authentication Center (AUC)_A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protects network operators from different types of fraud found in today's cellular world.

5. Equipment Identity Register (EIR) The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.

III. GSM NETWORK AREAS

In a GSM network, the following areas are defined:

A. Cell*:* Cell is the basic service area: one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

B. Location Area: A group of cells form a Location Area. This is the area that is paged when a subscriber gets an incoming call. Each Location Area is assigned a Location Area Identity (LAI). Each Location Area is served by one or more BSCs.

C. MSC/VLR Service Area*:* The area covered by one MSC is called the MSC/VLR service area.

D. PLMN*:* The area covered by one network operator is called PLMN. A PLMN can contain one or more MSCs[1].

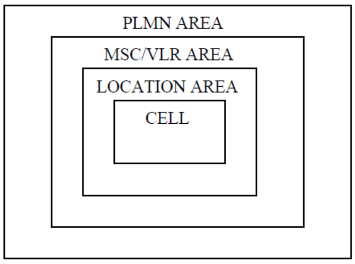


Fig 2. GSM Areas

IV. GSM SERVICES

Three basic types of services offered through GSM [1]

- Telephony (also referred to as teleservices) Services
- Data (also referred to as bearer services) Services.
- Supplementary Services

A. Teleservices or Telephony Services*:*

Teleservice utilises the capabilities of a Bearer Service to transport data, defining which capabilities are required and how they should be set up.

1. Voice Calls*:*

The most basic Teleservice supported by GSM is telephony. This includes Full-rate speech at 13 Kbps and emergency calls, where the nearest emergency- service provider is notified by dialing three digits. A very basic example of emergency service is 911 service available in USA.

2. Videotext and Facsmile*:*

Another group of teleservices includes Videotext access, Teletex transmission, Facsimile alternate speech and facsimile Group 3, Automatic facsimile Group 3 etc.

3. Short Text Messages:

SMS (Short Messaging Service) service is a text messaging which allow you to send and receive text messages on your GSM Mobile phone. Services available from many of the world's GSM networks today - in addition to simple user generated text message services - include news, sport, financial, language and location based services, as well as many early examples of mobile commerce such as stocks and share prices, mobile banking facilities and leisure booking services.

B. Bearer Services or Data Services

Using your GSM phone to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

C. Supplementary Services

Supplementary services are provided on top of teleservices or bearer services, and include features such as caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

- Call related services :
- Call Waiting- Notification of an incoming call while on the handset
- Call Hold- Put a caller on hold to take another call
- Call Barring- All calls, outgoing calls, or incoming calls
- Call Forwarding- Calls can be sent to various numbers defined by the user
- Multi Party Call Conferencing - Link multiple calls together
- CLIP – Caller line identification presentation
- CLIR – Caller line identification restriction
- CUG – Closed user group.

V. EXISTING SECURITY MEASURES IN GSM

A. Authentication

When a new subscriber is registered in the GSM network, the mobile system is given a 128 bit subscriber authentication key K_i , and the telephone number or international Mobile Subscriber identity (IMSI) which are used in the network to identify the Mobile System. The Authentication algorithm is A3 algorithm**. [4]**The K_i and the IMSI are stored in both the mobile and Authentication Center (AUC). This uses the K_i and IMSI, which are inputs to the A3 algorithm to calculate the 32-bit identification parameter called the Signal Response (SRES).

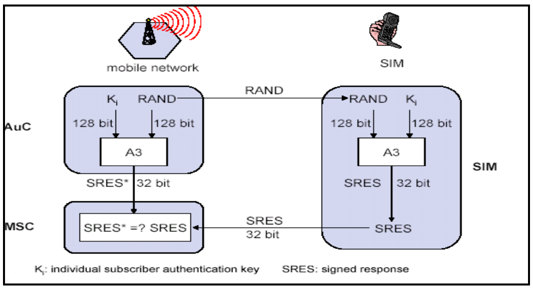


Fig .3 Authentication in GSM

In actual sense, A3 generates 128-bit output but only the first 32-bit form the SRES. SRES is calculated as a function of K and a 128-bit random number(RAND) generated by AUC as shown in Figure 4 and then stored in the HLR for use in set-up procedures.Set-up or registration will not be accepted until authentication, as in Figure 0 has been performed. Using the mobile system's IMSI, the MSC fetches the corresponding RAND and SRES from the HLR. RAND is sent to the mobile system, which uses its stored K value to calculate SRES. It then returns the calculated SRES to the MSC, where it is compared with the SRES value received from the HLR. If the values tally, the set up is accepted, if not, it is rejected.

