AUTHENTICATION AND SECURITY SOLUTIONS FOR GSM WIRELESS SYSTEMS

[1] Siddhant Mehta, [2] Jitendra Kumar
[1,2]*Electronics and Computers Engineering, Maharishi Dayanand University, India*

ABSTRACT

In this paper, we focus on the authentication as well as the security aspect of the Global System for Mobile communication (GSM) networks,a communication architecture-GSM (originally from Groupe Spécial Mobile) network, used in public-key cryptography for user authentication and stream cipher for message encryption as well as decryption. An authentication protocol and a key generation method present in this architecture. Cryptographic authentication and authorization of the user (the holder of the SIM card) and the terminal equipment as well as the encryption for radio interfaceshows that the authentication protocol is secure and efficient. Results indicate that the key generated method can always produce key strings with infinite period. The objective is to have strong subscriber authentication and data security over the radio interface dependingupon the algorithms selected.In this paper, we investigate the security issues in the mobile communication systemsand focus especially on the security functions of the GSM, the first digital mobile network architecture used for transmitting mobile voice and data services with a brief review of its security problems.

Keywords—*Authentication, cipher, cryptography,decryption, encryption, GSM*

I. INTRODUCTION

1.1 History

The GSM emerged from the idea of cell-based mobile radio systems at Bell Laboratories in the early 1970s and is the name of a standardization group established in 1982 to create a common European mobile telephone standarddeveloped by the European Telecommunications Standards Institute (ETSI).[1]More than 6 billion people worldwide use the Global System for Mobile Communications (GSM) family of technologies. GSM is available in 219 countries and territories worldwide, with a market share of more than 90 per cent.GSM includes one emergency number (112), which can be used in any country of the world.

GSM is the legacy network of the evolution of the third generation (3G) technologies Universal Mobile Telecommunication System (UMTS), also known as WCDMA, and High Speed Packet Access (HSPA). The following diagram represents the GSM family of technologies - the evolution from second generation (2G) GSM and General Packet Radio System (GPRS) to 3G Enhanced Data for GSM Evolution (EDGE), UMTS and HSPA.

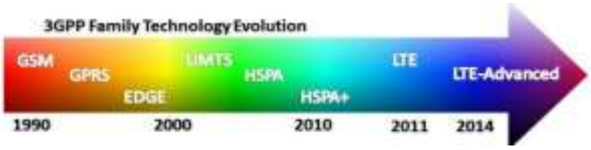

Fig. 1 GSM Family of Technologies

The GSM is a circuit-switched system that divides each 200kHz channel into eight 25 kHz time-slots. The GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmission of signals to carry 64 kbps to 120 Mbps of data rates[1].The GSM provides basic to advanced voice and data services including roaming service. Roaming can be seen as ability to use your GSM phone number on another GSM network ,then digitizes and compresses the data which sends it down via a channel with two other streams of user data into its each own time slot. It functions at either 900 MHz, or at 1,800 MHz frequency band.[6]

II. Why GSM?

- International roaming
- Improved spectrum efficiency.
- Low-cost mobile sets and base stations (BSs).[1]

It's much easier to swap phones on GSM networks, because the carriers put customers' information on a removable SIM card. Take that card out, insert it intoanother different phone and the new phone now has your same existingnumber.[4]

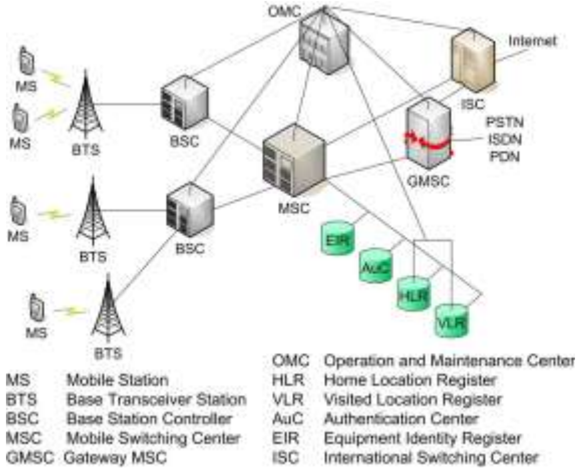
OMC
Internet
ISC
PSTN
ISDN
PDN
GMSC
MSC
BSC
BTS
MS
EIR
AuC
HLR
VLR
MS Mobile Station
BTS Base Transceiver Station
BSC Base Station Controller
MSC Mobile Switching Center
GMSC Gateway MSC
OMC Operation and Maintenance Center
HLR Home Location Register
VLR Visited Location Register
AuC Authentication Center
EIR Equipment Identity Register
ISC International Switching Center

