Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 08

Lecture - 44

Wireless Cellular Network Security : Part 2

Hello, in this lecture, we will continue our discussion of wireless cellular network security. In particular, we will discuss the security of GSM. So, there are two principal tasks involved in providing security in GSM. The first task is entity authentication and key agreement, in which the mobile device proves to the base station that it is indeed the correct mobile device, and the key that will be used for encryption and message integrity is agreed upon. So, this is done as part of the first task, which is entity authentication and key agreement.

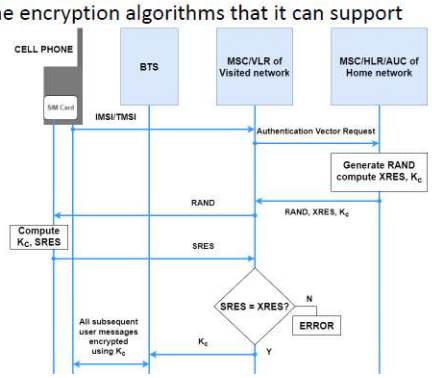
And the second task is message protection, that is, encryption of the messages that are sent. The integrity and encryption keys that are agreed upon as part of task one, that is, the authentication phase, are then used to protect messages between the cell phone and the base station. Now, we will discuss each of these tasks. First, we'll discuss authentication and key agreement. Later on, we'll discuss encryption and message integrity.

So, the GSM standard does not specify how often authentication takes place. So, this decision is implementation-dependent. Authentication may occur once in several days or at the start of each call. But the latter option is very unlikely. So, message authentication is done less frequently than at the start of each call.

On the other hand, authentication is necessarily performed when a subscriber moves into a new network. The main steps in authentication are shown in this figure. So, this is the cell phone which contains the SIM card. The SIM card is shown here, and this is the base transceiver station (BTS), and this is the MSC of the visited network and the corresponding VLR or visitor location register, and this is the MSC of the home network of this subscriber. So, to summarize this process, first the cell phone sends its identity and the list of security algorithms that it supports.

And this list is forwarded by the BTS to the MSC of the visited network. Then the MSC of the visited network requests the MSC of the home network for authentication vectors, which will be used to authenticate the mobile device. So, these authentication vectors are generated and sent to the MSC/VLR of the visited network. And then the MSC sends a challenge to the cell phone, that is this number, RAND. And then the cell phone computes the response to this challenge, which is SRES.

- 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



And then the MSC/VLR performs a check whether the response to the challenge is correct or not. If it is correct, then the authentication is successful. And then the key that is to be used for encryption that is computed by the cell phone at this stage, and it is shared by the MSC with the BTS, and then all subsequent user messages are encrypted using this encryption key, that is K_C. So, we'll now discuss this process in detail. So, in step 1, the cell phone requests for authorization with the network.

So, the cell phone sends to the base station the encryption algorithms that it can support. And it also sends its IMSI or TMSI to the MSC for identification of the cell phone. In particular, the identification of the SIM card. If the cell phone is away from its home network, then the IMSI will be received by the MSC of the visited network. So, that scenario is shown here, where the IMSI is received by the MSC of the visited network.

The MSC of the visited network then communicates the IMSI to the MSC/HLR of the cell phone's home network. So, that is shown here. And in the same communication, the MSC/VLR requests the MSC/HLR to provide a challenge to be sent to the cell phone. So, that is this message where the MSC/VLR of the visited network requests the MSC/HLR of the home network for a challenge that is to be sent to the cell phone. Then the next step is

creation and transmission of the authentication vectors, which includes the challenge that is to be sent to the mobile device.

The MSC for the home network receives the IMSI of the cell phone. So, once the MSC/HLR of the home network receives this message, it has obtained the IMSI of the cell phone. Then this IMSI is used to index into the HLR, from which the MSC/HLR obtains the key K_i. So, recall that this key K_i is present only in the SIM card and in the MSC/HLR. The MSC/HLR uses the IMSI as an index into the HLR and obtains the key K_i.

- 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

So, K_i is shared only between the SIM and the HLR of its home network. The MSC/HLR generates a 128-bit random number, RAND, which functions as a challenge in the challenge response authentication protocol. So, this is the challenge that is to be sent to the cell phone, which will pass it on to the SIM card. And knowledge of the secret K_i is required to respond correctly to this challenge RAND. The MSC/HLR then computes two quantities, XRES and K_C, as follows:

XRES = A3(RAND, K_i), and K_C = A8(RAND, K_i), where A3 and A8 are two keyed hash functions. So, they are some cryptographic hash functions. So, these functions A3 and A8 are used to compute XRES and K_C. XRES stands for expected response. So, XRES is the correct response to the challenge RAND.