B. Encryption.

GSM, which is a form of radio communication, can be intercepted by practically anyone in the immediate surroundings. Therefore, protection against eaves dropping is an important service in a mobile network. This is done by using an encrypted air interface both for traffic and control channels. Since encryption of voice requires digital coding, it cannot be used in analog mobile networks[5].

The encryption algorithm used in GSM voice ciphering is a stream cipher known as the A5 algorithm. Multiple versions of A5 exists which implement various levels of encryption. They are

- A5/0 which utilizes no encryption
- A5/1 which is the original A5 algorithm used in Europe
- A5/2 which is a weaker encryption algorithm created for export and used in the United States.
- A5/3 which is a stronger encryption algorithm created as part of the Third Generation Partnership Project (3GPP)[6].

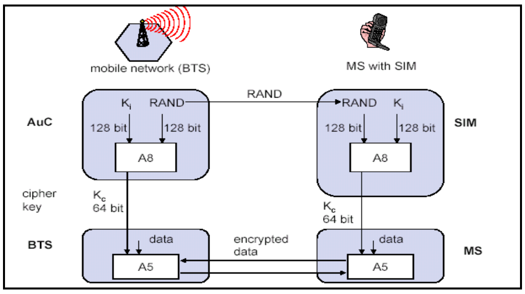


Fig.4 Encryption in GSM

In A5/1 and A5/2, voice encryption is done using the calculated session key K_c, based on K_i and RAND by the AuC, in addition to the SRES it generates as shown in Figure 7. This key is stored in the HLR together with the RAND and SRES.

The mobile system also calculates a K_c values based on both the RAND value received from the MSC and on the K_i value stored in the mobile system. If the result of the authentication is approved, the MSC will also store the encryption key in the base station (via the BSC) for use in encryption/ decryption operations. The BSC then sends a "test signal" (encryption mode command) to the mobile system. In response, the mobile system should generate an encrypted signal (encryption mode complete) which if the BSC can interpret it, permits continued signaling and communication.

C. Equipment Identification.

Equipment identification is a form of checking the mobile systems used within in the network. This is to ensure that no stolen or otherwise unauthorized mobile systems are used in the network. To this end, every mobile system in the network is provided with a tamper proof equipment number in the manufacturing process, called International Mobile Equipment Identity (IMEI). During the set-up phase, the MSC can request this number from the mobile system and then send it on for checking in the EIR[4]**.** If the number is barred or unknown, the set-up attempt is rejected

D. Subscriber Identity Confidentiality

Subscriber identity confidentiality means that the operator tries to protect the users telephone number (the IMSI) from unauthorized tapping. A temporary mobile subscriber number (TMSI) is used in the dialogue between the mobile system and the network, except for the first contact attempt in a set-up phase. The MSC gives the mobile system a random IMSI for each set-[4].

VI. VARIOUS ATTACKS ON GSM

A. SIM Attacks

The GSM SIM was originally designed to be tamper proof, copy proof and generally as difficult to break as possible. Overtime, series of issues have been discovered that have made the SIM less secure.SIM card using freely available tools and eventually "clone" a SIM[3]. SIM cloning which is made by breaking the COMP 128 algorithm could take up to 8-15 hours and requires physical access to the SIM [7]. Nevertheless; a tool has been discovered to be popularly in use known as the Dejan Karavic's SIM Scan. IBM researchers used 1000 randomly chosen inputs even though 500 random inputs should be sufficient and this reduces the amount of time to clone a SIM to minutes at most, seconds at best.

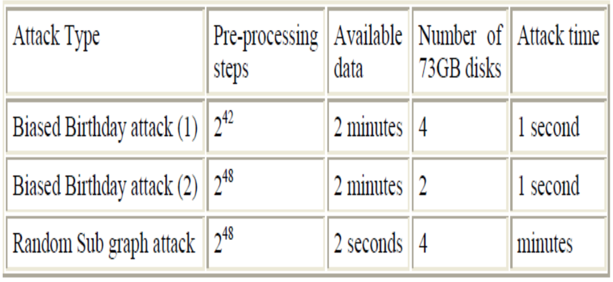
Researchers in IBM discovered a way of using side channels to obtain Ki [8].

