Network Security

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

Week - 08

Lecture - 48

Wireless Cellular Network Security : Part 6

Hello, in this lecture, we will continue our discussion of the EPS security architecture. So, in particular, we will discuss the EPS authentication and key agreement process. We'll see that this has several similarities with the 3G authentication and key agreement process, but there are some differences, which we'll discuss. Before we discuss authentication and key agreement, let's discuss the process for user identification in EPS. EPS uses a similar mechanism to that used in GSM and UMTS.

In particular, EPS uses the IMSI number, which is the International Mobile Subscriber Identity. So, EPS uses the IMSI, which is a permanent subscriber identity. That is, it's an identity of the SIM card to uniquely identify a subscriber. The IMSI is crucial for EPS security because the permanent authentication key, that is, denoted by K, which is used in EPS authentication and key agreement, is identified by the IMSI. So, in our discussion of 2G and 3G, we had a key K_i, which was stored in the SIM card and in the HLR.

- K is stored in the Authentication Centre (AuC) and in the Universal Subscriber Identity Module (USIM), but nowhere else
- this is similar to the case in GSM and UMTS, where the permanent authentication key K_i was identified by IMSI

So, this was a permanent authentication key of the SIM card, and its copy was also stored in the HLR. Here, instead, we have the authentication key K, and that is identified by the IMSI. K is stored in the authentication center, which is attached to the HSS or Home Subscriber Server, which is an evolution of the HLR. So, it's very similar to that in 2G and 3G. There also, the HLR and AUC were connected, and the key K_i was stored in the HLR and AUC.

So, in the context of EPS, the secret key K is stored in the authentication center and in the Universal Subscriber Identity Module, or USIM, but nowhere else. USIM is the technical name for a SIM card in the EPS architecture. So, this is similar to the case in GSM and

UMTS, which we discussed earlier, where the permanent authentication key K_i was identified by IMSI. For user identity confidentiality, a temporary identity is associated with an IMSI in EPS. And that is known as GUTI, which stands for Globally Unique Temporary UE Identity.

So, it is similar to the TMSI, which was used in the case of GSM and UMTS and which we discussed earlier. So, in GSM and UMTS, TMSI was used instead of GUTI. GUTI in EPS performs a similar function, that is, it makes it difficult for an intruder to identify the subscriber and track the subscriber. Since a temporary identifier is used for the SIM card, instead of using the permanent identifier, the IMSI. So, EPS protects the confidentiality of the user identity similar to that in GSM and UMTS.

In particular, the network assigns the user a temporary identity or GUTI. This identity is sent in a message that is protected from eavesdropping. So, an intruder who is eavesdropping on the channel between the cell phone and the base station is not able to capture the value of GUTI since it is encrypted. GUTI provides an unambiguous identification of the UE that does not reveal the user's permanent identity, which is the IMSI. And GUTI can be used by the network and the UE during signaling between them and it can be translated by them to the IMSI.

Hence, these are interchangeable. From the IMSI, the GUTI can be inferred, and vice versa. From the GUTI, the IMSI can be inferred. So, the GUTI is used as a temporary identifier in place of the IMSI to prevent tracking of the subscriber. The MME sends the GUTI to the UE only after protection for the non-access stratum signaling has been enabled.

Recall that non-access stratum signaling is the signaling between the MME and the UE. So, only after this has been enabled, the MME sends the GUTI to the UE. This prevents an intruder from obtaining the value of the GUTI. Hence, the intruder is not able to track the UE. Thus, by using a temporary identifier, namely the GUTI, in place of the IMSI, one can prevent intruders from tracking the subscribers.

We have so far discussed subscriber confidentiality—that is, protecting the identity of the subscriber or SIM card. Now, we discuss another form of identification: the identification of the cell phone. The cell phone is also known as the terminal. So, we now discuss the mechanism for identification of the cell phone or the terminal. GSM, 3G, and EPS all use the same type of permanent terminal identity or phone identity, and that is the IMEI number.