- Each triplet is:
  - $< RAND, XRES, K_c >$
- The triplets are sent to the MSC of the home network by the HLR

So, to compute XRES from this equation, we can see that one needs to know the secret K_i to compute the expected response XRES. XRES is the expected response in the challenge response authentication protocol, as we just mentioned. K_C is the encryption key that will be used for encryption of the data messages that are exchanged after the authentication process is successful. The HLR creates five authentication triplets, each seeded by freshly chosen random numbers. So, each triplet is of this form: $\langle RAND, XRES, K_C \rangle$.

So, once an authentication vector is sent by the MSC/VLR of the visited network to the MSC/HLR of the home network, the home network generates five authentication triplets, each of this form: $\langle RAND, XRES, K_C \rangle$, and sends these five authentication vectors to the MSC/VLR of the visited network. So, why does it send five templates in one go? So, these templates are sent to the MSC of the home network by the HLR. And then the MSC of the home network forwards these to the MSC of the visited network. So, if the cell phone is visiting a foreign network, then the MSC forwards the triplets to the MSC of the visited network as in this scenario in this picture.

So, five triplets are sent so that four subsequent authentications can be performed without the need to repeatedly involve the MSC/HLR of the home network. So, once the MSC/HLR of the home network has sent five authentication vectors to the MSC/VLR of the visited network, then, in some duration subsequently, the MSC/VLR can authenticate the cell phone or the SIM card five times without having to repeatedly contact the MSC/HLR of the home network. So, this saves on the overheads that are involved in authentication. So, for this reason, five authentication triplets are sent in one go from the MSC/HLR of the home network to the MSC/VLR of the visitor network. The MSC then sends the challenge, that is RAND, from the first template to the base station, who forwards it to the SIM on the cell phone.

So, that is shown by this arrow. The challenge RAND is sent to the BTS, which forwards it to the cell phone. And then the cell phone passes it on to the SIM card, which is in the cell phone. Then the next step is cell phone response. So, once the SIM has received the challenge RAND, it computes the response to the challenge SRES using SRES = A3(RAND, K_i).

- **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

So, this is the same function A3, which the MSC/HLR used to compute XRES. So, for the authentication to be successful, SRES should equal XRES. SRES stands for signed response. And it can only be computed by an entity with knowledge of K_i, which is the key shared between the SIM and the HLR. So, K_i is known only to the SIM card and the MSC/HLR.

The MSC/HLR uses K_i to find out XRES, and the SIM card uses K_i to calculate SRES, and SRES should be equal to XRES for the authentication to be successful. The cell phone sends SRES to the base station, which forwards it to the MSC. So, that is shown here. The cell phone sends SRES to the MSC/VLR of the visited network. The MSC checks whether SRES = XRES.

So, that is shown by this decision box. So, this checks whether SRES = XRES. If they are not equal, then the authentication fails. So, that is shown here. So, that's an error, and the authentication is refused by the MSC of the visited network.

If SRES and XRES are equal, then the authentication is successful, and the MSC concludes that the SIM knows K_i and hence it is a genuine subscriber. So, in this case, the authentication is successful. The next step is the computation and receipt of the encryption key. So, the SIM computes K_C using the equation $K_C = A8(RAND, K_i)$. On the network side, recall that this K_C was part of the authentication triplets.

So, each triplet has a different K_C. This K_C was sent by the MSC/HLR of the home network to the MSC/VLR of the visitor network in this step. Now, the MSC extracts K_C from its authentication triplet and communicates it to the base station. So, that is shown over here by this arrow. K_C is communicated from the MSC of the visited network to the base transceiver station.

Subsequently, all user messages between the cell phone and the base station are encrypted using the key K_C. All subsequent user messages are encrypted using the secret key K_C, which is the encryption key. This concludes our discussion of the authentication and key agreement process. So, at this stage, the cell phone has authenticated itself successfully with the network, and subsequently it must exchange data messages with the network, and these must be encrypted. We now discuss the encryption process.

Encryption of messages between the cell phone and the base station are performed by a stream cipher. So, we discussed that WEP uses the stream cipher RC4. So, GSM also use the stream cipher for encryption of messages between the cell phone and the base station. The key stream generator for this cipher is denoted by A5. So, the key stream is a function of the 64-bit encryption key K_C and 22-bit frame number.

In particular, the KEYSTREAM = $A5(K_C$, frame number). So, the frame number is different for different frames. Hence the key stream is different for different frames. And

the key stream is XORed bitwise with the plaintext to get the ciphertext. The frame number is incremented for each frame that is transmitted.

- 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

So, it's a sequence number. So, the key stream changes for every frame that is sent during a call. The ciphertext is the bitwise XOR of the plaintext and the key stream. So, this is similar to the case for WEP, which we discussed earlier in Wi-Fi. So, there also the ciphertext was the bitwise XOR of the plaintext and the keystream.

