ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

A Review on Security in Mobile Communication Technology

Shaik Aleem Ur Rehaman[1], Tanveer Baig Z[2], Prithvi G Hardikar[3], Mr.Saqib Rashid[4],Mr.Zahid Nazir Moon[5]
Yassar arfath khan[6]

UG Students, Dept. of Electronics and communication Engineering, HKBK College of Engineering, Bangalore, India

ABSTRACT: This papers aims to provide an overview of security and its needs in mobile communication technology The objective of mobile communications is to provide truly Anytime, Anywhere communication. The GSM subscriber is provided with a SIM which is used to identify and authenticate the subscriber over the networks. The ME has a unique number coded into it when it is manufactured. This can be checked against a database every time the mobile makes a call to validate the actual equipment. The subscriber is authenticated by use of a smart card known as a Subscriber Identity Module (SIM), again this allows the network to check a MS subscriber against a database for authentication.

KEYWORDS: Global System for Mobile Communication (GSM), Subscriber Identity Module (SIM), Mobile Equipment(ME)

I. INTRODUCTION

The AMPS cellular service was available in United States in 1983. AMPS is essentially generation 1 analog cellular system in contrast to generation 2 digital cellular systems of GSM and CDMA (1S-95) The economically most successful wireless application in the first half of the 20th century was radio broadcast. There is one transmitter, the so-called radio station. Information, such as news, music, etc. is transmitted from the radio station to the receiver equipment, the radio device. Although mobile telephony can be seen in broad sense as the wireless communication and wireless services can be offered through various technologies like GSM, CDMA etc. but here we will talk about GSM (Global System for Mobile Communication) as a wireless communication technology. Global System for Mobile communications (GSM) is the most widely used wireless technology in the world today. GSM is a second generation (2G) wireless technology that provides high-quality voice and circuit-switched data services in a wide variety of spectrum bands. GSM pioneered many of the world's most popular data services, such as Short Message Service (SMS) and Multimedia Message Service.The most important part of the communication network is circuit switched network and packet switched network.Circuit-switched PSTN networks, traditionally controlled by the telecom operators are less prone to risks as compared to a packet-switched network based on an open protocol like the IP. However, due to the growing demand for data and video services and the limitations of the circuit-switched technology, telecom operators find it economically prohibitive to expand their circuit-switched networks to meet demand. This has led to a gradual move towards the adoption of packet-based switching technology. Newer 2G and 3G mobile phone systems like GPRS, EDGE and HSPA that are designed for data transmissions are also based on packet-based switching technology.Packet-based switching technology used in Next Generation Networks is usually implemented through the use of the IP suite. IP was based on open standards and not originally designed for security implementations. The weaknesses in the IP have been exploited since long and therefore risks are involved in adopting an IP based network. Both the traditional circuit-switched networks and the packet-based next generation networks are exposed to different threats and attacks – both from external and internal sources – that target the various parts of the telecommunications network. These attacks may be targeted at any part of the telecom network, including the radio path of the access network. Attacks on one telecom operator's network could also spread to multiple networks over the interconnection interfaces.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

A smart phone user is exposed to various threats when they use their phone. In just the last two quarters of 2012, the number of unique mobile threats grew by 26% according to ABI research [1].

II.RELATED WORK

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. Here in the US, digital scanners are illegal. The GSM Alliance of North America has claimed that none of its members use the A5/1 algorithm, opting for more recently developed algorithms. The ISAAC security research group claims it is technologically possible to build a fake base station for roughly. This allows a "man-In the-middle" attack. Essentially, the fake base station can flood the real base station and force a mobile station to connect to it. The base station could then inform the phone to use A5/0 (no encryption) and eavesdrop on the conversationGSM has a lot of security systems to build safe communication.to provide more secure communication and to avoid disclosing of user's identity. This means someone intercepting communications should not be able to learn if a particular mobile user is in the area. Using SIM as security module; Incase SIM card was taken by opponent, there is still PIN code measurement GSM makes use of a ciphering key to Protect both user data and signalling 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. The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data on the fly. Some argue that GSM is not as secure, as publicized. The GSM standard was created in secrecy and 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.