It stands for International Mobile Equipment Identity. It's a unique identifier for every cell phone. GSM, 3G, and EPS all use this IMEI number to identify the cell phone. IMEI has several uses. The cellular network uses the IMEI number to identify the phone that is accessing the network.

The cellular network can identify the SIM card or the subscriber using the IMSI number. But for identifying the phone, the IMEI number is used. If a mobile phone is stolen, then the owner can have his/her network provider use the IMEI number to blocklist the phone. So, once the phone is blocklisted then someone who has stolen the phone is not able to use that phone since it will be blocked. Hence, the person who stole the phone will not be able to use that to communicate with the network.

Another application of the IMEI is that law enforcement and intelligence services can use an IMEI number as input for tracking phones. So, using the IMEI number that the phone sends to the network, these law enforcement and intelligence services can track phones and this tracking can be very accurate. These services can sometimes locate a phone with an accuracy of as high as a few meters. So, IMEI number can be used for tracking cell phones and this is especially useful where the cell phone has been stolen or the cell phone is being used by some person suspected of a crime and so on and so forth. So, IMEI number is useful for such tracking applications.

Now, recall that a mechanism for protecting the user identity confidentiality in EPS is the same as it was in GSM and UMTS. In EPS, the identifier GUTI is used in place of TMSI which was used in GSM and UMTS. In contrast, there is an improvement in EPS with respect to GSM and UMTS regarding the terminal identity confidentiality. We'll now discuss the process used for terminal identity confidentiality in EPS. In GSM and UMTS, it is possible that the network requests the terminal identity at any time, even before the signaling protection has been set up.

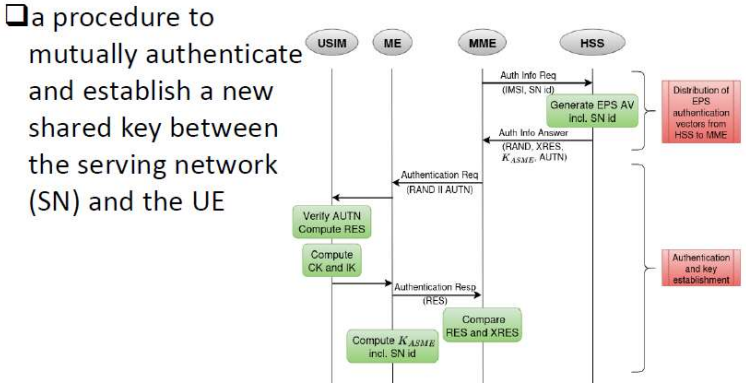
So, once the cell phone sends its terminal identity to the network, then if an intruder is eavesdropping on the channel, then the intruder will obtain the terminal identity and thus the intruder will be able to track the cell phone. So, without signaling protection already set up, when the network requests the terminal identity, the UE responds by sending the terminal identity in the clear. And the cell phone does not have a one-to-one mapping with the SIM card because we can remove a SIM card from a cell phone and place it in another cell phone. But typically most users tend to use the same terminal for an extended period of time. Hence, the terminal identity also gives strong hints regarding the user identity.

So, by tracking the terminal identity, an intruder can track the user identity. This was a limitation of terminal identity protection in GSM and UMPS. It was possible for an intruder to track the terminal identity and from there, the intruder could get hints about the user identity. But in contrast, this is no longer possible in EPS. In EPS, the UE does not send the IMEI to the network upon a network request before the NAS security has been activated.

Once the NAS security has been activated, only after that does the UE send the IMEI to the network. Since it is encrypted, the IMEI cannot be found by an intruder who is sniffing the channel between the UE and the network. So, this concludes our discussion on terminal identity confidentiality. So, we have discussed how the identity of the subscriber is protected and how the identity of the terminal is protected. Next, we will discuss the authentication and key agreement process in EPS.

The EPS authentication and key agreement procedure consists of the steps shown in this figure. This is the SIM card, and this is the mobile equipment or the cell phone. This is the MME, the Mobility Management Entity, which is a control plane element, and this is the Home Subscriber Server or HSS. So, the process is quite similar to that in UMTS or 3G. First, the cell phone requests for authentication, and then the MME of the serving network that sends a request to the home subscriber server for getting authentication information.

