Authentication issues in EPS-AKA protocol of 4G Cellular Networks and their respective 5G improvements

Ankit Pradhan   Venu Madhav Yatam
School of Electrical Sciences, IIT Bhubaneswar, {ap36, yvm10}@iitbbs.ac.in

April 26, 2019

Contents

1 Overview of 4G Architecture

The main 4G architectural components are :

1. User Equipment (UE): User equpiment is the 4G mobile device that includes a UICC (Universal Integrated Circuit Card) and USIM (Universal Subscriber Identity Module) running on it. This is also refered as the End User (EU).

   The mobile equipment constitutes of the following important modules:

   (a) Mobile Termination (MT) : Mobile Termination takes care of all the communication functions.

   (b) Terminal Equipment (TE) : Terminal Equipment terminates the data streams.

   (c) Universal Integrated Circuit Card (UICC) : This is the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM). Specifically, USIM stores the user and network related information such as the International Mobile Subscriber Identity (IMSI) or the users's phone number, the subscriber's Secret key etc. The IMSI uniquely identifies a subscriber and consists of three parts:

      i. Mobile Country Code (MCC)

      ii. Mobile Network Code (MNC) which specifies the subscriber's carrier network

      iii. Mobile Subscriber Identification Number (MSIN) that identifies the subscriber in the mobile network

      The USIM in the subscriber performs the authentication process.

2. Evolved Universal Terrestrial Radio Access Network (E-UTRAN) : This is also known as the access network. Evolved Node B (eNodeB) is the main component of the E-UTRAN. User equipments are connected to the core network via the eNodeBs. The architecture of the E-UTRAN (Figure 1) is described as below:

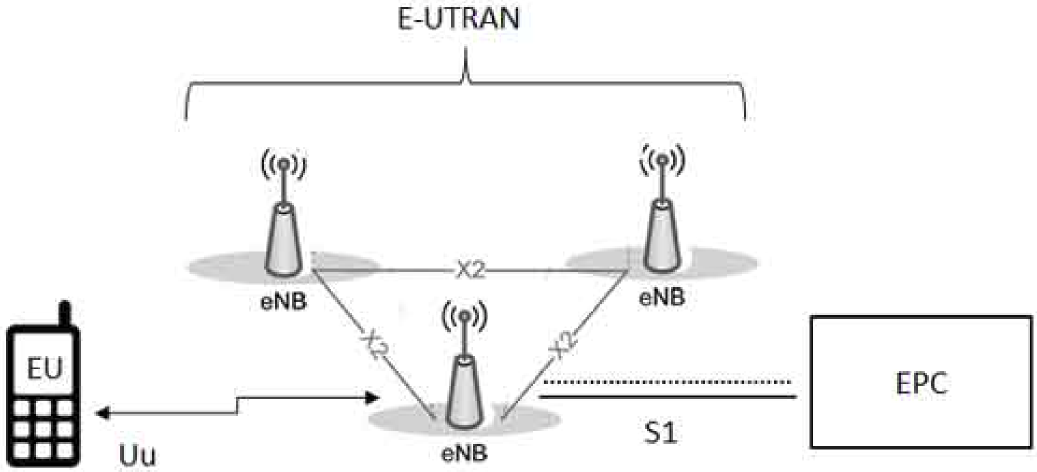

Figure 1: E-UTRAN architecture

Every eNodeB is a base station serving a region. The base station that is directly communicating with a UE is known as its serving eNodeB. A home eNodeB (HeNB) is a base station that is purchased by a user to provide services only within the home. A home eNodeB belongs to a closed subscriber group and can only be accessed by mobiles with a USIM that belongs only to the particular subscriber group.

3. The Evolved Packet Core (EPC) : The main components of the Evolved Packet Core are as shown in Figure 2:

   (a) Home Subscriber Server (HSS) : It is a central database storing the network subscriber's data and the secret keys. This is responsible for holding and generating all the necessary cryptographic information and replies back the authenticated data to the MME.