III.ARCHITECTURE OF GSM NETWORK

A GSM network comprises of various subsystems as described below
(1) Mobile Station (MS):
Comprises Mobile Handset and SIM (Subscriber Identity Module)
(2) Base Station Subsystem (BSS):
BTS: Base Transceiver Station
BSC: Base Station Controller
(3) Network Switching Subsystem:
VLR: Visitor Location Register
HLR: Home Location Register
AUC: Authentication Centre
(4)OSS- Operation Support and Subsystem
(5) Interfaces Um – MS to BTS, Abis –BTS to BSC and A – BSC to MSC

GSM Network Structure

Every telephone network needs a well-designed structure in order to route incoming call to the correct exchange and finally to the called subscriber. In a mobile network, this structure is of great importance because of the mobility of all its subscribers. In the GSM system, the network is divided into the following partitioned areas
•Cell (BTS Coverage Area)
•Location Area (LA)
•PLMN (Public Land Mobile Network) service area;
•GSM service area
Fig 1 describes the cell structure. A cell is the smallest geographical coverage area of a GSM network. The coverage area of a BTS is called a Cell. BTS coverage is further divided in to 3 sub-cells, called as sectors. A number of such cells (BTS) are further grouped to form a Location Area (LA).A BTS is further connected to a BSC. A BSC controls a

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

group of BTS. Thus a BSC is controlling one or more Location Areas (LA). A BTS is used to provide radio resources to a GSM subscriber (user) but this is not incorporated with control functionalities. A BSC is provided with all the intelligence which controls a number of BTS and manages the radio resources.

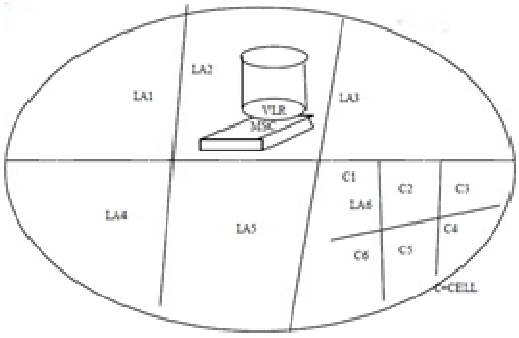

Fig 1. GSM network areas

IV.DIGITAL AIR INTERFACE

The main reasons why GSM uses a digital air interface:
• It is “noise robust”, enabling the use of tighter frequency re-use patterns and minimizing interference problems;
• It incorporates error correction, thus protecting the traffic that it carries;
• It offers greatly enhanced privacy to subscribers and security to network providers.
The VLR controls the allocation of new Temporary Mobile Subscriber Identity (TMSI) numbers and notifies them to the HLR. The TMSI will be updated frequently, this makes it very difficult for the call to be traced and therefore provides a high degree of security for the subscriber. The TMSI may be updated in any of the following situations: Call setup, On entry to a new LAI, On entry to a new VLR.GSM also offers the capability to encrypt all signaling over the air interface. Different levels of encryption are available to meet different subscriber/country requirements. With the authentication processes for both the ME and subscriber, together with the encryption and the digital encoding of the air interface signals, it makes it very difficult for the casual “hacker” to listen-in to personal calls. In addition to this, the GSM air interface supports frequency hopping; this entails each “burst” of information being transmitted to/from the MS/base site on a different frequency, again making it very difficult for an observer (hacker) to follow/listen to a specific call. Although it should be noted that frequency hopping is employed to optimize network performance by overcoming interference problems in busy areas, to increase call quality and capacity. The SIM card, and the high degree of inbuilt system security, provide protection of the subscribers information and protection of networks against fraudulent access. SIM cards are designed to be difficult to duplicate. The SIM can be protected by use of Personal Identity Number (PIN) password, similar to bank/credit charge cards, to prevent unauthorized use of the card. It contains security related information (IMSI, Ki, PIN), other subscriber related information and the algorithms A3 and A8.

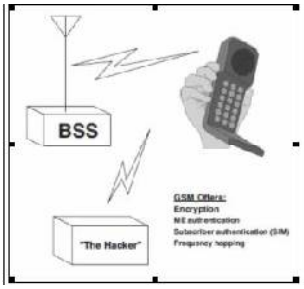

Fig 2.interface between BSS and ME

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

V. NEED FOR SECURITY

The interconnection of the PSTN networks of fixed and mobile phone systems and the next generation network has increased the attack surface of the telecom networks. The wide range of end-user devices that can now connect to the telecom networks has added to the complexity of the networks, thereby increasing the risks and vulnerabilities as well. Telecom operators should adopt a robust, managed security programed to ensure that their networks are protected against malicious attacks, both external and internal, while also ensuring compliance to the local regulatory environment. This requires a holistic approach to implement security measures, based on globally accepted security standards. When the application is installed the signing of this application is verified by a series of certificates. One can create a valid certificate and add it to the list [2].