Fig. 2 GSM Architecture

What's more, a carrier must accept any GSM-compatible phone so thatthe carriers don't have total control of the phone whichyou're using.[5]

GSM is popular among the operators and their customers:

- **Clear voice quality**, which makes GSM a possible alternative to wire-line telephony for businesses and consumers.
- **International roaming** with service available in more than 219 countries. As a result, users enjoy the suitability of being reachable along with their GSM devices and phone numbers when travelling abroad with the ability to access messages and other advanced services in their home markets.[2]
- **Spectral flexibility**, with the help of user device network infrastructure and available for numerous spectrum bands - Tri- and quad-band GSM phones are very much in common, decreasing the chances that a user will only travel to an area without at least single GSM network to which they can connect.
- **Tight security**, including inherent protection from hacking and eavesdropping. This helps GSM data andvoice an attractive substitute to analog Wi-Fiand cellular in the eyes of customers.
- **Data support**, including the daily use ofSMS and web browsing.
- **Subscriber Identity Module (SIM) cards**, which allow customers to buy a new or additional phone, or a GSM PC Card modem, and instantly transfer their settings, preferences and contacts to the other device.
- **Product selection**. The GSM family's market share also translates into large volumes of user devices and network infrastructure, which cut down costs. For operators, they can price their devices and services even more competitively.
- **Research and development** is immensely supported for the entire GSM family due to the scope and scale of over 6 billion customers worldwide.

III. GSM SPECIAL FEATURES

- High Spectrum efficiency
- High-quality speech
- Signal is less deteriorated inside the buildings
- Ability to use repeaters
- Talk time is higher due to the pulse nature of transmission

- Large capacity
- High voice quality
- Open interfaces epic
- High security
- Interconnection with Integrated Services Digital Network (ISDN) and PSTN.
- Roaming function
- Diversified services
- Inter-cell handover
- Automatic call-back, Call redirect
- Transparent G-3 fax mode

Fig. 3 Different kinds ofGSM Phones

IV. SERVICES PROVIDED BY GSM

- Telephony services,
- Data services, and
- Supplementary services.

Various types of subscribers' advanced services are Call bearing, Call waiting and Called Line Identification (CLIP), and Voice Mails, Call hold-indication of incoming calls during the conversation and the ability to switch without dropping the first one, prevention against the display of the calling or called (CLIR) number, short message service (SMS),multi-party calls up to five parties, GPRS internet on mobile, Data calls, multiple subscriber number.[3]

V. SECURITY MEASURES IN GSM

- PIN code (authentication of SIM isconsidereda local security measurein which a network is not involved)
- User authentication (performed by the network)
- Ciphering of information is sent over the air interface
- Usage of Temporary Mobile Subscriber Identity (instead of IMSI) over the air interface.[8]

VI. APPLICATIONS FOR GSM

Digital Communication such as Global Positioning System (GPS), Cell Phones (handsets), PCs,Laptops,etc.[11]

VII. GSM SECURITY MODEL

7.2.1 The Purpose of GSM Security

The use of radio communications for sending to the mobile subscribers makes GSM PublicLand Mobile Networks (PLMN) sensitive to misuse of their resources byunauthorized persons using altered the Mobile

Stations, who try to pretend authorisedsubscribers and the eavesdropping of the various types of information, which are regularly exchanged on the radio path.

The security features in GSM PLMN is executed to prevent:

- The access to the mobile services.
- Anyother necessary item from being discoveredon the radio pathto ensure theprivacy of the user-related information.

7.2. Security Features of GSM

Several security functions were built into GSM to safeguard subscriber’s privacy. These include:

- Subscriber identity protection
- Subscribers registered are authenticatedso that the operator knows who is using that system for the billing purpose
- Secure transfer of data via the use of encryption
- Mobile phones are impractical without a SIM
- Duplicate SIM are not allowed on the GSM network
- Securely storedkey(Ki).
- User Data and signalling protection so that user data sending over the radio path is protected.

