IMSI Exchange over the air for LTE Access Network

Munawwar Sohul and Jeff Reed
Virginia Tech

(Provided as background/input to the WSRD Workshop X: Security from a Wireless Spectrum Perspective: Technology Innovation and Policy Research Needs on 09/13/2018 in Washington D.C.)

- 4G architecture, also known as SAE (System Architecture Evolution) comprises of LTE and EPC.
- The UE connects to the 4G network by signaling its presence in the eNB cell. The process is known as camping – the UE camps on a suitable cell. The suitable cell meets the following requirements:
    i. It's part of the selected PLMN
    ii. It's part of a registered PLMN or part of the equivalent PLMN list as per the most recent update from the NAS
    iii. The cell should not be barred, not reserved, and should not be in the list of forbidden areas for roaming.
- Once these criteria are met,
    i. UE sends an *Attach Request* message over the LTE radio interface to this eNB, asking to attach to the network.
    ii. eNB sends this message to the MME via the S1-MME interface.
    iii. MME validates the UE request against the HSS credentials and then selects an appropriate SGW that has access to the PLMN requested by the UE.
    iv. Once the access request reaches the PGW (which is the UE's anchor point to the desired PLMN), it is replied with an IP address. After verifying with the PCRF, the PGW may even create dedicated bearers for this UE immediately after attach.
    v. HSS drives the selection of the SGW and the SGW in turn selects the PGW based on the information already decided by the HSS. The MME is selected based on the network topology. The eNB tries to select the MME that minimizes the probability of handover and that provides load balancing with other MMEs.
    vi. The *Attach Request* message sent by the UE to the eNB contains, among other parameters, the **IMSI (International Mobile Subscriber Identity)**.
- Once attached and authenticated, it is the responsibility of the eNB to proxy the UE's message to the MME and also to establish secure connections with the UE and other core network in order to protect the UE's traffic at the radio/Ethernet border.
- Being at the border between these two topologies, the eNB is exposed to the security issues arising from both the radio and the IP networks.

❖ Security Architecture:

- The standard [TS 33.401, SAE - Security Architecture, section 5.3] describes the security requirements necessary for a secure eNB operation environment and secure eNB functioning. It leaves these specifications at a requirements level, permitting the operator to implement the exact protocols he considers for his network. These protocols are compliant to the standard as long as they meet the security requirements defined. A few key requirements include:

i. eNB should have a way of securing the cryptographic keys and information inside the device

ii. it should have secure communication links both over the air with the UE and with the MME (via the S1-MME interface), SGW (via the S1-U interface) and other eNBs (via the X2 interfaces, if they exist) for control-plane and user-plane traffic.

If the operator has a secure environment where these communications happen, he may not implement any precise security measure for the requirements defined.

- Five main area of concern with the security of the 4F architecture are:

i. Network Access Security: refers mostly to the radio attacks.

ii. Network Domain Security: defines the requirements and rules to prevent attacks over the wire, when exchanging control-plane and user-plane.

iii. User Domain Security: deals with securing the access to mobile terminals

iv. Application Domain Security: standardizes the set of rules for secure message exchange between applications on clients and servers

v. Visibility and Configurability of Security: features that informs the users about a particular security feature and whether this feature is applicable or not to the services the user is trying to access

- Authentication and Key Agreement (AKA):