Then, the HSS generates an authentication vector and sends it to the MME. So, this authentication vector is shown over here. Then, the MME sends an authentication request to the cell phone. That authentication request is shown here. This authentication request includes an AUTN, which is similar to that in UMTS, and this is used to authenticate the network to the cell phone.



At this point, the SIM card verifies the value of AUTN and thereby checks whether the network is legitimate or not. And it also computes the response to the challenge in the authentication request. The challenge is this number RAND and SIM card computes the responds to this challenge. The SIM card also computes the ciphering key and the integrity key which will be used for protection of the messages that are exchanged subsequently by the cell phone with the network. So, these ciphering key and integrity key are then sent to the mobile equipment or the cell phone.

And from this, the cell phone computes K_{ASME}, which is the root key used for generating the keys that will be used for encryption and message integrity. And the K_{ASME} also has been conveyed to the MME in this step from the HSS. So, at this point, ME and the MME both have the K_{ASME}. They have agreed upon the K_{ASME}. Now, the mobile equipment sends an authentication response to the MME and the MME compares the response with the expected response or XRES.

If it is correct, then the USIM has successfully authenticated itself to the network. So, this is the process for authentication and key agreement. Now, let's discuss it in detail. So, the authentication and key agreement procedure consists of a procedure to generate EPS authentication vectors in the home subscriber server upon request from the MME. So, this shows the generation of the authentication vectors in the home subscriber server and the HSS distributes these authentication vectors to the MME and the MME can then use the authentication vectors for authenticating itself to the SIM card as well as for authenticating the SIM card.

So, the EPS authentication and key agreement procedure also includes a procedure to mutually authenticate and establish a new shared key between the serving network and the UE. So, the serving network is represented by the Mobility Management Entity (MME), which is shown here. This MME and the UE can mutually authenticate themselves. And the procedure for this mutual authentication is provided by the EPS authentication and key agreement procedure. The goals achieved by the EPS authentication and key agreement process are similar to those for UMTS AKA, which we discussed earlier.

But there is an enhancement: the EPS authentication and key agreement process provides implicit serving network authentication, which UMTS authentication and key agreement does not provide. So, that is provided as follows. So, we can see here that this is the MME of the serving network. When it contacts the HSS for getting authentication vectors, it sends its serving network id to the HSS. So, that is shown over here.

The serving network id is included in the authentication request sent from the MME to the HSS. Now, the HSS has a secure connection with the MME, and it verifies whether this SN id is the same as the actual SN id of the MME which has connected with it. And only after this verification—if the verification is successful—will it generate the authentication vector. This authentication vector is a function of the serving network id. So, implicit serving network authentication is achieved as follows.

SN id is one of the inputs used in the computation of the K_{ASME}. So, this K_{ASME}, which is a part of the authentication vector that is sent from the HSS to the MME; this K_{ASME} is computed using a process in which SN id is one of the inputs. The home network HSS, that is, home subscriber server, verifies the identity of a serving network requesting the authentication vectors. So, when the MME connects to the HSS for getting authentication vectors, the HSS verifies the identity of the MME. And the home network or HSS ensures that the SN id used as input for computation of the key K_{ASME} in the authentication vectors matches the verified identity of the serving network to which the authentication vectors are sent.

So, we have seen that SN id is used as one of the inputs for the computation of the K_{ASME} that is sent in this step. The HSS verifies that the SN id that is used to generate this K_{ASME} matches the SN id of the MME which is connecting to the HSS. So, MME connects to the HSS and requests for authentication vectors. So, the SN id of this MME is the same as the SN id that is used to generate this key, K_{ASME}. Hence, serving network cannot obtain authentication vectors with keys corresponding to the id of another serving network.