B. Encryption Attacks

Data in the GSM network have been said to be encrypted using the A5/1 or A5/2 encryption algorithm. A5/0 uses no encryption and it is deployed in countries with political obstacles in supplying cryptographic hardware. Examples of such are the former Soviet Union countries and some countries in the Middle East. A5/1, which is said to be the stronger of the two algorithms in use, has been studied by cryptographic professionals and mathematicians and has been discovered to be highly susceptible to cryptanalytic attacks.

Researchers like M. Briceno, R. Anderson, M. Roe and J. Golic [9] had carried out various forms of attacks on the algorithm and their research have severed as the back ground for the most popular attacks on the algorithm. These attacks are the Baised Birthday Attack and the Random Sub graph Attack. The first attack requires two minutes of data and one minute of processing time while the second attack two seconds of data and several minutes of processing time [7]**.** For each of these attacks, there are many trade-off parameters and three of them could be summed up in Table 1.

I. Table



Attack Type	Pre-processing steps	Available data	Number of 73GB disks	Attack time
Biased Birthday attack (1)	2^{42}	2 minutes	4	1 second
Biased Birthday attack (2)	2^{48}	2 minutes	2	1 second
Random Sub graph attack	2^{48}	2 seconds	4	minutes

(Baised Birthday Attack and the Random Sub graph Attack.)

As earlier mentioned, the COMP 128 algorithm used for A3/A8 has many flaws which will be discussed later in this section. This makes it possible to obtain the Ki and the IMSI and these can be successfully used to program another

C. SMS Attacks:

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non repudiation was omitted during the design of GSM architecture. In this section we discuss some of the security problems of using SMS.

When the SMS is used as a bearer for mobile business applications which need high security, e.g. payment, shopping or mobile betting, there is a possibility that an attacker might capture the message context which includes user privacy, or amend the message causing a fraudulent transaction.

1. SMS disclosure

With no protection on confidentiality and integrity, SMS messages could be intercepted and snooped during transmission and the user privacy is at stake. Although SMS messages are encrypted when it is sent across the air, the encryption algorithm chosen for SMS message encryption must be the network-specific algorithms, such as A5 for GSM. These algorithms have been susceptible to cryptanalysis and [10] demonstrated that the secret key of A5 could be cracked in minutes. The SMS messages sent over the SS7 networks are unencrypted; moreover, most Service Providers communicate with the SMSC via SMPP SMPP (Short Message Peer to Peer [11] protocol over the Internet, and the cryptographic protection is not available for SMPP protocol. So, the attacker could read or amend the message content in some way. In addition, SMS messages are stored as plain text in the SMSC before they are successfully delivered to the intended recipient, these messages could be viewed or amended by users in the SMSC who have access to the messaging system. Furthermore, lack of protection of the BSS makes it possible to read and/or manipulate SMS messages in transit.

2. SMS spoofing

SMS spoofing is a very feasible threat because an attacker can manage to inject SMS messages into the messaging network with a 'spoofed' originator IDs. An attacker can spoof a legitimate ME by sending a SMS message from the internet with the correct headers. The ME isn't able to detect that it comes from the internet and a transaction will be conducted according to the attacker.

If an attacker knows the authenticating information of a user, he could consist in impersonating the genuine user to conduct a transaction with a legitimate AS. The authenticating information of the user can be eavesdropped easily as mentioned in Section above section.

3. Replay of messages

The possibility exists that an attacker arranges for authentication request and/or authentication response messages to be replayed. Though an attack on the reply of an authentication request message does not seem obvious, replaying an authentication response could be a more serious vulnerability. If such a replay is possible, it can be used to impersonate a legitimate user and hence authenticate a false transaction. Please note that this attack will not work if there exists an authentication request number (anti-replay mechanisms) that must be included in the response.

6. Brute Force Attack

Brute Force Attack comes under cryptography technique for find an secure key from encrypted data. I.e. a brute force attack consists of trying every possible code, combination, or password until you find the right one.

In brute force attack it systematically checks all possible keys until the correct key is found. So it totally depends upon the key length as longer keys exponentially more difficult to crack the password than shorter ones. This is the most used method for cracking password [12]

7. Denial-of-Service Attack

Traditionally a denial-of-service (DoS) attack is an attempt to make a computer resource unavailable to its intended users.