   (b) Mobility Management Entity (MME) : It is the main control node of the network. MME performs authentication and is establishes the communication link between E-TRAN and the HSS. It also decides the route of the data packets by tracking the EU's location within the network.

   (c) Packet Data Network Gateway (P-GW) : It is a router that communicates with the outside world. Connecting the core network to the external networks, it is primarily responsible to provide information for billing and charging. The Policy Control and Charging Rules Function (PCRF) in the P-GW is the policy controller. It also provides the EU's their IP addresses.

   (d) Serving Gateway (S-GW) : It is a router that forwards data between the base station and the PDN gateway.

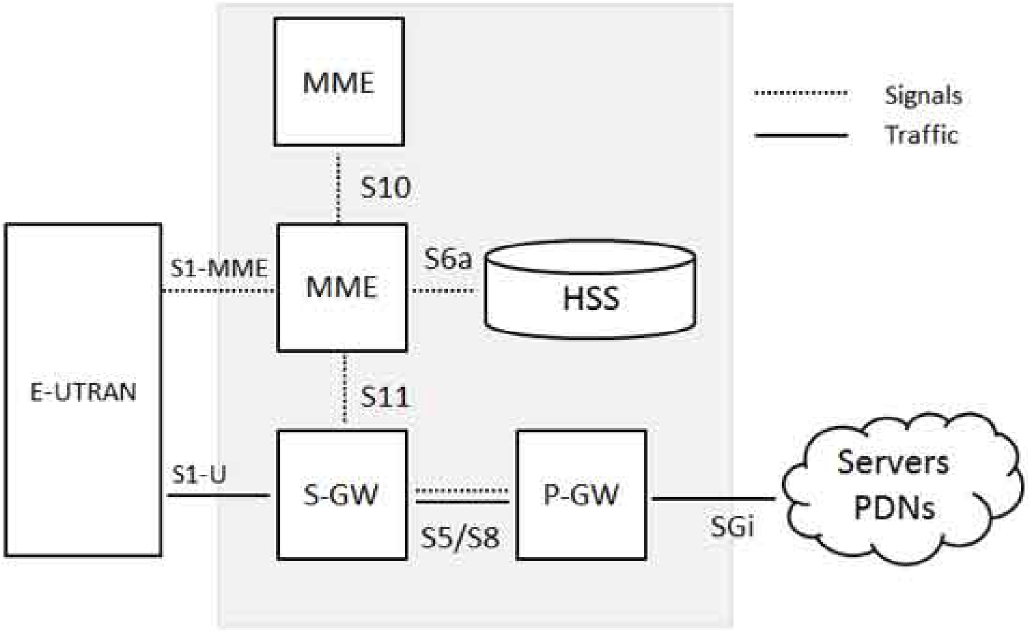

Figure 2: EPC architecture

2 EPS-AKA Protocol

EPS-AKA protocol supports the 4G authentication process in LTE networks. It is primarily an authentication and key agreement (AKA) protocol between the 4G network and UE. One of the key services provided by EPS-AKA is mutual authentication via symmetric key cryptography where the serving network and the UE authenticate each other. The authentication process also serves as an access control or authorization process allowing the UE to access the network resources. The procedure followed for authentication (Figure 3) is described as below:

1. UE first sends an *Attach Request* message to the MME containing the IMSI of the UE or the Global Unique Temporary Identifier (GUTI). GUTI is an upgradation over TMSI, which was used in 2G and 3G networks, since the same TMSI can be used by different MMEs for different UEs. GUTI was aimed at protecting the IMSI from eavesdropping attacks where the UEs location can be compromised by adversarial tracking.

2. Suppose the MME fails to recognize the GUTI (at initial request), it sends an *Identity Request* message is sent back to the UE requesting the IMSI as the response (*Identitty Response* message).

