2.31 SECURITY IN GSM

- In any of the digital cellular systems, security provision is relatively easy compared to analog systems. Methods like encryption, scrambling, FEC etc. can be employed to ensure security in the system.
- GSM offers several security services based on the information stored in AUC and SIM. The security services offered by GSM are :

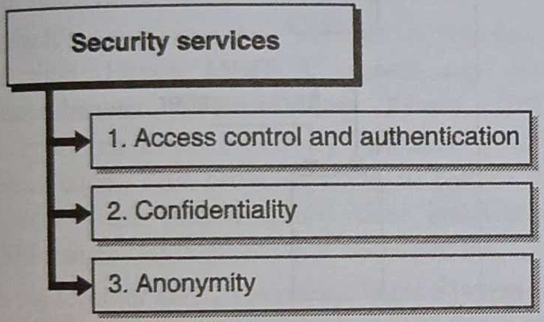

Fig. 2.31.1 : Security services

1. Access control and authentication

Access to the GSM network is allowed only through user authentication process. For this first user needs to have valid PIN to access the SIM and then using challenge response scheme authentication is done in mobile originated and mobile terminated calls.

2. Confidentiality

Once the authentication is done all the user data, voice etc. are encrypted to provide confidentiality. It exists only between MS and BTS.

3. Anonymity

- User's real identity is never transmitted on air. Every user is allocated with TMSI which is unique for each call. And VLR can change TMSI at any time.
- These three services are achieved by three algorithms in GSM network.
  1. A3 algorithm for authentication
  2. A5 algorithm for encryption
  3. A8 algorithm for generation of a cipher key

2.31.1 Authentication using A3 Algorithm

- Authentication is done with the help of SIM. SIM stores authentication key Ki and the user IMSI.
- Authentication is done by challenge response or request response method between MS and BTS.
- RAND random number is generated by AC (access control) which acts as a challenge and SIM responds to it by SRES (signed response).
- AUC generates RAND, SRES and cipher key Kc for each IMSI received and then forwards this to HLR. VLR may ask for these values from HLR.
- This RAND is sent to SIM by VLR for authentication purpose.
- On network side as well as on SIM side algorithm A3 is carried out on the RAND and Ki. Then MS sends SRES generated by SIM on air and VLR compares this received value with the one generated in the network.
- If both the values matches, subscriber is allowed to access the network otherwise he is denied the access. Refer Fig. 2.31.2.

- Using strong authentication to verify the identity of the users who access the network.
- Employing layers of security controls to limit the damage, should one layer of security be overcome
- Deploying many layers of security to make it much harder for an attacker to overcome the combined security mechanisms
  - o Initially changing SSID is beneficial.
  - o Next important measure is to limit the access to the wireless network to specific adapters.
  - o Some of the switches and WAPs can perform MAC filtering. MAC filtering uses the MAC address assigned to each network adapter to enable or block access to the network.
  - o For increasing the security of the network, WEP devices can be exchanged to WPA or WPA2.

Syllabus Topic : UMTS Security

5.2 UMTS SECURITY

- The security in UMTS is built on the security of GSM and GPRS. This means UMTS makes use of the security features used in GSM. This also maintains the compatibility with GSM.
- Since the compatibility in GSM is maintained, handoff and internetworking between GSM and UMTS is easy.
- The security features in UMTS correct the problems with GSM by addressing its real and perceived security weaknesses.
- UMTS uses public keys. In UMTS mutual authentication between the mobile and BS occurs; thus there is no fake BS attack. UMTS has increased key lengths and provides end-to-end security.
- Additional UMTS security features which are not present in GSM security mechanism are mentioned as below :
  1. Security against using false base stations with mutual authentication.
  2. Encryption extended from air interface only to include Node-B to RNC connection.
  3. Security data in the network will be protected in data storages and while transmitting ciphering keys and authentication data in the system.

Mechanism for upgrading security features

- The other security features of UMTS are listed below:
  1. Subscriber individual key K: It is user specific.
  2. Authentication center and USIM share User-specific secret key K, Message authentication functions f_1, f_2 and Key generating functions f_3, f_4, f_5.
- The authentication center has a random number generator. The authentication center has a scheme to generate fresh sequence numbers. USIM has a scheme to verify freshness of received sequence numbers.
- Authentication functions f_1, f_2 are MAC (XMAC) and RES (XRES).
- Key generating functions f_3, f_4, f_5 are as mentioned below:
  1. f_3: ciphering key CK (128 bit);
  2. f_4: integrity key IK (128 bit) and
  3. f_5: anonymity key AK (128 bit).
- Key management is independent of equipment. Subscribers can change handsets without compromising security. Assure user and network that CK / IK have not been used before.
- Integrity function f_9 and ciphering function f_8 are based on the Kasumi block cipher.

5.2.1 UMTS Specification has Five Security Feature Groups

- **Network access security:** The set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link.
- **Network domain security:** The set of security features that enable nodes in the provider domain to securely exchange signalling data and protect against attacks on the wireline network.
- **User domain security:** The set of security features that secure access to mobile stations.
- **Application domain security:** The set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security:** The set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Syllabus Topic : Bluetooth Security

5.3 BLUETOOTH SECURITY

- Refer Fig. 5.3.1. It shows Bluetooth security architecture.

