Survey of Network Access Security in UMTS/LTE Networks

Daniel Caragata
Departamento Electronica, Carrera Telematica
Universidad Tecnica Federico Santa Maria
Valparaiso, Chile
daniel.caragata@usm.cl

Safwan El Assad, Kassem Ahmad
Polytech'Nantes
Universite de Nantes
Nantes, France
safwan.elassad@univ-nantes.fr

Abstract — **Mobile communications have known an impressive development in recent years, and are characterized by a trend towards broadband communications and extremely diverse applications. For some of these applications, such as financial transactions, shopping or online social networks, security is of extreme importance. This paper presents a survey of the most important and most vulnerable part of the security of wireless networks: network access. The study includes the protocols used by UMTS and LTE standards as well as some of the latest protocols proposed in the literature.**

Keywords: ***UMTS, LTE, network access, security, mobile communications***.

I. Introduction

The forth generation of mobile networks, known as Long Term Evolution (LTE) or Evolved Packet System (EPS) is currently being deployed worldwide and has an impressive impact on the world given that the total number of subscriptions, 6.8 billions, is approaching world population figure, 7.1 billion [1].

The forth generation of mobile networks has been optimized for data transmission and is designed to provide broadband data at speeds of around 100 Mbps for the downlink and 50 Mbps for the uplink, very low delay, improved Quality of Service (QoS), interoperability with 2G and 3G systems and high levels of security.

Its security protocols have been improved compared to 3G Universal Mobile Telecommunications System (UMTS) in order to make it resilient to new attacks. These new attacks were possible because of the massive increase of computing power, of the availability of complex attack tools, and of the security vulnerabilities that the protocol had. The technical specifications of EPS are frequently being updated, thus showing an increased research interest and a coherent strategy to improve the security of 4th generation networks.

This paper focuses on the most critical aspect of mobile networks security, the wireless network access, and is structured as follows. Section II provides an overview of the network structure in UMTS and LTE networks. This is important in order to understand the role of the different entities that are involved in the security protocols. Section III presents the current security protocols that allow secure network access, mutual authentication and key management in both 3G and 4G networks. In section IV the latest proposals for improvement of the secure network access are presented. Section V concludes the paper identifying the main characteristics that are likely to characterize the security of 5G networks.

II. Network architecture

In this section we will present the general structure and main parts of network architecture for UMTS and LTE. Both networks contain three main components:

- User Equipment (UE): composed of two parts: the Mobile Equipment (ME) and a secure smart card (Universal Integrated Circuit Card – UICC) running a specific application (Universal Subscriber Identity Module – USIM).
- Access network (Universal Terrestrial Radio Access Network – UTRAN): also known as Service Network (SN), is the network where the UE has direct wireless connectivity. It manages temporary data about the UE, such as location information or temporary authentication data.
- Core Netork: also known as Home Network (HN) is the network that issued the secure smart card of the UE to whom the user is registered. It manages permanent data about the UE, such as type of subscription or permanent authentication data.

A. UMTS network architecture

The structure of UMTS networks is presented in Fig. 1.

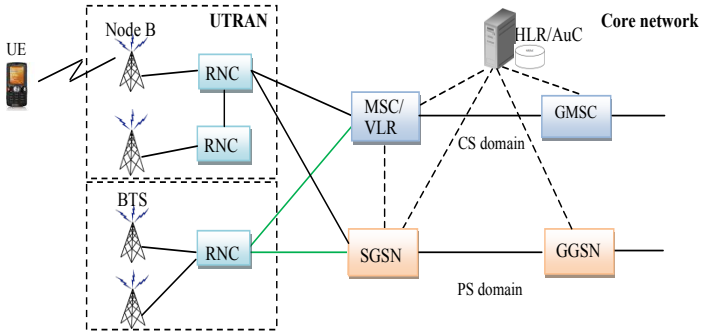


Figure 1. Architecture of UMTS network

We see that the UTRAN network, which connects the UE to the network, has two components: NodeB and the Radio Network Component (RNC). The NodeB is the radio interface of the network and manages the physical layer of the connection: channel coding, interleaving, bandwidth adaptation, etc. The RNC controls and manages the radio resources of one or more NodeB using the Radio Resource Control (RRC) protocol.