One such method is to flood a network, thereby preventing legitimate network traffic. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. Such an attack is extendable to any mobile environment. A mobile device is rendered ineffective should a mobile device be flooded with this type of SMS messages. Furthermore, should a “Silent” SMS DoS attack [13] takes place on the handset, the intended victim would be oblivious to the attack. The only visible symptom would be an abnormal decline in battery charge capacity and the inability to receive calls etc. This ineffectiveness of the handset is due to SMS messages making use of the signaling layer, also used in performing other network events. Not only will a “Silent” SMS consume battery power but it will clog the signaling channel. This may be the reasoning behind the motivation in performing a “Silent” DoS attack. Primarily it may be done for economic advantage to elude another party to communicate, or may be used to ensure that a given party is not notified of some events.

VII. SUGGESTIONS ON MITIGATING SECURITY THREATS

Most of the security threats in the GSM Network could be subdued even though it might be cost intensive. Signaling security treats require physical access to the signaling link and/ or operator's console. Hence operators should establish regular assessments to ensure that other systems (cables or SGSN in the GPRS Network) are not at risk of compromise from the attackers. The cost associated with compromise of operator systems could be immense and is unlikely to be detected unless the service is interrupted [7]**.**

In the Authentication Center, the whole authentication could be broken down in to several security domains, each having its own unique security configuration. This will obviously be cost implicative but the system is less vulnerable to attack and this approach confines the damage of a compromised certification within a singe security domain. Unless all certification centers are compromised, no key can be forged [14]**.**

In securing the A3 algorithm from crypto attackers, the most efficient approach will be to use a more cryptographically secure algorithm. This will imply new SIM cards to all subscribers and updating HLR software; only when this is done can SIM cloning, which is one of the most dangerous attacks, be minimized the most. Here, there is no need for hardware or software manufacturers' support or permission from the GSM Consortium. The main draw back, however, is the cost implication and the tedious tasks of redistributing new SIM cards to "all almost 1 billion" GSM subscribers[15]. For the A5 crypto attacks, a strong encryption is required. This will prevent the attacker from recording transmitted frames since he most likely will not be able to crack them. Implementing this will involve the equipment manufacturer and the GSM Consortium. The hardware and software manufacturers will need to release new versions [16].

A. Security measures for secure SMS

The following subsections describe how the Secure SMS protocol conforms to the general security requirements.

1. Confidentiality

This is achieved by encrypting the message using a symmetric secret one-time password. The one-time password is only shared between the user and the bank server. The strength of the confidentiality depends on the security strength of the passwords generation algorithm used and the strength of the ciphering algorithm used. It is assumed that only the authorized user will know his/her list of passwords and the passwords are never shared with other people.AES algorithms were considered to perform the message encryption. NSA15 has conducted a review and analysis of using AES to protect classified information. AES is an NSA approved cryptographic algorithm to be used for United States national security information and system at all classification levels [17]. The use of 128 bits key length is approved to be sufficient to protect classified information up to the US national secret level.

2. Integrity

The message digest is the hashed value of the message content calculated server application and the mobile phone application. If the content is altered during transmission, the hashing algorithm will generate a different digest value at the receiver side. If the digests mismatch, the receiver will know that the integrity of the message has been compromised. The strength of the integrity checks depends on the strength of the algorithm used to generate the digest value and it also depends on the strength of the encryption algorithm used to hide the confidential data. A message digest is use to maintain the message integrity for each SMS message. The speed of calculating the message must be efficient and it must calculate the message digest relatively fast in the mobile phone environment. The message digest calculation algorithm used for this project is SHA1.

3. Authentication

For the receiver to authenticate the user, the user must provide his/her authentication detail(s) to the receiver. This authentication process is performed by validating the message PIN with the receiver stored PIN. The PIN is previously selected by the user when the user registers for a mobile banking account. The strength of the authentication depends on the password selection strategies used. The authentication detail (PIN) of the user is protected within the encrypted banking details. The attacker cannot read the authentication detail of the user therefore the attacker cannot use the authentication detail to perform masquerading attacks.

