Network Security

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

Week - 08

Lecture - 47

Wireless Cellular Network Security : Part 5

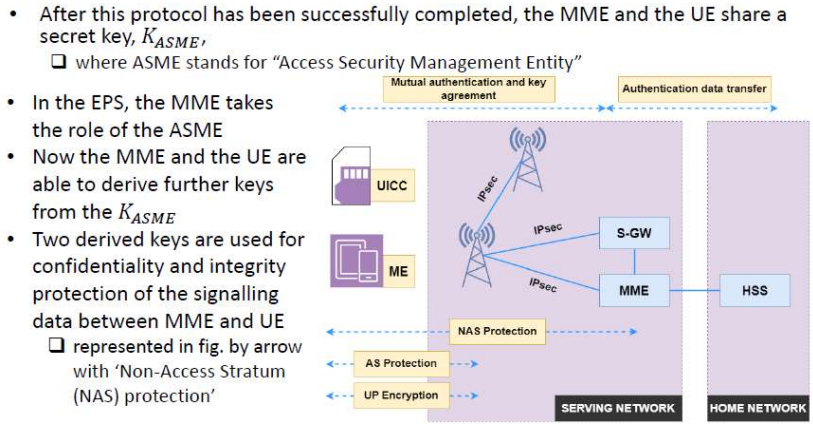
Hello, recall that in the previous lecture, we discussed the architecture of LTE networks, that is, 4G cellular networks. In this lecture and the next few lectures, we will discuss the security of LTE networks. We discussed the EPS security architecture. Recall that EPS is the technical name for LTE advanced networks. EPS stands for Evolved Packet System.

We have discussed in detail earlier the security of 2G and 3G networks. EPS brings two new major ingredients, which are not there in 2G and 3G networks. One is the radio network part of the system that is known as E-UTRAN which stands for Evolved Universal Terrestrial Radio Access Network. This has a new radio interface, and the other part is the core network. It is a completely packet-switched core network.

It is an Internet Protocol (IP)-based core network known as Evolved Packet Core (EPC). So, the core network of LTE is known as EPC, and the radio access network is known as E-UTRAN. Thus, GSM and 3G security mechanisms provide a good basis for the EPS security architecture. We will see that there are many similarities between the security mechanisms in EPS and those in GSM and 3G, which we discussed earlier. But due to the significant difference in the architecture of EPS relative to GSM and 3G systems, each GSM or 3G mechanism, if reused to be applicable in the EPS context, needs to be adapted from the original context and embedded to the EPS architecture.

So, we'll see such differences when we discuss EPS security in detail. EPS must also be able to interwork with legacy systems; that is, if any 3G or 2G systems are connected to the 4G network. So, these adaptations have to be done in a backward-compatible manner. In addition to adaptations from security functionalities already existing in legacy systems, many new extensions and enhancements have been introduced in the EPS security architecture. So, for example, there's an extensive key hierarchy used in EPS.

We'll discuss the key hierarchy of EPS later on. We now start our discussion of the EPS security architecture. This architecture is shown in this figure. This is the SIM card, and this is the cell phone. The SIM card is in the cell phone.



These are the base stations, known as eNodeBs in EPS terminology. These are elements of the core network, namely the Mobility Management Entity and Serving Gateway. And this is the Home Subscriber Server (HSS). So, notice that this HSS is an evolution of the HLR, or Home Location Register, in the case of 2G and 3G networks. So, after the User Equipment (UE), which is shown over here, has been identified, the Mobility Management Entity (MME) in the serving network, which is shown here, fetches authentication data from the home network.

So, the MME has a connection with the home network. In this picture, this is the serving network, as shown by this label here, and this is the home network. And the serving network has a connection with the home network. So, after the UE has been identified, the MME in the serving network fetches authentication data from the home network. Next, the MME triggers the authentication and key agreement protocol with the UE.

We will see that this authentication and key agreement protocol has many similarities with that in 3G systems. After this protocol has been successfully completed, the MME and the UE share a secret key, known as K_{ASME}. And ASME here stands for Access Security Management Entity. So, that is a difference in EPS compared to 3G. In the case of 3G, the MME and the UE shared two secret keys: the ciphering key and the integrity key, at the end of the authentication and key agreement process.

Here, instead, the MME and the UE share a secret key, K_{ASME}, and from this key, further keys used for ciphering and integrity protection are derived. In the EPS, the MME takes

the role of the ASME, the Access Security Management Entity. So, it is responsible for the authentication of the UE. Now, the MME and the UE are able to derive further keys from K_{ASME}. They derive further keys, which are used for encryption and message integrity.

In particular, two derived keys are used for confidentiality and integrity protection of the signaling data between the MME and UE. So, there is signaling data or control information exchanged between the UE and the MME. That is shown by this arrow: NAS protection. NAS stands for Non-Access Stratum. As we have discussed before, the connection between the UE and the MME is known as Non-Access Stratum, and the connection between the UE and the base station is known as Access Stratum.

So, two derived keys are used for confidentiality and integrity protection of the signaling data between the MME and UE. That is shown by this arrow. And another derived key is transported from the MME to the eNodeB. So, it is transported over this secure link from the MME to the eNodeB. Three more keys are subsequently derived both in the eNodeB and in the UE.

So, what are the functions of these three keys, which are derived in the eNodeB and the UE? So, two of these keys are used for confidentiality and integrity protection of the signaling data between the eNodeB and the UE. So, this is shown by this arrow labeled as AS protection. AS is Access Stratum. So, two of the keys derived—two of the three keys—are used for confidentiality and integrity protection of the signaling data between the eNodeB and the UE.