VI. METHODS FOR SECURITY CONTROL

(a) ACCESS CONTROL

Access Control - enables the OMC System Administrator to change the command partitioning options for all users. Depending on which security area the user has access to, they will be allowed/disallowed options on the OMC user interface that could be used to alter OMC/BSS information. Access control provides a level of safety so that OMC users cannot invoke commands accidentally/maliciously that they are not privileged to use, and also improves the way the OMC works by providing users with a more applicable selection of menu options from which to choose. The security of the OMC system is the responsibility of the System Administrator, who should pay particular attention to the following:

- How many users are on the OMC system
- Which users require special privileges (for example login id omc admin), normal
- OMC software access or restricted OMC software access
- The regular update of OMC user passwords.
- Any network file that contains security related information
- Checking for unauthorized access to the OMC system through the X.25 or LAN interfaces.
- Ensuring that the remote X terminals have screen lock enabled.
- Ensuring that all remote X terminals have a unique local configuration file set up

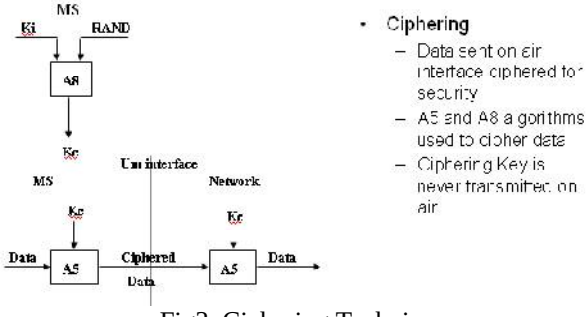

Fig3. Ciphering Technique

(b) ENCRYPTION:

Encryption is a process of a protecting voice or data information from being obtained by unauthorized users. Encryption involves the use of a data processing algorithm (formula program) that uses one or more secret keys (numbers values) that both the sender and receiver of the information use to encrypt and decrypt the information. Without the encryption algorithm and key(s), authorized listeners cannot decode the message .The encryption algorithm is stored on the Sim card program memory .There can be more than one different encryption algorithms in different parts of the World .The BCCH channel of the base system broadcasts a code to tell the mobile station which of the encryption algorithms is in use that particular base GSM installations. The GSM voice privacy encryption process uses the Vernam cipher algorithm (called A5 in type GSM system) that modifies all the data bits that are to be transmitted with an encryption code. The encryption code (cipher mask) continuously varies and is synchronized to the hyper-

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

frame counter at both the base and mobile stations. This produces a random ever changing group of 116 cipher mask bits for each normal burst in the data stream that is synchronized with the hyper-frame counter. While this group of bits appears to be random both the base and mobile stations have properly synchronized copies of it. The cipher mask is added (modulo 2) to the transmit information and flag bits before differential encoding and modulation, and the same cipher mask is "subtracted" (modulo 2) at the corresponding point in the receiver. Thus,a person in the middle who has a radio receiver can receive the bit stream , but cannot understand its correct value without possessing a third copy of the properly synchronized cipher mask. Using a secret number called Kc, that is set to a different value for each call, generates the cipher mask. This number is used together with the hyper-frame counter in a process involving repeated re-arrangement and modulo 2 addition of the bits from the two items. The secret number is derived from the authentication process, described below

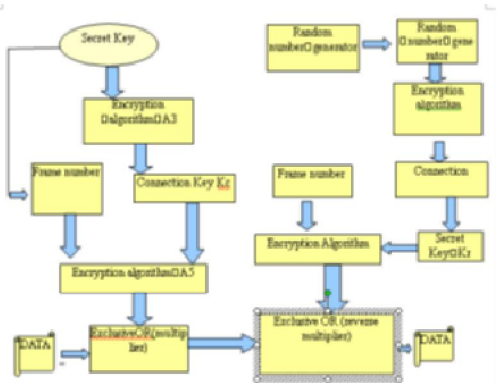

Fig 4.GSM voice channel diagram

Figure 4 shows the basic GSM voice channel encryption process . The encryption cipher mask uses a Kc key , which is created at the beginning of each call, with an A8 encryption algorithm. Throughout the call, the A5 algorithm uses the Kc key to scramble voice data sent to and from the mobile telephone. Since the cellular system has access to the same set of secret information, it generates the same encryption mask as the mobile telephone and uses it to unscramble the voice data before sending it to the land line network.

(c) CIPHERING :

The security function that ciphers the information sent and received by the MS required the cipher key Kc. The generation of the Kc is based on the crypto graphical algorithms A8, and the Ki. Also A8 is located on the SIM.

Ciphering Start Procedure

This ciphering start procedure is initiated from the MSC/VLR by sending the message a cipher mode command the Kc. The Kc will be removed from the message by the BTS before sending it on to the MS, so that the Kc will be never be sent on the air. When the MS receives this message it will be send the message cipher mode complete in the cipher mode using the calculated Kc stored on the SIM card. If the BTS can decipher this message it will be inform the MSC/VLR that ciphering has started.