7.2.1 Subscriber Identity Module (SIM)

A key feature of GSM is the Subscriber Identity Module (SIM) card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his/ her information after switching handsets.

7.2.2 Subscriber identity protection

The IMSI (International Mobile Subscriber Identity) is stored in the SIM card. This is to ensure subscriber identity confidentiality called Temporary Mobile Subscriber Identity (TMSI).The TMSI is sent to the MS after the authentication and encryption procedures have been taking place. The MS responds by confirming the reception area of TMSI. The TMSI is valid in the location area where it was issued. Outside the location area, the Location Area Identification (LAI) is mandatory in addition to the TMSI.

7.2.3 Smartcard

The smart card is like a micro-computerconsisting of a memory, a CPU and an operating system. By programming the Read Only Memory (ROM), it can accumulate the sensitive data with a very high security level, thus providing a good way to store the Ki , IMSI and other sensitive user data.

7.2.3 Authentication of the subscribers registered

International Mobile Subscriber identity (IMSI) authentication is the corroboration by the land basedpart of the system that the subscriber identity (IMSI or TMSI).The purpose ofthis security feature is to protect the network against any unauthorized use. It enables prevention of the GSM PLMN subscribers by denying the possibility for any intruder toimpersonate authorized users.to ensure correct billing.

7.2.3.1 The authentication procedure

- The MS send IMSI to the network
- Then the network received IMSI and established the Ki of that IMSI.
- The network generates a 128 bit (RAND) random number and sent it to the MS over the air interface.
- The MS calculates an SRES with the A3 algorithm using the given Challenge (RAND) and thekey Ki occupies in the SIM.[10]
- At the same time, the network calculates the SRES using the A3 algorithm
- Thensends the SRES to the network
- The network istested in the SRES for validation.

7.2.4 User Authentication

Over the radio interface, the authentication key (Ki) is never sent.

This procedure checks the validity of the subscriber’s SIM card and then decideswhether the MS is allowed on any particular network. The network validates thesubscriber via the use of a challenge-response method. Firstly, a 128 bit random number (RAND) is transmitted to the mobile station over the air interface.[7] The RAND is passed to the SIM card, where it is sent via the A3 algorithm in addition with the KI. The output is the signed response (SRES) is transmitted via the air interface from the MS back to the network. On the network, the Authentication Centre compares its value of SRES with the value of SRES it has received from the MS.If the two values of SRES match, then the authentication is successful and the subscriber readily joins the network.

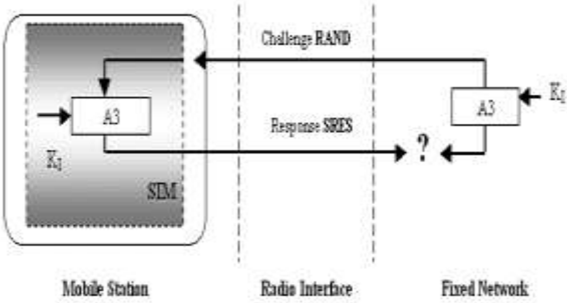

Fig. 4 User Authentication

VIII. ENCRYPTION AND DECRYPTION OF DATAIN GSM

During authentication, a new ciphering key (Kc) is generatedfor each call.

GSM makes use of a ciphering key to protect both user data and signalling on the vulnerable air interface. Once the user is validated, the RAND (delivered from the network) togetherwith the KI (from the SIM) is sent through the A8 algorithm, to produce a ciphering key (KC). The A8 algorithms aregenerally stored on the SIM card. The KC generated by the A8 algorithm is used with the A5 algorithm to encipher or decipher that data. The A5 algorithm is carried out in the hardware of the cell phone, to encrypt and decrypt data on the fly zone.