The core network has two domains: the Packet Switched (PS) domain, for IP communications and the Circuit Switched (CS) domain, legacy from Global System for Mobile Communications (GSM) and Public Switched Telephone Network ((PSTN).

The most important components of the core network are the Mobile Switching Center (MSC) responsible with network routing, the Home Location Register (HLR) a database with the permanent information of all the users registered on the network, the Authentication Center (AuC) that manages the authentication and security data, the Visiting Location Register (VLR) a database with information about the users that are registered in a certain geographical location, the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) that allow connecting the mobile network with external IP networks.

B. LTE network architecture

Fig. 2 shows the LTE network architecture.

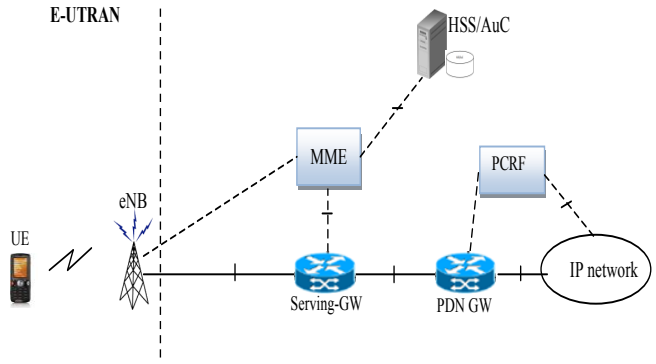


Figure 2. Architecture of EPS network

It can be seen that the structure of the network has been simplified: the core network only has the PS domain, the CS being eliminated, and there are less components with more complex functions.

The access network, called evolved UTRAN (eUTRAN) is composed only of evolved NodeB (eNB). The eNB integrates the functions of the NodeB and some of the functions of the RNC in order to reduce system latency.

The main components of the core network are the Mobility Management Entity (MME) that manages signaling between the UE and the core network, authenticates subscribers and derives security keys, among others, the Home Subscriber Service (HSS) that is an evolved VLR, the Policy and Charging Rules Factor (PCRF), an optional component that manages billing and charging, and two gateways that connect to other IP networks or UMTS networks.

III. Security protocols

In this section we will present the standard network access security protocols that are implemented in UMTS and LTE networks.

A. UMTS network access protocols

3GPP has defined the security standards for UMTS as an improvement over the existing GSM security [2]. Therefore, the robust elements of GSM standards have been preserved while new functions and services have been added on top.

UMTS security uses the Authentication and Key Agreement (AKA) procedure for both network access and key establishment. This procedure, presented in Fig. 3, is initiated by the UE that will send his International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI) to the service network in order to set up a call or to send data.

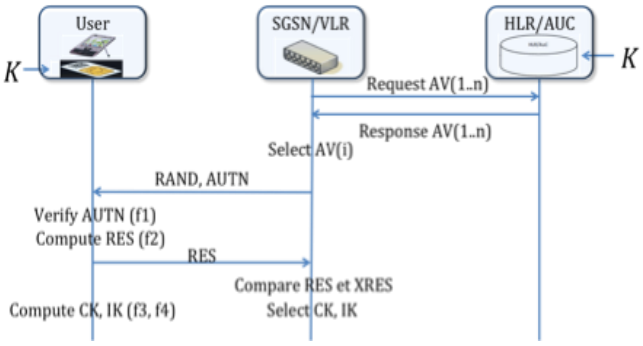
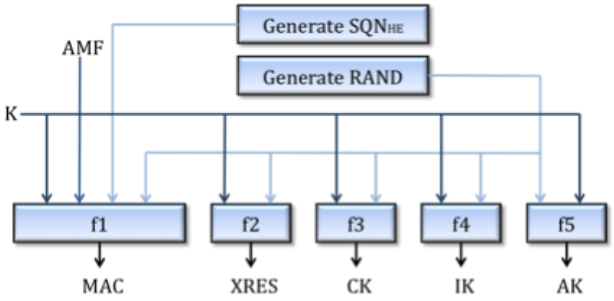


Figure 3. Authentication and Key Agreement

In an initial stage, the Service Network (SN) will ask the Home Network (HN) for a set of Authentication Vectors AV(1..n).

