ePathshala
पाठशाला

Information Technology

Mobile Computing

Module: GSM Security

Introduction

The wireless-radio medium is open to all .Being a wireless network, GSM is also sensitive to unauthorized use of resources. GSM offers precise security measures some of which maintains privacy and confidentiality of users' identity and data while others ensure that only registered users access the network. This module provides detail discussion of GSM's Security mechanisms and their implementation. The topics covered in this module are:

- Goals of Security features of GSM
- Introduction to principles of security namely access control, anonymity authentication and encryption
- Understanding of Security algorithms and mechanisms provided by GSM

Goals of Security features

The security features should be provided two sided i.e. from the Operator Side as well as User Side

Operator Side: From operator's point of view it should be ensured that operators

- Bill the right person
- There should be mechanisms to avoid fraud
- Services should be protected from

Subscriber side: The security measures need to be more promising and precise on subscribers side. They should aim at

- Maintaining privacy and anonymity of user which means that identification and location of the subscriber should be concealed
- Confidentiality of communication over air should be maintained by providing proper encryption methods
- There should be strong access control mechanisms for devices and SIM card
- Only authenticated users should be able to access the network

Rules of GSM Security

The Security features should adhere to the following rules:

1. Should not add much load to voice calls or data communication
2. Should not increase the error rate
3. Should not increase the complexity of system
4. Should not demand for more bandwidth
5. Should be useful and cost efficient

Principles of GSM Security

GSM provides security under followingmechanisms:

- **Access Control** to SIM card: This is done by use of Personal Identification Number (PIN) to get access to the SIM card
- **Anonymity:** Hiding the identity and location of user. This is done by using a TMSI number
- **Authentication** of subscriber so as to ensure only registered and authorized users have access to network
- **Encryption** of Data and signal to protect them against interception

Now we see how security measures described in above outlines are implemented by GSM network

Access control

SIM **Subscriber identity module** stores confidential information which can be personal as well as network specific. It stores the following information:

- **International Mobile Subscriber Identity (IMSI) number:**A globally unique identifier allocated to each GSM subscriber. It is permanently stored both in the HLR of the user and in the SIM of the user terminal. Any GSM subscriber can be uniquely identified by its IMSI number. This International Mobile Subscriber Identity (IMSI) number is composed of theMobile Country Code (MCC, three digits), the Mobile Network Code (MNC, two digits) and the Mobile Subscriber Identification Number (MSIN, ten digits).
- **Subscriber Authentication key (K_i):** 128 bit shared key used for authentication of the subscriber by the network
- **A3 and A8 Security algorithms:** Algorithms used for authentication and generation of cipher key.

Therefore it is necessary to protect the SIM card

Access Control Mechanisms

- **PIN (Personal Identification Number):** GSM provides provision of protection of SIM card by using a PIN. The user needs to know the PIN to unlock the SIM card. The SIM card automatically “Lock Out” after 3 unsuccessful attempts by feeding wrong PIN.
- **PUK (Personal Unlocking Key):** A PIN unblocking key should be entered which is provided by the user to unlock the SIM which is locked after giving the wrong PIN. If the PUK entered incorrectly a number of times, (normally 10) the access to inform is refused permanently and SIM becomes useless.

Anonymity providing Mechanism

To preventeavesdroping, the identity of the user should be hidden. The identity of user is hidden by use of TSMI (Temporary Mobile Subscriber Identity) in place of IMSI of the user .When a MS makes initial contact with the GSM network, an unencrypted subscriber identifier (IMSI) has to be transmitted.The IMSI is sent only once, then a temporary mobile subscriber identity (TMSI) is assigned (encrypted) and used in the entire range of the MSC.When the MS moves into the range of another MSC a new TMSI is assigned. The IMSI is not sent over the radio interface so as to prevent the user from being traced. A TMSI is used instead of IMSI. It is valid in the area of associated MSC i.e. will be valid only till the user is in the area of MSC for communication .Outside location area, it is used along with LAI (Location Area Identification). The TMSI identifies the user along with the location area. The TMSI is updated every time user moves to a new geographical area. It can contain 4 * 8 bits (4 octets). But all 32 bits as one cannot be allocated. TMSI is stored in SIM and all 1’s in SIM indicates no TMSI. The VLR must be capable of correlating an allocated TMSI with IMSI of MS to which it is allocated. At the time of paging, to localize the mobile phone the TMSI is broadcasted.

