NETWORK-SIDE TRUST MODEL FOR ROAMING AND NON-ROAMING CASES

Fozilov Firdavs Dilshod o'gli
Student of Tashkent University of Information Technologies named after Muhammad Khwarizmi
Beknazarova Saida Safibullayevna
Doctor of Technical Sciences, prof. Tashkent University of Information Technologies named after Muhammad Khwarizmi

Evolution of the trust model: The trust model changes as we move from a non-autonomous to an autonomous 5G system. It is believed that the trust in the network decreases as you move away from the core. This affects the decisions made when developing a 5G security system.

The trust model in the UE is quite simple: there are two trust domains - the Universal Integrated Circuit Card (UICC), which contains the USIM card (Universal Subscriber Identity Module) and mobile equipment (Mobile Equipment - ME). ME and USIM together form the UE.

The network-side trust model for roaming and non-roaming cases is shown in Figures 1 and 2, respectively, which demonstrate trust at multiple levels, like an onion.

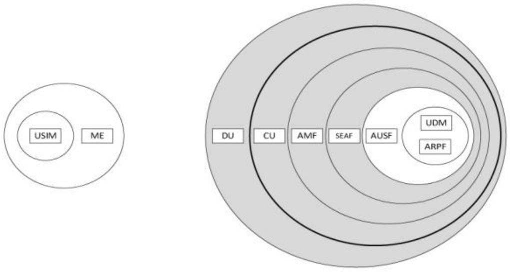

Figure 1 Trust model of non-roaming scenario

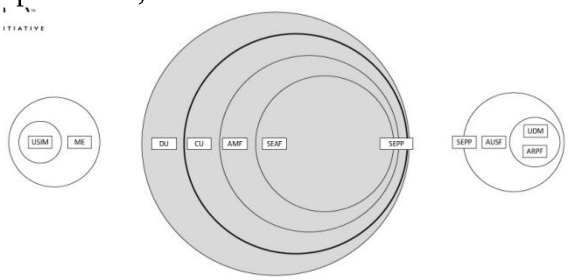

Figure 2 Trust model of roaming scenario

The Radio Access Network (RAN) is divided into distributed units (DU) and central units (CU) - DU and CU together form gNB, the 5G base station. DU does not have access to communication with clients, as it can be deployed on uncontrolled sites. The CU and Non-3GPP interaction feature (N3IWF - not shown in the figures), which completes the security of the Access Stratum (AS) layer, will be deployed to sites with more restricted access.

The Access Management Function (AMF) completes the security of the Non-Access Stratum (NAS) layer on the underlying network. In the 3GPP 5G Phase 1 standard, AMF is combined with the Security Anchor Function (SEAF), which contains the root key ("anchor key") for the visited network.

The Authentication Server Function (AUSF) stores the key obtained after authentication for reuse in the case of simultaneous registration of the UE in various network access technologies, i.e., 3GPP access networks and Non-3GPP access networks, such as the IEEE 802.11 wireless Local Area Network (WLAN). The Authentication credential Repository and Processing Function (ARPF) stores the authentication credentials. This is reflected by using USIM on the client side, that is, on the UE side. The subscriber information is stored in the Unified Data Repository (UDR). Unified Data Management (UDM) uses data stored in the UDR and implements application logic to perform various functions, such as creating authentication credentials, user identification, session continuity, etc. Active and passive attacks through the cloud service are considered both at the management level and at the user level. In a roaming architecture, the home and guest network are connected via a Security Edge Protection Proxy (SEPP) to control the inter - network connection plane. This improvement is made in 5G due to the number of detected attacks, such as key theft and altered routing attacks in SS7, as well as network node simulation and source address spoofing in signaling messages in DIAMETER, which exploited the trust nature of the internetwork.

5G Phase 1 Security (Release 15): Phase 1 5G introduces several improvements to 4G LTE security.

Primary Authentication. Device authentication in a 5G network is based on primary authentication. This is similar to what was implemented in 4G, but with some differences. The authentication mechanism has built-in home control, allowing the home operator to know if the device is authenticated on a given network and accept the final authentication call. In Step 1 of 5G, there are two mandatory authentication options: 5G Key authentication and negotiation (5G-AKA) and the Extended Authentication Protocol (EAP-AKA). Optionally, other EAP-based authentication mechanisms are also allowed in 5G. In addition, primary authentication is independent of radio access technology, so it can work with technologies other than 3GPP, such as IEEE 802.11 WLAN.

Secondary authentication: Secondary authentication in 5G is intended for authentication in data networks outside the mobile operator's domain. Various EAP-based authentication methods and associated credentials can be used for this purpose. A similar service was possible in 4G, but now it is integrated into the 5G architecture.

Security between operators: In the inter-operator interface, there are several security issues that arise from the SS7 or Diameter protocols in earlier generations of mobile communication systems. 5G Phase 1 provides security between operators from the very beginning.

Privacy Policy: The problems associated with subscriber identification have been known since the days of 4G and earlier generations of mobile systems. 5G has developed a privacy solution that protects the persistent user ID from active attacks. The public key of the home network is used to ensure the confidentiality of the subscriber's identification.

Service-based architecture (SBA): The underlying 5G network is based on a service-oriented architecture that was not present in 4G and earlier generations.

Central (CU) and distributed network units (DU): In 5G, the radio access network is logically divided into CU and DU. Security is provided for the CU-DU interface. This separation was also possible in 4G, but in 5G it is part of the architecture that can support different deployment options. DU's that are deployed at the very edge of the network do not have access to any user data when privacy protection is enabled. Even with CU-DU separation, the security point of the radio interface in 5G remains the same as in 4G, namely in the radio access network.