3. Now the communication is directed between the MME and HSS. The MME sends an *Authentication information* request to the HSS containing the SN identity (Serving Network Identifier) and the UE's IMSI. The home network is trusted by the UE about verifying the serving network identity (The specific serving network key K_{ASME} is computed by the home network using the SN identity).

4. The HSS generates a random number RAND and locates the UE's secret key K from the IMSI. It then provides these two items as inputs to defined cryptographic functions for generation of Authentication Vectors (AVs). An AV consists of the RAND, an AUTN (Authentication

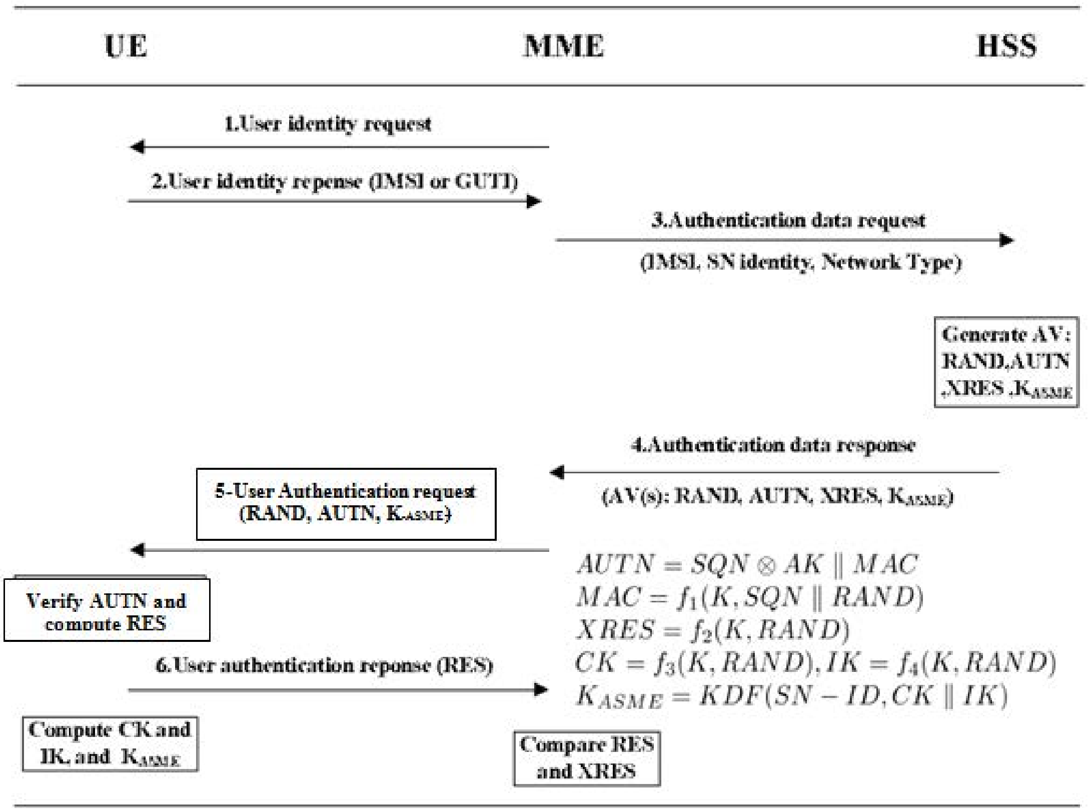
UE
MME
HSS
1.User identity request
2.User identity repense (IMSI or GUTI)
3.Authentication data request
(IMSI, SN identity, Network Type)
Generate AV: RAND,AUTN ,XRES ,K_{ASME}
4.Authentication data response
(AV(s): RAND, AUTN, XRES, K_{ASME})
5-User Authentication request (RAND, AUTN, K_{ASME})
Verify AUTN and comoute RES
$AUTN = SQN \otimes AK \parallel MAC$
$MAC = f_1(K, SQN \parallel RAND)$
$XRES = f_2(K, RAND)$
$CK = f_3(K, RAND), IK = f_4(K, RAND)$
$K_{ASME} = KDF(SN - ID, CK \parallel IK)$
6.User authentication reponse (RES)
Compute CK and IK, and K_{ASME}
Compare RES and XRES

Figure 3: EPS-AKA protocol

Token), a XRES (used by MME for authenticating the UE by checking its equality to the RES obtained from the UE), and a local master key K_{ASME}. SQN, a counter is another input to the cryptographic functions. The HSS possesses a counter for each UE. This counter is used to avoid reuse of AV by the MME and aids the UE in verifying the freshness of AVs, thus avoiding replay attacks.