The AV has five components generated using five security functions: *f1, f2, f3, f4* and *f5*, [9] as shown in Fig. 4.



$$AV = RAND \| XRES \| CK \| IK \| AUTN$$
$$AUTN = SQN_{HE} \oplus AK \| AMF \| MAC$$

Figure 4. Authentication Vector generation

The AV components are:

- RAND: random value,

- XRES: the response that the service network expects to receive from the user,
- CK: encryption key,
- IK: integrity key,
- AUTN: authentication token, verified by the user to authenticate the network.

AUTN has three components:

- SQN: a sequence number, masked with the key AK,
- AMF (Authentication Management Field): a 16 bits field used for management purposes.
- MAC: a message authentication code that is verified by the user.

Each AV will be used for one AKA procedure as follows:

- the service network will send the user a User Authentication Request containing the parameters RAND and AUTN;
- the USIM verifies the authenticity of the authentication token AUTN and uses RAND and the secret key K to compute his authentication token, RES;
- The SN will verify if the received RES message is equal to the expected value contained in the AV (XRES) and, if they agree, the authentication is successful and the UE can access the network;
- the AKA procedure finishes with both UE and SN setting up the secret keys CK and IK.

B. LTE network access protocols

The authentication and key establishment procedure used by LTE is called Evolved Packet System-AKA (EPS-AKA) and is largely inspired by the UMTS-AKA, with slight improvements. The first modification consists in the fact that EPS-AKA ensures implicit authentication of the service network, not only of the home network. The second improvement is the derivation of multiple keys from the key established by the AKA procedure.

EPS-AKA, just like UMTS-AKA, is based on a permanent secret key, K, shared by the USIM and the AuC, and can be divided into three stages:

1. upon demand from MME, the HSS generates authentication vectors and transmits them to the MME;
2. mutual authentication and establishment of a secret key K_{ASME}, shared by the service network and the UE;
3. distribution of authentication data within and between service networks.

LTE security standard [3] defines 4 security functions: user identity confidentiality, mutual authentication between the user and the network, signaling and data confidentiality and signaling integrity.

1) User identity confidentiality: The goal of this function is to prevent eavesdroppers from obtaining any information related to the identity of the communicating parties. First the user identifies himself using a temporal identity called Globally Unique Temporary UE Identity (GUTI). Only after a secure communication has been established, can users identify themselves using the International Mobile Subscriber Identity (IMSI); therefore this identity is never sent unencrypted, provided that the user has a valid GUTI.

2) Mutual authentication between the user and the network: This security function allows both the user and the network to verify each other's identities. This is realized using an improved version of the previously described AKA procedure, where the UE also verifies the identity of the service network where he logs on. In the UMTS AKA procedure the UE only verifies that it is connected to a SN authorized by his HN.

3) Signaling and data confidentiality: the goal of this security function is to encrypt the content of the messages exchanged over the radio link in order to make them incomprehensible to an eavesdropper. In general, the protocols concerning the UE are divided in two levels: Access Stratum (AS), containing protocols that are executed between the UE and the access network, i.e. eNB, and Non Access Stratum (NAS) containing the protocols that are executed between the UE and the core network, i.e. MME. The encryption of the AS signaling messages and of the user data is realized by the Packet Data Convergence Protocol (PDPC), while the encryption of the NAS signaling messages is realized by the NAS EPS Mobility Management (EMM) protocol.

4) Signaling integrity: LTE standards demand that signaling messages must have their integrity protected in order to ensure the authenticity of the messages and to be sure that they were not modified in transit. This service also offers protection against replay attacks. There are very few exceptions to this rule: the messages that are exchanged before security is established. Similarly to 3G, integrity is not offered for data messages because of the high data overhead and of the low risk of an attacker modifying the data messages.

IV. Proposed improvements

In this section we present some improvements to LTE network access security that have been proposed in the literature. This will allow us to identify the main research directions that will influence the security of 5G networks. The proposed protocols draw mainly from the security analyses realized in [4,5] and we recommend [10] for a more detailed analysis.