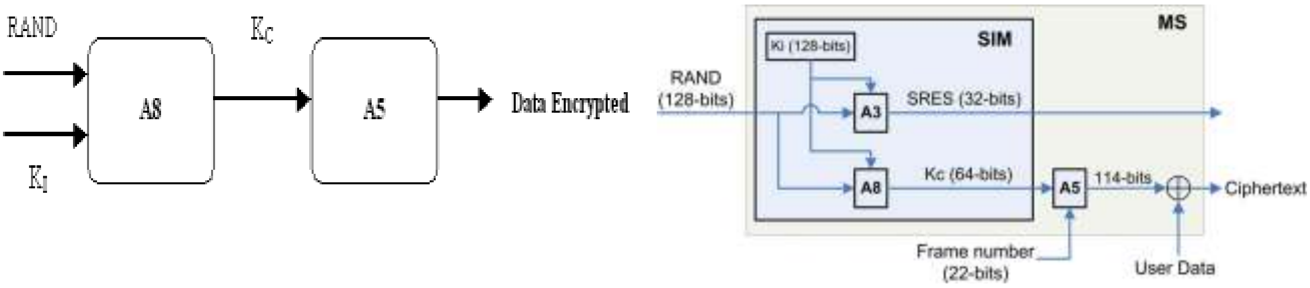

Fig.5 GSM Authentication, Session keygeneration, and Ciphering

IX. GSM CONFIDENTIALITY

The signalling information elements that are associated with the user, such as IMEI, IMSI and Calling subscriber directory number (originated calls) need to be protected after the connection establishment .The user information such as SMS, is sent in a connectionless packet mode over a signalling channel. It should be protected. User information on traffic channels over the radio interface should also be protected. For confidentiality purposes, a ciphering method, a key setting, the initialising of the enciphering and deciphering processes and synchronization are all required.[9]

The process can be briefly described as follows:

First, the network requests the MS to start its ciphering process and initialise its own deciphering process. The MS starts its ciphering and deciphering alternatively. From the MS , the first ciphered message reaches the network and is an exact ciphered message leads to the start of the ciphering process on the network side. The enciphering stream and deciphering stream at the both ends must be always synchronized.

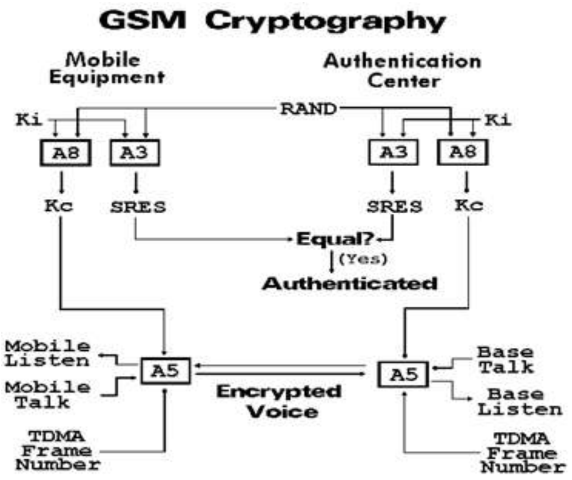

Fig. 6 GSM Cryptography

X. GSM ALGORITHMS

10.1 A3 (The MS Authentication Algorithm)

The A3 is the authentication algorithm in the GSM security model. Its purpose is to generate the SRES response required to the MSC's(Mobile Switching Centre) RAND which the MSC has received from the HLR. A3 is an operator-dependent and an operationaloption. It is a one-way function. That means it is easy to compute the output parameter SRES but very complex to retrieve the input parameters (RAND and KI) from the output parameter. Note that the key to GSM's security is keeping the KI unknown.

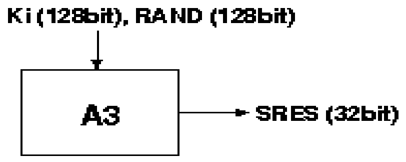

Fig.7 Signed response (SRES) calculation

Every GSM operator uses an algorithm called COMP128 for A3 as well as A8 algorithms. COMP128 is the reference algorithm of the tasks carried out by the GSM Consortium.

10.2 A8 (The Ciphering Key Generation Algorithm)

The A8 algorithm is the key generation algorithm in the GSM security model. The A8 algorithm generates the session key, Kc (64-bit), from the random challenge, RAND (128-bit), received from a secret key Ki and the MSC.

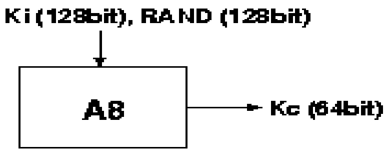

Fig.8 Session key (Kc) calculation

COMP128 is used for both the A3 and A8 algorithms in most of the GSM networks. The last 54 bits of the COMP128 output forms the session key, Kc, until the MS is authenticated once again.