In this way, serving network authentication is achieved. Consider an MME which tries to connect to an HSS pretending to be some other MME. So, in that case, the HSS will verify the serving network identity because it has a secure connection with the MME. So, there is a secure connection between the MME and the HSS. The HSS is able to find out the true identity of the MME and it can see that it is not the same as the SN id that is sent from the MME.

So, it knows that this is not the correct MME. So, it will reject that authentication request. Hence, a serving network cannot obtain authentication vectors with keys corresponding to the id of another serving network. In this way, serving network authentication is achieved. The MME invokes the procedure by requesting EPS authentication vectors from the HSS, so that is shown by this step.

This is a request for authentication vectors from the MME to the HSS. So, this authentication information request includes the IMSI of the subscriber to be authenticated and the SN id of the requesting MME. So, that is shown here. The IMSI of the subscriber as well as the SN id of the MME are included in the authentication information request. The SN id is required for the computation of the K_{ASME} in the HSS.

As we have already discussed, the SN id is one of the inputs used in the computation of K_{ASME} in the HSS. Upon receipt of the authentication information request from the MME, the HSS may have pre-computed authentication vectors available and will retrieve them from the HSS database. So, in this case, these are pre-computed authentication vectors for this particular MME requesting authentication vectors. The HSS already happens to have pre-computed authentication vectors available. That is, usually because the same MME had in the recent past connected with the HSS and requested for authentication vectors.

At that time, the HSS computed some authentication vectors and kept them ready for future use. So, in that case, the HSS may just respond with that authentication vector. The other case is when the HSS does not have pre-computed authentication vectors. In that case, the HSS computes the authentication vectors on demand. The HSS sends an authentication information answer back to the MME.

So, this is the authentication information answer. This authentication information answer, it contains an ordered array of n EPS authentication vectors. That is, (1, …, n). But typically n is 1. So, only one authentication vector is sent from the HSS to the MME. So, this is in contrast to UMTS in which five authentication vectors were typically sent.

- contains an ordered array of *n* EPS AVs $(1, \ldots, n)$
- if $n > 1$, the EPS AVs are ordered based on sequence number

So, if n>1 then the EPS authentication vectors are ordered based on the sequence number. But in the case of LTE, the recommended value is n=1. So, the LTE standard recommends n=1, so typically only one authentication vector is sent at a time. Recall that in GSM and UMTS authentication and key agreement, five authentication vectors are sent at a time. And the reason was that MSC/VLR does not have to repeatedly contact the HLR for getting authentication vectors in the case of GSM and UMTS.

For this reason, during an authentication and key agreement process, five authentication vectors were sent so that the MSC/VLR could authenticate the SIM card five times without having to repeatedly connect with the HLR. So, in contrast, the LTE standard recommends n=1, so only one authentication vector is sent from the HSS to the MME. So, what is the reason for this? So, the reason is that the need for frequently contacting the HSS for fresh authentication vectors has been reduced in EPS through the availability of the local master key K_{ASME}. This K_{ASME} is sent from the HSS to the MME as part of the authentication vector.

So that is shown here. The K_{ASME} is included in the authentication vector and it acts as a local master key with this MME. So, from this local master key, other keys are derived which are used for confidentiality and message integrity. So, this K_{ASME} itself is not used for confidentiality and message integrity, but instead keys that are derived from the K_{ASME}, they are used for confidentiality and message integrity. So, K_{ASME} is not used for encryption or message integrity.

Hence, it is not exposed like the ciphering key (CK) or the integrity key (IK), which is used in UMTS. So, recall that in UMTS, the authentication vector contains the ciphering key and integrity key which are used for ciphering and integrity protection of the data messages that are exchanged between the cell phone and the network. Hence, an intruder can collect a large amount of information that is encrypted using the CK and for which message integrity is provided using the IK. So, these keys CK and IK are exposed to the intruder. Hence, they have to be changed frequently.

So, for this reason, five authentication vectors are sent from the HLR to the MSC/VLR in the case of UMTS and GSM. K_{ASME}, as we have seen, is not used for encryption or message integrity. Hence, it does not need to be renewed very often. So, the same K_{ASME} can be used for a long time. The K_{ASME} is not changed frequently, but instead, the keys that are derived from the K_{ASME} are changed from time to time.