5. The HSS sends the AV to the MME whilst storing the K_{ASME} and XRES. The MME sends the RAND, AUTN and K_{ASME} to the UE.

6. The User SIM (USIM) located within the UE uses the secret key K and RAND to retrieve the SQN from AUTN. It further computes the XMAC using RAND, SQN, and the AMF of the AUTN and then compares the MAC of the AUTN with the XMAC. To ensure synchronization between HSS and UE, the USIM checks whether its own SQN is not very different from the SQN obtained from the HSS. This enables the UE to authenticate the network. By computing K_{ASME}, both UE and MME obtain the same secret key to ensure the security of the connections. MME also receives a RES computed by the USIM. The UE checks whether the SQN is in the expected range, otherwise it sends a *Synchronization Failure* message. It also sends a *MAC Failure* message if the XMAC is not equal to the MAC.

7. The authentication and key agreement process is completed by the MME by verifying whether XRES and RES are equal.

The next section discusses the authentication issues identified in EPS-AKA.

3 Authentication Issues: EPS-AKA Vulnerabilities

The following table (Table 1) summarizes the notable vulnerabilities in EPS-AKA protocol (pictorially depicted in Figure 4):

Vulnerability	Effect of Attack	Point of Compromise	Possible Solutions
IMSI (or GUTI) disclosure attacks	1. Affects user and subscriber confidentiality 2. Service theft with lower bandwidth utilization 3. Affect the revenue of operators (Theft of multimedia services like voice calls) 4. Wastage of memory of MME and computational power of HSS	1. Initial Attach Request between UE and MME 2. Handover between MMEs	Public Key Cryptography (costly to implement)
SN identity disclosure attacks	1. Subscriber Location Disclosure 2. Weakening UE's data security 3. DoS against the MME 4. Connections between the UE and the network are intercepted	All communications in the network between UE, MME, and HSS involving transfer of SN identity	Public Key Cryptography (costly to implement)
Replay Attacks	Subscriber Location Disclosure	1. Authentication Request and Response between UE and MME 2. Authentication Response from HSS to MME	Dynamic request counters on UE and MMEs
TAU (Tracking Area Update procedure) based attacks	Using rogue eNodeB to obtain TAU request message from UE and further sending TAU reject message to UE induces DoS attacks against the UE, thus disallowing service	Between UE and Network	Public Key Cryptography and Digital Signatures
Bidding down attacks	1. Disclosure of UE's network and security capabilities 2. DoS attacks against UE	Between UE and Network	Public Key Cryptography and Digital Signatures

Table 1: Table of EPS-AKA vulnerabilities and attacks, with their effects, points of compromise in the protocol and possible solutions

4 Improvements in 5G

New design choices have been incorporated for the AAA in the 5G architecture. Also, there are many retained technologies from the 4G, the most important one being the use of authentication based on symmetric key cryptography through some secure element instead of the usage of public key authentication. A new type of identifier is introduced by 5G called the Subscriber Permanent Identifier (SUPI) which is identical to IMSI. The SUPI is advanced in the way that it can also be used securedly for IoT devices. The different formats availed by SUPI include the IMSI and NAI (Network Access Identifier). The utility of NAI is higher since it can include multiple identifiers including the IMSI. The public key of the subscriber's home network is used to encrypt the MSIN of the identifier for the security of the end users. This addresses the disclosure vulnerability of the IMSI.