Authentication and Encryption

GSM ensures authentication of subscriber before it can use any services of the network. At the same time privacy of user data and signal should also be maintained by proper encryption mechanisms. Three security algorithms are documented in GSM specifications for this purpose. They are called A3, A5 and A8. A3 is authentication algorithm, A8 is ciphering key generating algorithm and A5 is a stream cipher for encryption of user data transmitted between mobile and base station. The GSM specifications for security were designed by GSM consortium in secrecy. The consortium used **“Security by obscurity”** which says algorithm would be difficult to crack if they are not publicly available. Therefore algorithms were made available only to hardware and software manufactures and GSM network operators.A3 and A8 are stored on SIM card and at AUC. A5 is stored on device. A3 and A8 are not that strong therefore the network providers can use their own algorithms or users can use their own algorithms but the encryption algorithmA5 is implemented on device and should be identical for all providers. A3 and A8 are symmetric algorithms using the same key embedded on SIM card.

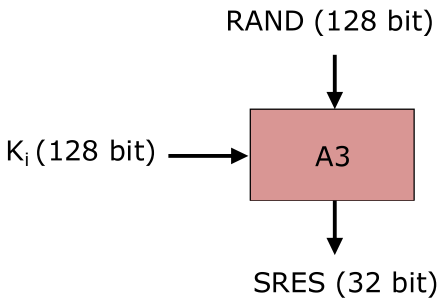


Figure 1: A3 algorithm

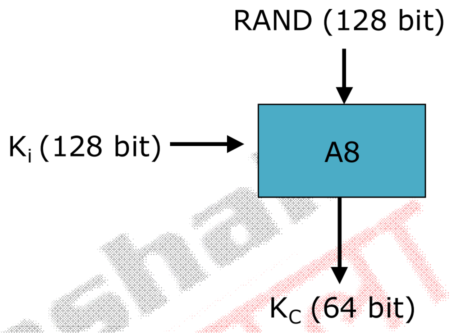


Figure 2: A8 algorithm

Both are one way functions which means output can be found if inputs are known but it is impossible to find inputs if output is known. A3 and A8 use **COMP128** which is a keyed hash function.Both are one way functions which means output can be found if inputs are known but it is impossible to find inputs if output is known. A3 and A8 use **COMP128** which is a keyed hash function.It takes 128 bit key and 128 bit RAND number as input and produces 128 bit output. The first 32 bits of 128 bit form SRES i.e. Signed response and next 54 bits forms the cipher key which is used for authentication and encryption.

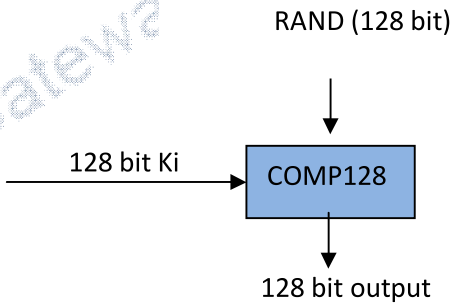


Figure 3: COMP 128 algorithm

Authentication mechanism

Authentication is performed using following entities and a technique called **“Challenge Response”**

- A3 Algorithm for Authentication
- 128 bit key $K_i$stored at SIM card and AUC
- RAND number auto generated by AUC known as Challenge

Following steps are followed for authentication

1. Mobile station sends IMSI to network
2. Network accepts IMSI and find corresponding **K_i** which is 128 bit secret key stored on the SIM card as well as available with the authentication center
3. The AUC generates 128 bit random number **RAND** and sends to the mobile station. This is called “challenge”
4. SIM card accepts this challenge and uses the random number and key K_i as input to A3 algorithm. SIM has a microcontrollerto execute the algorithm A3. It produces 32 bit output called signature response **SRES** using K_i and RAND as input
5. Network also calculates output using same inputs i.e. $K_{i,}$RAND and algorithm A3.
6. MS sends SRES to network
7. Network matches both SRES, if matched subscriber is authenticated.