4. Non-Repudiation

Only the account holder and the bank server are supposed to have the one-time password. The bank server does not generate the same one-time password more than once. Therefore every onetime password is unique in the server s database. Each pair of one-time password and sequence number is only allowed to be used for a single user. Therefore the user cannot deny not sending the message because only that specific user has that unique pair of password and sequence number to encrypt the message. If the bank server can use the same sequence-password pair to decrypt the message, then it indicates that user must have sent the message.

5. Availability

The availability of this protocol depends on the availability of the cellular network. The time it takes for a message to be delivered depends on the density of network operator base towers. The number of transactions that the server can handle at once depends on the hardware capability. If the server s hardware can handle multiple incoming messages then the server can perform multiprocessing to accommodate for more requests. The protocol has no restriction on the type of hardware needed. Therefore it is up to the developers to decide the hardware specifications.

6. Replay Attacks

Assuming the attacker managed to get hold of the transmitting message and he/she performs replay attacks. For every received message, the bank server needs to check for the sequence number for the specific account identifier given in the received message. If the message s sequence number does not match the sequence number from the bank database, then the message is discarded.

To further enhance replay attacks prevention, the bank server stores every received message into the database16. When a new message is received, the bank server can check it against those messages that are stored in the database.

To test for replay attacks, we deliberately send the same messages to the bank server multiple times. The server received the first message and performed the transaction, when the next identical message is received; the message is ignored and discarded because of the received message is already exist in the database.

7. Masquerading Attacks

Masquerading attack is when the attacker pretends to be a legitimate account user. It is assume that the attacker managed to get hold of the legitimate account identifier. The attacker cannot perform banking transaction because he does not have the account identifier s PIN. We further assume the attacker managed to get hold of the user s PIN.

The attacker still cannot perform bank transaction because the attacker does not have the required One-Time Password to correctly encrypt the banking details for the bank to interpret.

We then used an invalid One-Time Password to encrypt the banking message. When the message gets delivered to the bank server, the server cannot decrypt the message using the database password, therefore the message decryption failed. Since the message cannot be decrypted by the bank server, the bank server does not have to check for the message
PIN because it cannot be read.

8. Increasing Security against a Brute Force Attack

From the example above, PIN security could be increased by:

- Increasing the PIN's length
- Allowing the PIN to contain characters other than numbers, such as * or #
- Imposing a 30 second delay between failed authentication attempts
- Locking the account after 5 failed authentication attempts

A brute force attack will always succeed, eventually. However, brute force attacks against systems with sufficiently long key sizes may require billions of years to complete.

REFERENCES

1. http://www.tutorialspoint.com/gsm/gsm_overview.htm
2. Wetten, L. A. (2003), A Study of GSM Technology in Nigeria and its Place in the International Scene, Unpublished (B.Eng) Final Year Project, Federal University of Technology, Minna.
3. Paul Yousef *"GSM-Security: a Survey and Evaluation of the Current Situation"* Master's thesis Linköping, Mars 2004
4. (www.ericsson.com/support/telecom/part-d/d-6-4.shtml)
5. (www.ericsson.com/support/telecom/part-d/d-6-4.shtml
6. (www.gsmsecurity.com/faq.shtml)
7. Lord, S. (2003), "Modern GSM Insecurities", X-Force Security Assessments White Paper.
8. www.research.ibm.com/resources/news/20020507_simcard.shtml.
9. (www.cryptome.org/a51-bsw.htm)
10. A. Biryukov, A. Shamir, D. Wagner, Real Time Cryptanalysis of A5/1 on a PC, 2000. http://cryptome.org/a51-bsw.htm. Accessed on: 13 February 2007.
11. SMS Forum, Short Message Peer-to-Peer Protocol Specification version 5.0, (http://www.smsforum.net.)
12. http://www.tech-faq.com/brute-force-attack.html.
13. N.J Croft, M.S Olivier "A Silent SMS Denial of Service (DoS) Attack".Information and Computer Security Architectures (ICSA) Research Group South Africa.
14. Isomaki, M. (1999), "Security in the Traditional Networks and in the Internet", White Paper, University of Technology, Helsinki.
15. Laurie, P. (1999), "GSM Interception", White Paper, University of Technology, Helsinki

16. www.chiark.greenend.org.uk/pipermail/ukcrypto/002552.html

17. Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison ”*Security of Mobile Banking”* Data Networks Architecture Group Department of Computer Science University of Cape Town Rondebosch 7701, South Africa