SUCI (Subscription Concealed Identifier) contains the covered SUPI inside. The secure element of the UE must store the public key of the home network to prevent key leakage. Also, there is a 5G-GUTI, similar to the identifier GUTI in the 4G architecture. 5G authentication mechanisms are similar in working to those of the 4G systems. An end user doesn't feel any change as the authentication differences are only in the network. AKA mechanisms in 5G systems, like in 4G systems, use "serving network name" in deriving the anchor key. Hence, the specific network

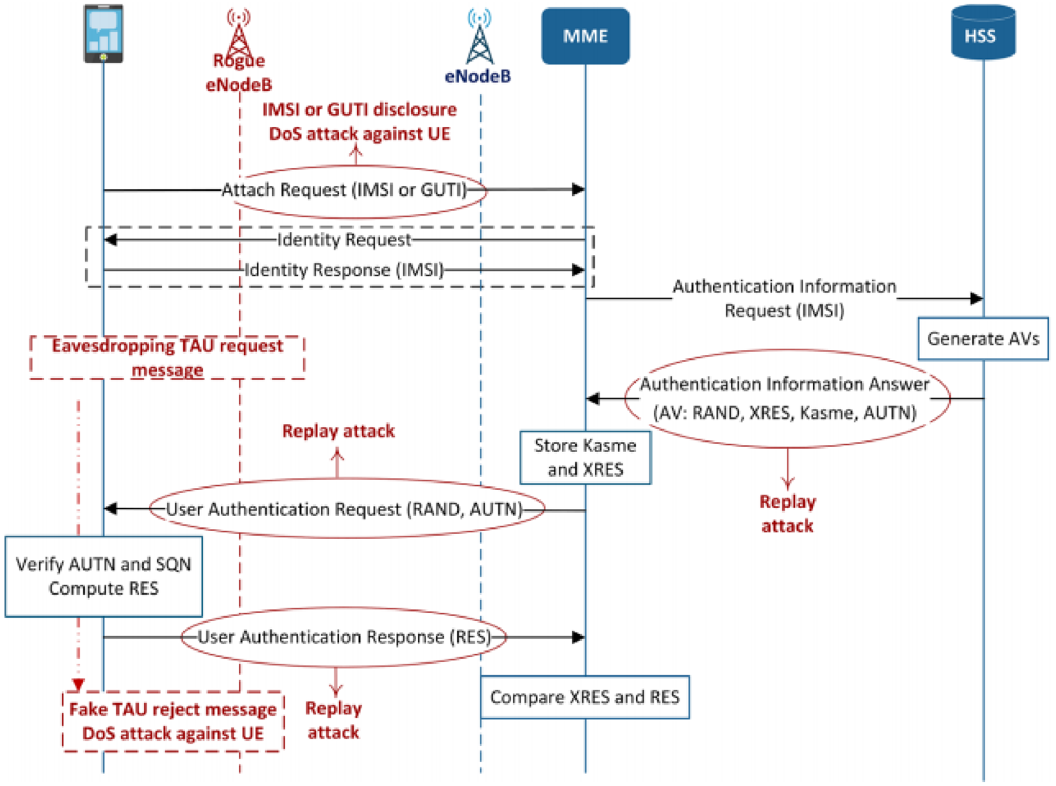

Figure 4: Attacks against EPS-AKA protocol

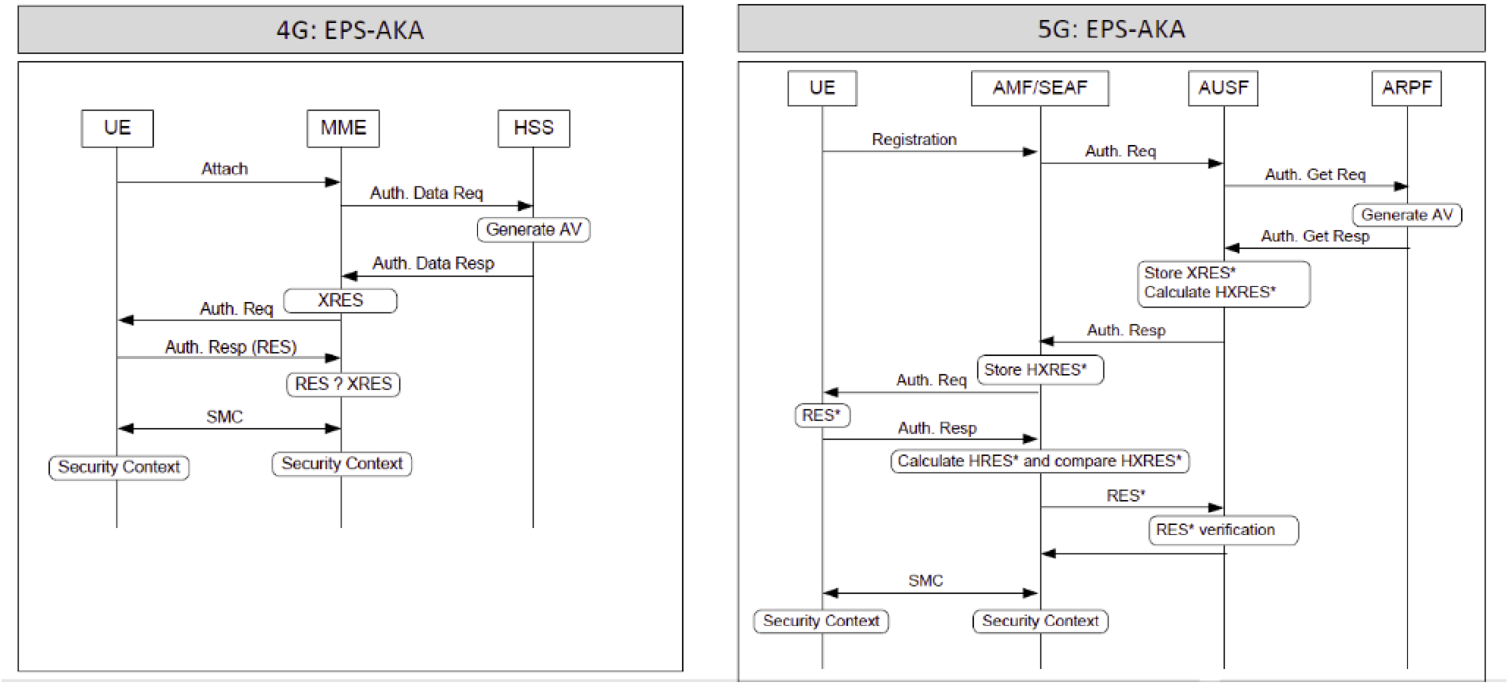

Figure 5: Differences between 4G and 5G AKA

serving the UE is in possession of the anchor key, preventing this serving network from pretending to be any another serving network. Moreover, 5G systems include a secondary protection in AKA mechanisms. To confirm the success of the UE's authentication, the visited network provides an *Authentication Confirmation* message to the home network. Also for 5G systems, the anchor key can also be used in a non-3GPP access without the necessity of initiating new authentication process. 4G systems use EPS-AKA for 3GPP access and EAP-AKA for non-3GPP access, but 5G systems allows flexibility such that both of 5G-AKA and EAP-AKA' can be used in both 3GPP access and non-3GPP access. The differences are collectively as shown in Figure 5.

References

[1] 3GPP, "Security Architecture," TS 33.401, Tech. Spec. 15.1.0, 2017

[2] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes, http://arxiv.org/abs/1708.04027/.

[3] 4G architecture https://www.tutorialspoint.com/lte/lte_network_architecture.htm

[4] New 3GPP Security Features in 5G Phase 1 https://www.researchgate.net/publication/328232888_New_3GPP_Security_Features_in_5G_Phase_1