And the third key is used for confidentiality protection of the user plane data between the eNodeB and the UE. This is shown by this arrow labeled as UP encryption or user plane encryption. So, in summary, three keys are derived at the UE, and the same three keys are derived at the eNodeB, and they are used for these functions, which we just discussed. There is also confidentiality and integrity protection for the signaling and user data carried over the interface between the eNodeB and the core network. So, that interface is shown by this.

This is an interface between the eNodeB and the core network. This is another interface between the eNodeB and the core network. So, as we have seen before, the MME is a control plane element, and the serving gateway is a data plane element. The eNodeB is connected to the serving gateway as well as to the MME, and there is confidentiality and integrity protection for the signaling and user plane data carried over these interfaces

between the eNodeB and the core network elements, serving gateway and MME. Signaling data is transferred between the UE and the MME over the S1-MME interface.

This interface between the eNodeB and the serving gateway is the S1-U interface, and this interface between the eNodeB and the MME is the S1-MME interface. So, in a nutshell, the connections between the eNodeB and the core network are known as S1 interfaces. In particular, the signaling data is transferred between the UE and the MME over the S1-MME interface, and user data is transferred between the UE and the serving gateway over the S1-U interface. So, S1-MME and S1-U are different types of S1 interfaces that connect the eNodeBs to the core network. If cryptographic protection is applied to the S1 interfaces, which we just discussed here, then the protection mechanism uses IPsec, which we discussed earlier. So, this provides network layer security.

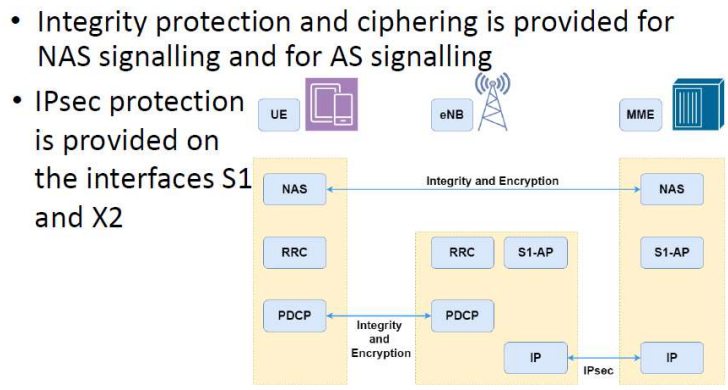
So, that is shown over here. These interfaces are protected using IPsec. The required keys are not specific to the UE. So, for example, an eNodeB may be serving many UEs in its cell. The traffic of all those UEs is transferred over these connections to the serving gateway and to the MME.

And the keys that are used for confidentiality and integrity protection are not UE-specific. So, the same keys are used for all the UEs. The X2-interface between two eNodeBs is shown over here. So, this is the X2-interface between two eNodeBs. We discussed earlier that it can be used for carrying out handovers between different eNodeBs when a UE moves from the range of one eNodeB to the range of another eNodeB.

So, these X2-interfaces between two eNodeBs are similarly protected by IPsec with keys that are not specific to the UE in case cryptographic protection is applied. So, again, these X2-interfaces are protected using IPsec, and the keys that are used are not UE-specific. So, the same keys are used for every UE. Now, this figure shows how confidentiality and integrity protection mechanisms are embedded in the signaling plane protocols. So, this is the UE, this is the eNodeB, and this is the MME.

And recall that non-access stratum is the connection between the UE and the MME in which the eNodeB acts as a relay. So, integrative protection and ciphering is provided for this NAS signaling which is shown over here. The signaling between the UE and the MME. This is the signaling information that is exchanged in the access stratum or this is the AS signaling and integrative protection and ciphering is provided for the AS signaling as well. So that is shown here. So, this is the AS signaling. Now, what are RRC, PDCP, and so on? These are different layers in the 4G network stack, we'll not discuss these in detail, but

these RRC, PDCP, etc., are different layers in the 4G protocol stack, and they perform different functions.



IPsec protection is provided on the interfaces S1 and X2. So, this is the S1 interface and IPsec protection is provided on this S1 interface and similarly, the connection between this eNodeB and other eNodeBs is the X2 interface and that is also protected using IPsec. This figure illustrates how user plane protection is provided. So, this is the UE, this is the eNodeB and the user plane element or the data plane element is the serving gateway. User plane protection is provided through confidentiality and message integrity.

So, for user data confidentiality protection is optionally provided between the UE and the eNodeB. That is shown over here. There is optional encryption between the UE and the eNodeB. And integrity protection is not applied on the user data between the UE and the eNodeB. So, we can see that on this arrow there is no integrity.

So, if integrity protection is required then that needs to be provided by the application. We see that for the user plane data encryption is provided but not integrity. For X2 and S1 interfaces, cryptographic protection for user data is provided in a way similar to that for the corresponding control plane interfaces, which we discussed on the previous slide. And the protection is by means of the IPsec protocol. One example of that is shown here.

The connection between the eNodeB and the serving gateway, this connection is secured using the IPsec protocol. So, in summary, we started our discussion of the EPS security architecture. We discussed that the authentication and key agreement protocol is performed between the MME and the UE. And subsequently, signaling data and user plane data is protected via confidentiality and message integrity is provided in the signaling data and user plane data. We will continue our discussion of LTE security in the next lecture.

Thank you.