VII.SECURITY AGENCY

The organization which authorizes interception of calls, and is responsible for handling the results.

MONITORING CENTER AND PROVISIONING CENTER:

The Monitoring center and Provisioning center may or may not be co-located. This Nortel application allows for two configurations; centralized and non-centralized. In the former only a single Provisioning center is required. From this center it is possible to provision a call interception for up to five Security agencies whose Monitoring centers may be remotely located. In the latter configuration one Provisioning center is required per Security agency (sometimes more

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

than one security agency could share a non-centralized CIPC). This Provisioning center performs the provisioning for this and only this Security agency.
A three port conference bridge is used to provide the voice interception capability on the DMS-MSC when combined channel monitoring is used. The ISUP call to the Monitoring centre is one way making the interception action invisible to the target subscriber. All call content is captured from the alerting indication until the communication is disconnected at the target subscriber. The non -target party may be another mobile subscriber, a PSTN subscriber, a network tone, or a network announcement. If both the originator and terminator of the monitored call are target subscribers then two three port conference bridges are used when combined channel is used. One bridge is used to monitor each subscriber. Although the call contents will be the same, they are delivered separately.

VIII. CONCLUSION

The problems encountered by some operators is virtually non-existent and the unscrupulous were quick to recognize this. With some of the first generation systems it has been estimated that upto 20% of cellular phone calls are stolen. Hence the enhancement of security in handsets can reduce the risk of stolen phone calls .we made use of infrastructure provided by BSNL to carry out our research work for this paper.

REFERENCES

[1] BOYD and increased Malware threats help driving Billion Dollar Mobile Security services market 2013, ABI research
[2].Becher 2009, p.66
[3] 24. Geier, Jim. Wireless Network Industry Report 2007, Wireless-Nets, Ltd., 2008.
[4] Goldsmith, Andrea (2005). Wireless Communications. Cambridge University Press. ISBN 0-521-83716-2
[5]Andreas (2005). Wireless Communications. Wiley-IEEE Press. ISBN 0-470-84888-X.
[6]Pahlavan, Kaveh; Krishnamurthy, Prashant (2002). Principles of Wireless Networks – a Unified Approach. Prentice Hall ISBN 0-13-093003-2.
[7]Rappaport, Theodore (2002).Wireless Communications: Principles and Practice. Prentice Hall. ISBN 0-13-042232-0
[8]Rhoton, John (2001). The Wireless Internet Explained. Digital Press. ISBN 1-55558-257-5.
[9]Larsson, Erik; Stoica, Petre (2003). Space-Time Block Coding For Wireless Communications. Cambridge University Press.
[10]Redl, Siegmund M.; Weber, Matthias K.; Oliphant, Malcolm W (February 1995).
[11]An Introduction to GSM. Artech House. ISBN 978-0-89006-785-7.
[12]Redl, Siegmund M.; Weber, Matthias K.; Oliphant, Malcolm W (April 1998). GSM and Personal Communications Handbook.
[13]Artech House Mobile Communications Library. Artech House. ISBN 978-0-89006-957-8.
[14]Hillenbrand, Fried helmed. (December 2001). GSM and UMTS, the Creation of Global Mobile Communications. John Wiley &Sons. ISBN 978-0-470-84322-2.
[15]Mouly, Michel; Paulette, Marie-Bernadette (June 2002). The GSM System for Mobile Communications. Telecom Publishing. ISBN 978-0-945592-15-0.

BIOGRAPHY

1. **Shaik Aleem Ur Rehaman** is currently pursuing his BE in electronics and communication engineering from HKBK college of engineering, Bangalore. He has presented over 40 papers in various national and international conferences.His area of interests are VLSI, Automation ,Telecommunications,Embedded Systems And Robotics.
2. **Tanveer Baig Z** is currently working as assistant professor in Dept of ECE in HKBK college of engineering, Bangalore. His area of specialization is telecommunication.He has presented over 5 papers in various international conference and journals.
3. **Prithvi G Hardikar** is currently pursuing her BE in information science engineering from HKBK college of engineering, Bangalore.Her area of interests are cryptography and JAVA programming. Presenting her first paper.
4. **Saqib Rashid** is currently pursuing his BE in electronics and communication engineering from HKBK college of engineering, Bangalore.His area of interests are Embedded systems and Robotics.
5. **Zahid Nazir Moon** is currently pursuing his BE in electronics and communication engineering from HKBK college of engineering, Bangalore. His area of interest is Networking,Embedded systems and Robotics.