The computations of the keystream and encryption do not require input from any of the static secrets stored on the SIM, such as K_i. Hence, these operations are performed by the cell phone, not the SIM. Thus, this keystream is computed by the cell phone. The cell phone has knowledge of the key K_C. But the cell phone does not know the secret K_i.

The secret K_i is only known to the SIM and the MSC/HLR. Computation of XRES and K_C requires the secret key K_i. Thus, K_i is a sensitive secret and should not leave the SIM. Therefore, K_i should be known only to the SIM and MSC/HLR. Hence, the functions A3 and A8 must be supported by the SIM, while A5 is typically not supported by the SIM.

A5 is supported by the cell phone. This concludes our discussion of GSM security, but it has some drawbacks which we will now discuss. The algorithms A3, A5, and A8 are based on COMP-128, which is a keyed hash function. This algorithm was designed by a small group of people in secret and remained secret for some time. But eventually the algorithm was leaked or it was reverse engineered, and major vulnerabilities were exposed.

- 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

So, here we remark that if the above algorithms had been placed in the public domain for general scrutiny, then many of their shortcomings would have been revealed early on. So, we discussed a security principle earlier that the algorithms used for encryption, message

integrity, and so on are generally public, but only the keys are secret. And that is so that security researchers can analyze the algorithms and find out if there are any flaws in them. But in the case of GSM, the algorithm that was used, that is, COMP-128, was a secret algorithm. But eventually, it was leaked, and at that point, major vulnerabilities were exposed.

So, this confirms our principle, which we studied earlier, that it's good to make the algorithms used for encryption and integrity protection, etc., public. So, only the keys should be secret. There have been several attacks on A3 and A8 that attempt to reduce the value of K_i. For example, with access to the SIM, one can obtain the secret K_i using an attack that involves eight adaptively chosen plaintexts. So, first, the plaintext is provided.

And then the ciphertext is examined, and then, depending on the ciphertext, another adaptively chosen plaintext is fed in, and the ciphertext is examined, and so on. So, using this procedure, one can obtain the secret key K_i using an attack that involves eight adaptively chosen plaintexts. Once K_i is cloned, the SIM can be cloned, and this defeats one of the security goals of GSM. So, this is one attack on GSM security which renders it insecure. And several versions of the function A5 were used.

So, A5/0 is the version with no encryption. Then A5/1 and A5/2 were the most common. A5/1 was more secure than A5/2. And A5/3 is not based on COMP-128, and it is the strongest among these. However, there have been several successful attacks on all versions of A5, including A5/0, A5/1, A5/2, and A5/3.

So, one example is as follows. 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 that the encryption key, or K_C, which is 64 bits wide, was truncated to 54 bits and padded with 10 zeros, and this further weakened it. That is, it made it easier to guess the encryption key K_C since there were only 54 non-trivial bits in the encryption key K_C.

So, to be secure, a longer key is required. For example, 128 bits or 256 bits. But the key actually used was only 54 non-trivial bits. Since out of the 64 bits, 10 were zeros. Another drawback of GSM security is that the SIM card authenticates itself to the network, but the network doesn't authenticate itself to the SIM.

So, authentication was one way, it was not mutual. So, 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. So, the attacker can pose as a base station and fraudulently connect with a mobile device and steal its information. In a variation of this attack, the attacker spoofs the cipher mode command from the base station. This instructs the cell phone to suppress encryption.

So, once the cell phone suppresses encryption, all the information is sent in plain text form, and it can be read by a user. So, these attacks are possible because authentication is one way. Only the SIM authenticates itself to the network, but the network does not authenticate itself to the SIM. So, in this attack, the cell phone communicates its data in the clear, making it easy for the attacker to eavesdrop on the communication. So, this is what happens if the attacker spoofs a cipher mode command from the base station, which instructs the cell phone to suppress encryption.

Another drawback of GSM security is that messages are encrypted only between the cell phone and the base station, not beyond. For example, the connection between the BTS and the BSC does not send encrypted messages. In many cases, the link between the base station and the BSC is a microwave link, that is a wireless link using the microwave spectrum. And on this link, messages are transmitted in the clear. So, even though the link between the mobile and the base station is encrypted, but the link between the base station and the MSC transfers unencrypted messages, and hence they can be easily intercepted by the intruder.

So, such links can be eavesdropped upon. This defeats the purpose of GSM encryption. So, in summary, we discussed GSM security in this lecture. So, it has two phases. One is entity authentication and key agreement.

And the other phase is encryption. So, we discussed these phases. But we discussed that GSM security has several drawbacks, which we covered in this lecture as well. And because of these drawbacks, GSM security was replaced with a stronger security scheme as part of 3G security. In the next lecture, we'll discuss 3G security.

In particular, the security of UMTS. Thank you.