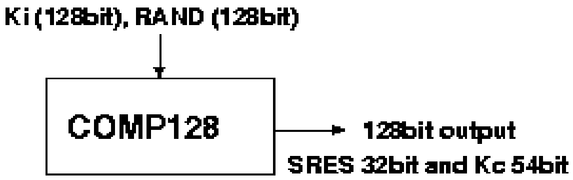

Fig. 9 COMP128 calculation

10.3 A5 (The Stream-Ciphering Algorithm)

The A5 algorithm is a stream cipher used to encrypt over-the-air transmissions. For every frame sent ,the stream cipher is initialized all over again. It begins with the session key, Kc, and the number of the frame being decrypted or encrypted. The same key Kc is used all along the call, but the 22-bit frame number changes, thus generating a unique keystream for each and every frame .

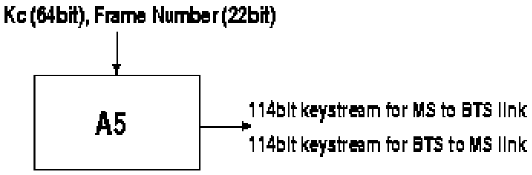
Kc (64bit), Frame Number (22bit)
A5
114bit keystream for MS to BTS link
114bit keystream for BTS to MS link

Fig. 10 Keystream generation

The most commonly used are A5/0, A5/1 and A5/2.

A5/1 is the strongest version used in Western Europe and America, the A5/2 in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption.

XI. PROBLEMS WITH GSM SECURITY

- Security by obscurity: means that all algorithms used are not accessible to the public
- Difficult to upgrade the existing cryptographic mechanisms [12]

- Lack of user visibility
- Only the mobile is authenticated and not the network[13]
- Base Station (BS) decides when to turn on encryption; mobiles have got no indicator
- Possible to set up a non-genuine BS that uses no encryption
- Integrity protection depends upon encryption, but some networks do not use encryption at all
- Early encryption algorithms build on COMP128 has now been broken. A5 cannot be enhanced without replacing the handset.
- No non-repudiation
- IMEI not authenticated: can be changed to prevent the tracking of stolen mobiles

XII. CONCLUSION

- The GSM is a first approach at a true personal and reasonably secure cellular telecommunications system.
- GSM provides a basic range of security enhanced features to ensure sufficient protection for both its operator and customer.
- The GSM architecture would still be susceptible to attacks, even if security algorithms were not broken, from inside which means the attack targeting the operator’s backbone network.

However, the security can be fixed up in some areas with simple measures focused on the protection of the air interface.

It is important to note that the whole security of GSM has always been kept in confidence. None of the ciphering algorithms and authentication procedures have ever been made public. All the information that is currently available comes from the reverse engineering process and leaks from the GSM developers.

The system is safe enough to protect relaxed subscribers from common attacks.

However, it has left a few backdoors for the organizations like government spy agencies to intercept the data transmitted between users they wish to inspect.

REFERENCES

[1] GSM Overview
http://www.tutorialspoint.com/gsm/gsm_overview.htm

[2]GSM Security Overview,Max Stepanov
ww.cs.huji.ac.il/~sans/students_lectures/GSM%20Security.ppt

[3] S.M. Siddique, and M. Amir, "GSM Security Issuesand Challenges," June 2006.

[4] Webmaster "GSM Technology" http://www.mobileworld.org/gsm_about.html

[5]Scourias, John "GSM - Global System For Mobile Communications" http://www.smarthomeforum.com/gsm.shtml

[6] GsmTechnology http://www.studymode.com/essays/Gsm-Technology-397218.html.

[7]PriyankaAgarwal, *Security of GSM System*, http://www.theukwebdesigncompany.com/articles/article.php?article=1191

[8] Security of Communication Protocols by MikkoSuominen 2003

[9]Michael Clayton,GSM Global System for MobileCommunications Security Domain-1991

[10] Solutions to the GSM Security Weaknesses Mohsen Toorani, Ali A. Beheshti

[11] GSM Tutorial http://ej.iop.org/links/rqPN3A4,P/Pj0p_COG2xG-BuLSav5vpA/joa4_4_003.pdf

[12] Security in GSM Yong LI , Yin CHEN, Tie-Jun MA.

[13] Network Security: GSM and 3G Security Tuomas Aura 2010.