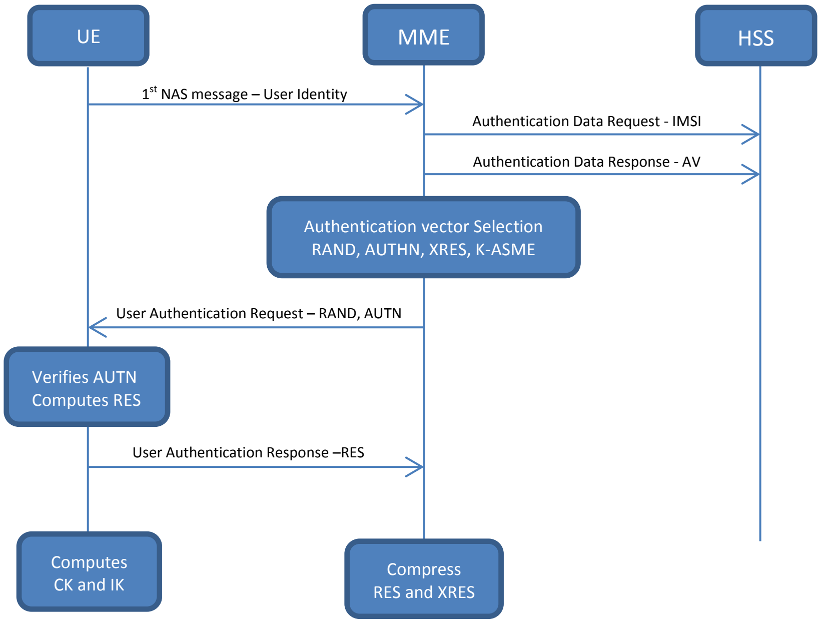
UE
MME
HSS
1st NAS message – User Identity
Authentication Data Request - IMSI
Authentication Data Response - AV
Authentication vector Selection
RAND, AUTHN, XRES, K-ASME
User Authentication Request – RAND, AUTN
Verifies AUTN
Computes RES
User Authentication Response –RES
Computes
CK and IK
Compress
RES and XRES

Figure 1: AKA exchange mechanism

- For LTE, the access procedure is Authentication and Key Agreement (AKA). The purpose of AKA mechanism is to create keying material for the Radio Resource Control (RRC) signaling, NAS signaling. It also generates ciphering and integrity keys for the user-plane. Figure 1 present the Aka procedure:
  - i. The first NAS message may be an *Attach Request,* a *Service Request* or a *PDN Connectivity Request*.
  - ii. After receiving the message, the MME verifies the UE's identity
    - a. If the UE is new to this network entirely, then the MME asks the UE for its permanent identity – the IMSI.
    - b. If the UE is not new to this network, but reached this MME by means of a TAU (tracking Area Procedure), then this MME should have a GUTI (Global Unique Temporary Identity) in the message received from the UE. MME sends the GUTI and the full TAU message to the previous MME and gets back the actual permanent IMSI and the authentication data for it. The message exchange between two MMEs takes place over the S10 interface.
    - c. If the UE roamed into this MME from a 3G network, the current UE tries to connect to the previous management entity of the UE, the SGSN (Serving GRPS Gateway) via the S3 interface and gets the IMSI information.
  - iii. The MME is the authenticator and the HSS is the authentication server. The communication between the MME and the HSS takes place over S6a interface.

❖ **Flows in Exchanging IMSI:**

- Figure 2 depicts the two flows in exchanging the IMSI for authentication purpose:
  - a. The first flow is sending the IMSI in the clear-text over the network in case of the first attach of the UE to the network or when the new MME cannot locate the previous MME.
  - b. The second flow occurs when two MMEs exchange the message to locate the IMSI of the UE for authentication purpose.

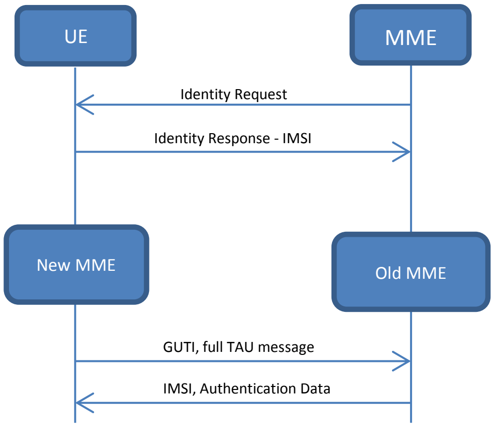

Figure 2: Message exchange to locate IMSI

The transmission of the permanent identity, IMSI, over the air at Initial Attach exchange presents a possible security scenario. EPS implements the GUTI value that is sent over the air instead of the IMSI in most of the cases as mentioned above. This way the AKA mechanism provides identity protection. The only cases that requires the transmission of the IMSI are the first Initial Attach and the attach request after the core network entities are de-synchronized. This vulnerability opens the door for a man-in-the-middle attack that can take place once the IMSI is captured.

- Cristina-Elena Vintila, Victor-Valeriu Patriciu, Ion Bica, “Security Analysis of LTE Access Network,” *ICN 2011, The Tenth International Conference on Networks*, pp 29-34, January 23, 2011

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov