Wireless Cellular Network Security: Part 2

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- B.L. Menezes, R. Kumar, “*Cryptography, Network Security, and Cyber Laws*”, Cengage Learning India Pvt. Ltd., 2018
- T.S. Rappaport, “*Wireless Communications: Principles and Practice*”, Prentice Hall of India, 2nd ed, 2002.

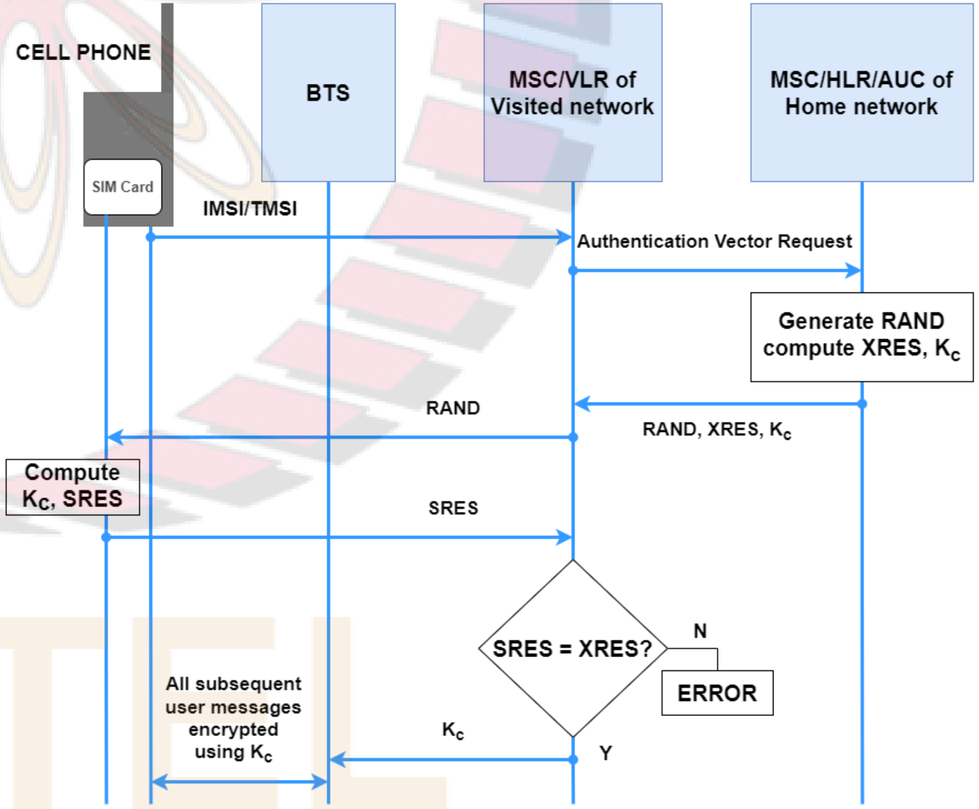
GSM (2G) Security

GSM (2G) Security

- Two principal tasks involved in providing security in GSM:
  a) Entity authentication and key agreement
  b) Message protection
- The integrity and encryption keys that are agreed upon as part of task (a) are then used to protect messages between the cellphone and the base station
- Next: we discuss each of the above tasks

Entity Authentication and Key Agreement

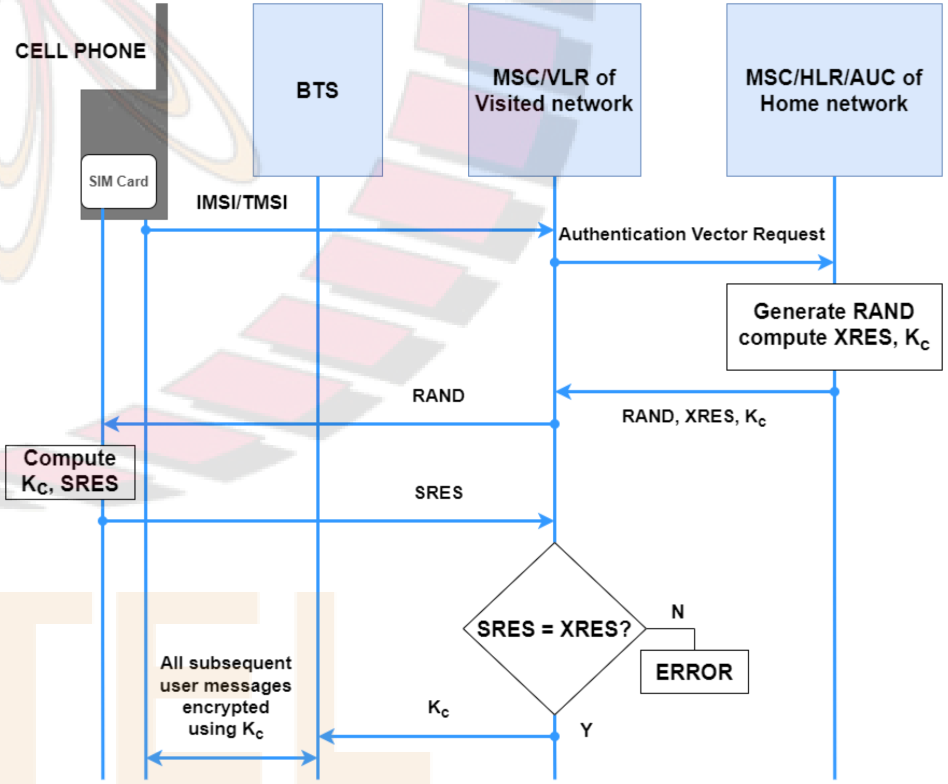
- GSM standard does not specify how often authentication takes place
- May occur once in several days or at the start of each call
  - ❑ However, latter option is very unlikely
- On the other hand, authentication is necessarily performed when a subscriber moves into a new network
- Main steps in authentication shown in fig.
- **Step 1: Authorization Request from Cellphone**
  - ❑ Cellphone sends to base station the encryption algorithms that it can support
  - ❑ Also sends its IMSI/ TMSI to MSC
  - ❑ If cellphone is away from its home network, IMSI will be received by the MSC of the visited network
  - ❑ Latter communicates the IMSI to the MSC/ HLR of the cellphone's home network with a request to provide a challenge to be sent to cellphone



Entity Authentication and Key Agreement (contd.)

- **Step 2: Creation and Transmission of Authentication Vectors**
- MSC for the home network receives the IMSI of the cellphone
- Used to index into the HLR from which it obtains key K_i
  - Recall: K_i is shared only between a SIM and the HLR of its home network
- The MSC/HLR generates a 128-bit random number, $RAND$, which functions as the challenge in the challenge-response authentication protocol
- It computes two quantities $XRES$ and K_c as follows:
  - $XRES = A3(RAND, K_i)$
  - $K_c = A8(RAND, K_i)$, where A3 and A8 are two keyed hash functions
- $XRES$ is the expected response in the challenge-response authentication protocol
- K_c is the encryption key
- The HLR creates five authentication triplets, each seeded by freshly chosen random numbers

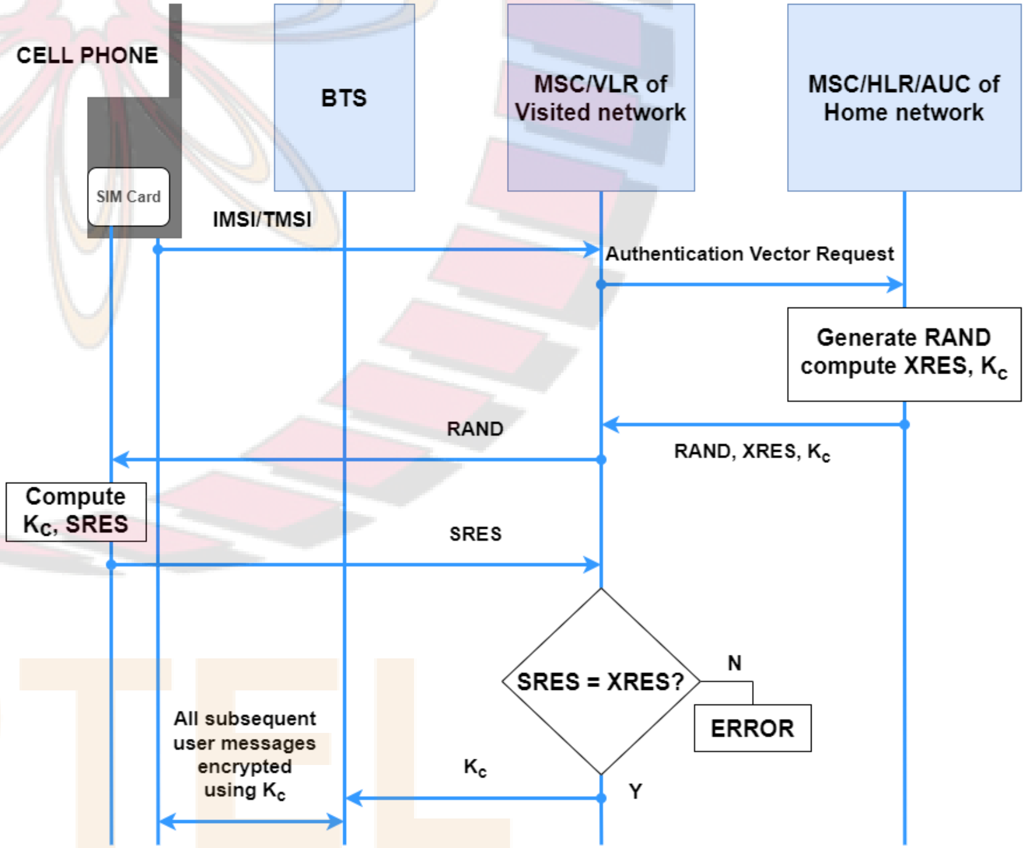
- Each triplet is:
  - $< RAND, XRES, K_c >$
- The triplets are sent to the MSC of the home network by the HLR
- If the cellphone is visiting a "foreign" network, the MSC forwards the triplets to the MSC of the visited network
- Five triplets are sent so that four subsequent authentications may be performed without the need to repeatedly involve the MSC/HLR of the home network
- MSC then sends the challenge $(RAND)$ from the first triplet to the base station who forwards it to the SIM on the cellphone



Entity Authentication and Key Agreement (contd.)

- **Step 3: Cellphone Response**
- Once the SIM has received $RAND$, it computes $SRES$ using $SRES = A3(RAND, K_i)$
  - ❑ $SRES$ stands for signed response
  - ❑ Can only be computed by an entity with the knowledge of K_i, the key shared between the SIM and the HLR
- Cellphone sends $SRES$ to the base station who forwards it to the MSC
- MSC checks whether $SRES$ equals $XRES$
- If they are equal, then MSC concludes that the SIM knows K_i and hence it is a genuine subscriber

- **Step 4: Computation/ Receipt of Encryption Key**
- SIM computes K_c using $K_c = A8(RAND, K_i)$
- On the network side, the MSC extracts K_c from its authentication triplet and communicates it to the base station
- Thereafter, all user messages between the cellphone and base station are encrypted using K_c



Encryption

- Encryption of messages between the cellphone and the base station performed by a stream cipher
- Keystream generator for this cipher denoted by $A5$
- Keystream is a function of the 64-bit encryption key, K_c, and a 22-bit frame number:
  - ❑ $KEYSTREAM = A5(K_c, FRAME\ NO.)$
- Frame no. is incremented for each frame transmitted
  - ❑ So keystream changes for each frame sent during a call
- Ciphertext is the bitwise XOR of the plaintext and the keystream
- Computations of the keystream and encryption do not require input from any of the static secrets stored on the SIM
- So these operations are performed by the cellphone, not the SIM
- On the other hand, computation of $XRES$ and K_c require K_i
- K_i is a sensitive secret that should not leave the SIM
- Hence, the functions $A3$ and $A8$ must be supported by the SIM, while $A5$ is typically not

Drawbacks of GSM Security

- The algorithms $A3$, $A5$, and $A8$ are based on $COMP - 128$, a keyed hash function
- This algorithm was designed by a small group of people in secret and remained so for a while
- Eventually leaked or was reverse engineered and major vulnerabilities were exposed
- **Note**: Had the above algorithms been placed in the public domain for general scrutiny, many of their shortcomings would have been revealed early on
- There have been several attacks on $A3$ and $A8$ that attempt to deduce the value of K_i
- E.g.:
  - ❑ with access to the SIM, one can obtain K_i using an attack that involves 8 adaptively chosen plaintexts
  - ❑ once K_i is known, the SIM can be cloned, thus defeating one of the security goals of GSM

Drawbacks of GSM Security (contd.)

- Several versions of $A5$ were used:
  - ❑ $A5/0$: version with no encryption at all
  - ❑ $A5/1$ and $A5/2$ were the most common
  - ❑ $A5/1$ was more secure than $A5/2$
  - ❑ $A5/3$ is not based on COMP-128 and is the strongest
- However, there have been several successful attacks on all versions of $A5$
- E.g.:
  - ❑ by eavesdropping on just the first two minutes of conversation, a ciphertext-only attack on $A5/2$ can reveal the encryption key in a few milliseconds on a modest desktop
  - ❑ $A5/1$ can also be compromised in just over a second using a similar attack
- **Note**: the encryption key, K_c, which is 64 bits wide, was truncated to 54 bits and padded with 10 zeros to further weaken it

Drawbacks of GSM Security (contd.)

- Another drawback: SIM authenticates itself to the network, but network does not authenticate itself to the SIM
- This could result in a false base station attack in which an attacker poses as a base station by sending more powerful beacon signals than the legitimate base station
- In a variation of the attack, the attacker spoofs a cipher mode command from the base station
  - instructs the cellphone to suppress encryption
- So the cellphone communicates its data in the clear, making it easy for attacker to eavesdrop on the communication
- Finally, messages are encrypted only between the cellphone and the base station, not beyond
- In many cases, the link between the base station and the BSC is a microwave link, wherein messages are transmitted in the clear
- Such links can be eavesdropped upon, thus defeating the purpose of GSM encryption