The above mentioned steps are described in the activity diagram and block diagram shown in Fig. 4&5

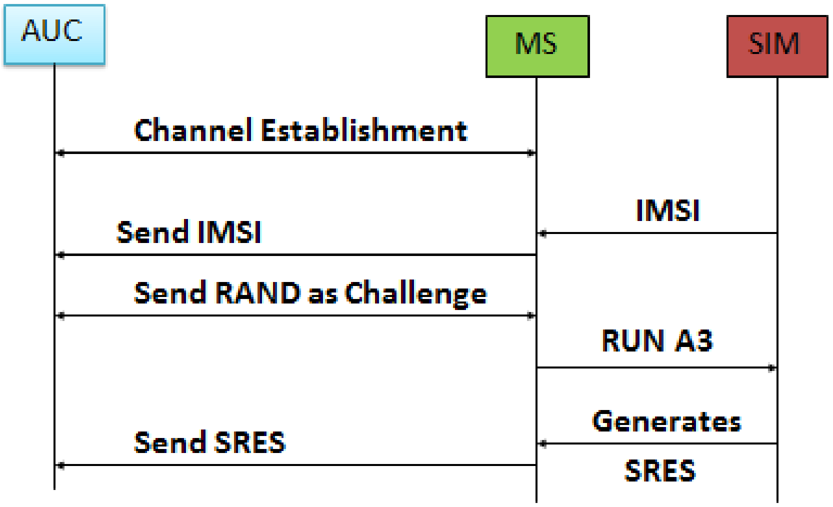


Figure 4: Authentication via Challenge Response

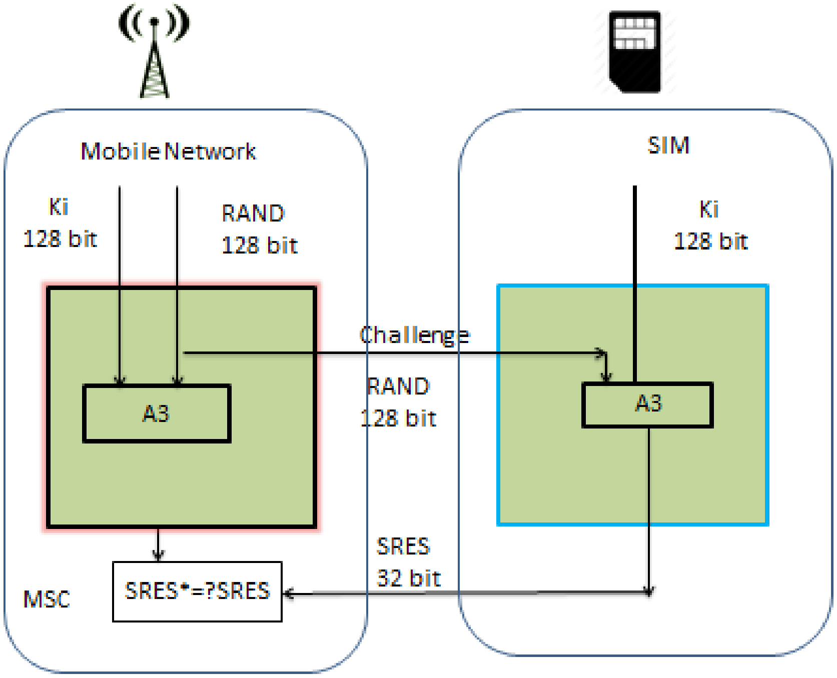


Figure 5: Authentication mechanism

Encryption

The data and signals are encrypted only between mobile station and base station.

Encrypted data

There is no end-to-end encryption

Therefore mechanisms for encryption need to be performed both at base station and mobile station. The algorithms A5 and A8 are used for encryption.Any encryption algorithm needs a cipher key. This cipher key is not statically available. It is dynamically generated using A8 algorithm. It takes 128 bit key Ki and 128 bit RAND to generate 54 bit cipher key. Then 10 zero bits are appended to the key to make it 64 bit. This is done to reduce the key space from 64 bits to 54 bits.

A5 algorithm

A5 is the encryption algorithm. It is a stream cipher. It works on bit-by-bit basis.A5 is stored on hardware as it has to encrypt and decrypt data during transmission and reception of information, which must be fast enough.A5 takes 64-bit cipher key and 22 bit function key as input and 114 bit plain text to generate 114-bit cipher text (Fig.7). The encryption decryption processes are performed both at Base station and Mobile station.