Based on the local master key, that is, the K_{ASME}, and keys derived from it, an MME can offer secure services even when links to the HSS are unavailable. So, because of some network connectivity problems, the MME may not be able to connect with the HSS. Even then, it can use its K_{ASME}, which it has obtained during a previous authentication. It can use this K_{ASME} to securely connect with the cell phone. Pre-computed authentication vectors are no longer usable when the user moves to a different serving network, owing to the

binding of the local master key K_{ASME} to the serving network ID. So, we have seen that this SN id, that is, used to generate the K_{ASME} that is specific to this MME.

So, this SN id is the id of this MME. So, if the mobile moves from the range of one MME to the range of another MME, then it has to repeat the authentication process. That is, the authentication process will run all over again, and another authentication request with the SN id of the new MME will be sent to the HSS, and a fresh K_{ASME} will be sent from the HSS to the new MME. Hence, pre-computed authentication vectors are no longer usable when the user moves to a different serving network. This is because of the binding of the local master key K_{ASME} to the SN id.

Each EPS authentication vector is used for one run of the AKA procedure between the MME and the USIM. So, one run of the AKA procedure between the MME and the USIM, it involves the authentication of the network to the cell phone and the authentication of the cell phone to the network. So, this AUTN authenticates the network to the cell phone and the response sent by the cell phone authenticates the cell phone to the network, in particular, the SIM card to the network. Now, we discuss how authentication vectors are generated. So, recall that a UMTS authentication vector consists of the following five quantities.

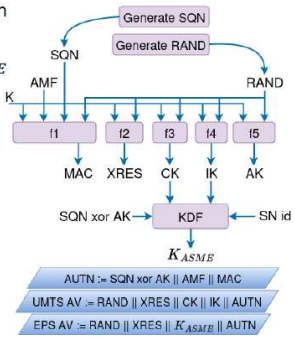
One is a random 128-bit string, RAND, then another is an expected response, XRES, then a ciphering key, an integrity key, and an authentication token, AUTN. In contrast, the EPS authentication vector consists of the following quantities. As before, RAND and XRES have the same meaning as before. AUTN also has the same meaning as before. But now instead of the ciphering key and the integrity key, we have a local master key, K_{ASME}, in the EPS authentication vector.

So, the difference is that ciphering key and integrity key are replaced with the K_{ASME} in the EPS authentication vector. This figure shows the generation of a UMTS authentication vector by the authentication center and the generation of an EPS authentication vector from this UMTS authentication vector by the home subscriber server. This part- this generation of the UMTS authentication vector, which is shown by these five quantities here, this happens in the authentication center, which is connected to the home subscriber server. These five quantities constitute the UMTS authentication vector. These five quantities are generated in the authentication center.

So, the authentication center generates UMTS authentication vectors for EPS authentication and key agreement in exactly the same format as for UMTS AKA. So, this is the UMTS authentication vector that is generated in the authentication center. The HSS

part outside the authentication center, it derives the K_{ASME} from the ciphering key and integrity key. That generation is shown here. The ciphering key and integrity key are input to the key derivation function which generates the K_{ASME}.

- Recall: a UMTS AV consists of:
  - a random 128-bit string (RAND), an expected response (XRES), a CK, an IK, and an authentication token (AUTN)
- In contrast, EPS AV consists of:
  - RAND, XRES, a local master key K_{ASME} and an AUTN
- Fig. shows generation of a UMTS AV by AuC, and generation of an EPS AV from this UMTS AV by HSS
- The AuC generates UMTS AVs for EPS AKA in exactly the same format as for UMTS AKA
- The HSS part outside the AuC derives K_{ASME} from CK and IK; in particular:
  - When the HSS receives the UMTS AV from the AuC, the HSS applies the KDF to CK, IK, SN id and, for technical cryptographic reasons, (SQN xor AK)
  - The result of the application of KDF is the key K_{ASME}
  - CK and IK can then be deleted in the HSS; they must never leave HSS



In particular, when the HSS receives the UMTS authentication vector from the authentication center, so that vector is shown here, the HSS applies the key derivation function to the ciphering key, integrity key, SN id, which is shown as one of the inputs over here, and for technical cryptographic reasons, sequence number XOR with anonymity key. So, this SQN is XORed with the anonymity key, and it is another input to the key derivation function. So, the reason that this SQN⊕AK is one of the inputs to the key derivation function is a technical cryptographic reason, which we won't discuss. But the result of the application of this KDF is the key K_{ASME}. That is shown over here.