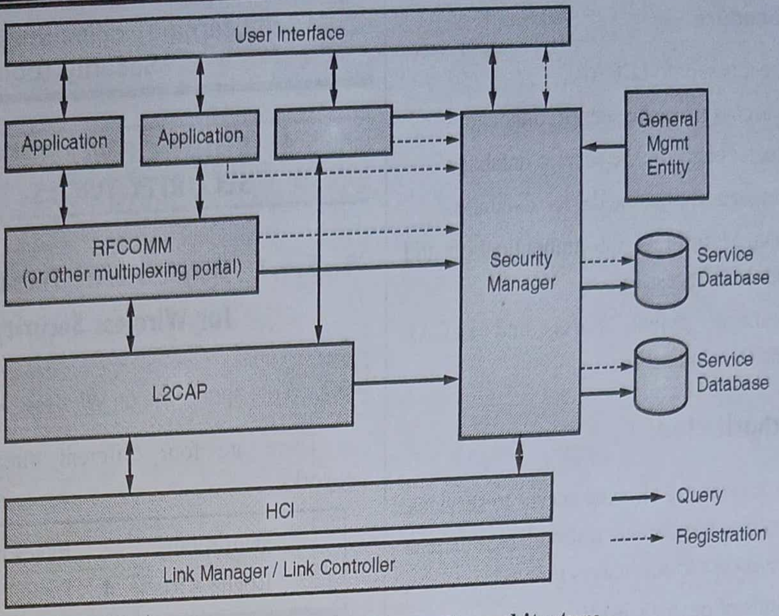

Fig. 5.3.1 : Bluetooth security architecture

- Authentication and encryption in Bluetooth are based on a secret link key that is shared by pair of devices. A pairing procedure is used when two devices communicate for the first time to generate this key.
- There are three security modes to a device

1. Non secure
2. Service level enforced security
3. Link level enforced security

1. **Non-secure :** A device will not initiate any security procedure.
2. **Service level enforced security :** A device does not initiate security procedures before channel establishment at the L2CAP level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel.
3. **Link level enforced security :** A device initiates security procedures before the link set-up at the LMP is completed.

5.3.1 Bluetooth Security Levels

There are two types of security levels

1. Authentication 2. Authorization.

5.3.1(A) Authentication

- It verifies the user present at the other end of the link. It is carried out with the help of the stored link key or by the pairing procedure.
- To meet different requirements on availability of services without user intervention, authentication is performed after determining what the security level of the requested service is.
- Thus, authentication cannot be performed when the ACL link is established. The authentication is performed when a connection request to a service is submitted.
- Authentication can be performed in both directions means the client authenticates server and vice versa.
- Refer Fig 5.3.2. It shows authentication procedure.

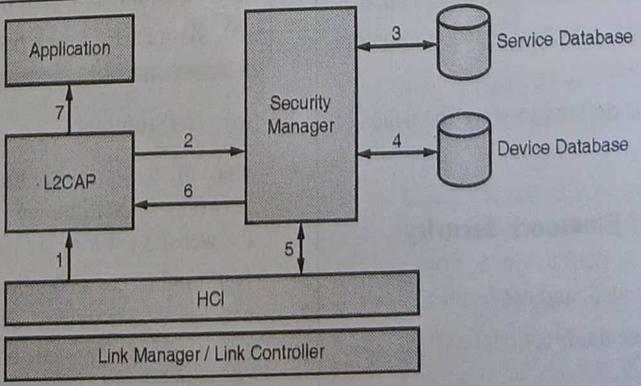

Fig. 5.3.2 : Authentication procedure

Authentication procedure

1. The connect request is sent to L2CAP.
2. L2CAP requests access from the security manager.
3. The security manager enquires the service database.
4. The security manager enquires the device database.
5. The security manager enforces the authentication and encryption procedure if necessary.
6. The security manager grants access, and L2CAP continues to set up the connection.

5.3.1(B) Authorization

- Only the trusted devices are allowed access to services. And untrusted devices need authorization based on user interaction before access to services is granted.
- There are two kinds of device trust levels:
  1. **Trusted device :** A device with a fixed relationship (paired) that has trusted and unrestricted access to all services.
  2. **Untrusted device :** This device has been previously authenticated, a link key is stored, but the device is not marked as trusted in the device database.
  3. **Unknown device :** It is also an untrusted device. No security information is available for this device.
- Independent set up of authorization, authentication, and encryption is done as per requirement by services.
- The access requirements define three security levels :
  1. **Services that require authorization and authentication :** Automatic access is only granted to trusted devices. Other devices need a manual authorization.
  2. **Services that require authentication only :** Authorization is not necessary.
  3. **Services open to all devices :** Authentication is not required, no access approval is required before service access is granted.
- A default security level is defined to serve the needs of legacy applications.

5.3.2 Limitations of Bluetooth Security

1. Only a device is authenticated, and not its user.
2. It is not possible to enforce unidirectional traffic.