A5 is not implemented as block cipher

The reason being that bit error rate on the wireless links is high. If there is an error of single bit in the cipher text it affects an entire clear text frame. In contrast to it, by using a Stream cipher, a single bit error in the cipher text affects only one single clear text bit. Therefore stream cipher is used for encryption in GSM.There are many implementation of algorithm. Most common one being A5/0 A5/1 A5/2 A5/3 A5/1 is the strongest one. A5/0 is literally no encryption.

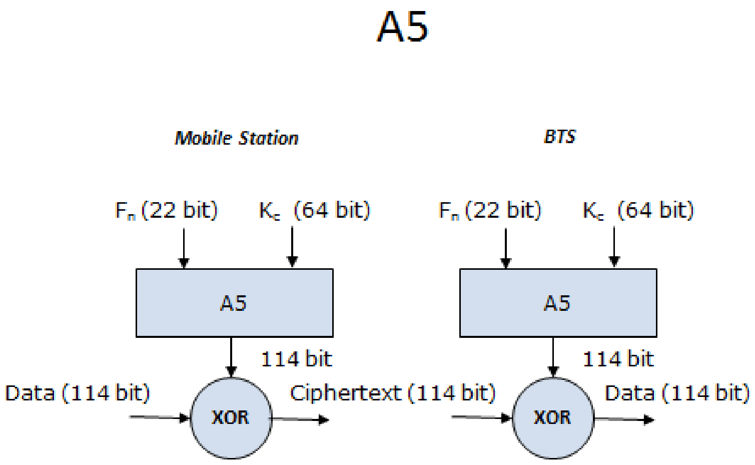
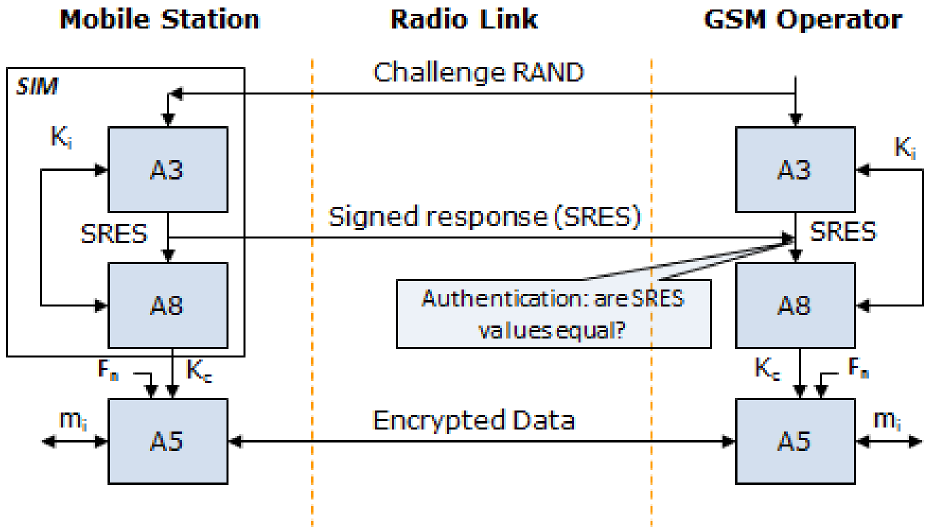


Figure 7: A5 algorithm

Steps followed during encryption

- Network initiates a ciphering mode request command
- Mobile station receives this command
- Network sends RAND number generated to generate the cipher key
- Mobile station uses RAND, K_i and RAND the network also generates K_c and distributes to BS

- As long as user is authenticated K_c remains same. If authentication is done again, another cipher key would be generated. During handovers if the mobile station has moved to a different base station but there is no need to authenticate it again, then the same key can be used by the new base station. The key would be forwarded to the new base station
- Once the cipher key is generated, it can be used to encrypt the data and signal using A5 algorithm.



GSM security issues

- Securityis not implemented in fixed part
- Encryptionis only between base station and mobile station Length of K_c (cipher key) is 64 bits which is not sufficient enough
- Authentication is from mobile station to network and vice versa is not possible
- No measures to maintain Integrityis provided
- Ciphering algorithms are not available for public

Summary

- GSM provides security to access control, user identification and data and signal via different techniques documented in GSM specifications
- The security principles follow security by obscurity
- Access control is provided by protecting the SIM via PIN and PUK
- To address anonymity of subscriber, a temporary identifier TMSI is used for IMSI
- Authentication and Encryption is performed using challenge response technique
- A3,A5 and A8 algorithms are used along with symmetric key K_c