Now, AUTN = $SQN \oplus AK \parallel AMF$, which has the same meaning as in UMTS, and concatenated with the message authentication code. The UMTS authentication vector consists of RAND, XRES, CK, IK, and AUTN and EPS authentication vector consists of RAND, XRES, K_{ASME}, and AUTN. In the case of UMTS, from these five, the authentication vector is generated and it is this, whereas in the case of EPS, the ciphering key and integrity key, along with the $SQN \oplus AK$ and SN id, these are used to generate the K_{ASME}. And the EPS authentication vector consists of these values, RAND, XRES, K_{ASME}, and AUTN. So, this shows the difference between UMTS authentication vectors and EPS authentication vectors.

So, after the K_{ASME} is generated, the ciphering key and integrity key can be deleted in the HSS. They must never leave the HSS. So, these ciphering key and integrity key are

discarded and instead the K_{ASME} is used to derive fresh keys for integrity protection and encryption. So, we now discuss mutual authentication and establishment of the shared key between the serving network and the UE. So, that process is shown here and we have discussed this earlier.

The purpose of this procedure is mutual authentication of the user and the MME, in particular, mutual authentication of the SIM card and the MME, and another function of this procedure is establishment of a new local master key K_{ASME} between the MME and the UE. So, this K_{ASME} is generated as part of the authentication vector generation in the HSS and is sent to the MME. And the mobile equipment computes the K_{ASME} in this step. And this K_{ASME} is the same as this K_{ASME}. The K_{ASME} is subsequently used for deriving keys for the protection of user plane data, RRC signaling, and NAS signaling.

So, user plane data is the data plane information and RRC signaling is exchanged between the user equipment and the eNodeB and NAS signaling is exchanged between the mobile and the MME. So, K_{ASME} is used for deriving keys for the protection of user plane data, RRC signaling and NAS signaling and this protection includes encryption and message integrity. The procedures used in EPS for handling of authentication requests and verification in the USIM and authentication responses are the same as in UMTS. So, in particular, this AUTN is used by the SIM card to verify whether the MME is genuine or not. And this response computed by the USIM that is used by the MME to verify whether the SIM card is genuine or not.

So, that is verified by the MME in this step, where it compares the response with the expected response. So, a difference between the authentication process in EPS and that in UMTS is as follows. When the mobile equipment receives ciphering key and integrity key from the USIM, so that is shown as in this step, in this step the mobile equipment receives the ciphering key and the integrity key from the USIM. Then, the mobile equipment computes K_{ASME} using the same key derivation function and the same input parameters as the home subscriber server. So, the mobile equipment computes K_{ASME} using the same key derivation function and the same input parameters, which we discussed earlier, as the HSS had used.

So, after this, the ciphering key and integrity key can be deleted in the mobile equipment. Subsequently, at the end of this process, the mobile equipment and the MME have the K_{ASME} in common. They can then use it for deriving further keys, which will be used for encryption and message integrity of the messages exchanged between the mobile

equipment and the network. So, in summary, we first discussed the processes of subscriber identification and terminal identification in the case of EPS. Then, we discussed authentication and key agreement in EPS.

It is similar to the authentication and key agreement in UMTS, but the main difference is that a master key, K_{ASME}, is derived in the case of EPS. This is used for deriving further keys, which are used for encryption and message integrity of the messages that the UE exchanges with the network. So, we will continue our discussion of EPS security in the next lecture. Thank you.