A. Security Enhanced-AKA (SE-AKA)

The SE-AKA protocol [6] introduces important improvements to the EPS-AKA, such as using public key algorithms to protect most of the messages exchanged within the LTE network, i.e. the IMSI, the connection between the MME and the HSS and the authentication request message. The public keys must be implemented as certificates before the execution of the protocol.

The UE begins executing the SE-AKA protocol by encrypting its IMSI with the public key of the HSS. The UE sends to the MME an access request message, A, containing its encrypted IMSI, and the ID of the HSS to which the user belongs to. Upon receiving this message, the MME encrypts its identity with the public key of the HSS, generates a message B with the encrypted ID and sends both messages, A and B, to the HSS. The HSS decrypts the messages it receives and extracts the IMSI of the user and the ID of the MME. Then, the HSS sends to the MME a message, C, containing *n*, Authentication Vectors and the IMSI of the user encrypted with the public key of the MME. Afterwards, the MME sends the UE an authentication request message, encrypted with the public key of the UE. The rest of the protocol is realized exactly like the EPS-AKA protocol.

Although SE-AKA brings some improvements to the EPS-AKA protocol, it has been demonstrated that it has its limitations [7]. The first limitation is that it will always encrypt the IMSI with the same key, therefore generating the same value. Thus, an attacker can follow the encrypted value instead of the clear one. A second limitation is given by the structure of the IMSI, where most of the digits are public (Mobile Country Code and the Mobile Network Code) and only a small part of the IMSI is different for each user. Therefore, an attacker can launch a successful brute force attack on the IMSI, instead of launching the attack on the private key. Also, SE-AKA can be subject to replay attacks, and denial of service attacks.

B. Ensured Confidentiality-AKA (EC-AKA)

The EC-AKA protocol [8] protects the integrity and confidentiality of messages using asymmetric cryptography for the first three messages of the protocol, i.e. the access request from the UE to the MME, the AV request from the MME to the HSS and the message containing the AVs, and symmetric cryptography for the following messages, which are exchanged between the UE and the MME. When asymmetric cryptography is used, the messages are encrypted with the public key of the entity that will receive the messages, while for symmetric cryptography a secret key, EK, is being used. EK is computed from the secret key, K, shared by the UE and the HSS and from the nonce RandomEncKey, which is sent by the UE in its access request message.

The EC-AKA proposes interesting enhancements for EPS-AKA, but it has its own vulnerabilities [7]. More precisely, it may be subject to replay attacks, denial of service attacks or attacks that attack the authentication of MME.

C. Full Protection-AKA (FP-AKA)

The main advantage of FP-AKA [7] is that it provides a secure channel between all entities at all times. The first two messages, i.e. the access request message from the UE to the MME and the AV request from the MME to the HSS are protected using asymmetric cryptography because there are no symmetric keys established yet. These first two messages are used to establish a number of parameters that will be later used to derive shared secret keys. The following messages are protected using symmetric cryptography because this type of cryptography is faster than asymmetric cryptography.

In order to implement FP-AKA, each user needs to posses only one digital certificate, containing the public key of his home network, HSS. The service network, MME, needs to be in possession of the digital certificates with the public key of all the HSS with whom it has a roaming agreement. Finally, the HSS needs to know the certificates of all the MME that connect to it. A trusted third party, Certification Authority (CA), generates all the certificates. To our knowledge, there are no published attacks against FP-AKA.

V. Conclusions

This paper has presented an overview of the network access security in UMTS and LTE networks as well as the protocols proposed lately in the literature. It can be noted that there is a continuous preoccupation from the standardization bodies and from the research community to improve the security of mobile networks. One important characteristic of these efforts is that the new protocols build upon the old ones rather that proposing revolutionary new solutions. Another important characteristic is that the newest protocols give more importance to user's privacy, by protection of the IMSI value in a more efficient way. We also note a trend in adding asymmetric cryptography to the standards.

Acknowledgment

This work has been supported by the 23.13.84 research project of DGIP-UTFSM.

References

[1] ITU, "The world in 2013, ICT Facts and Figures".

[2] 3GPP TS 33.120, "Security Objectives and principles", 2001.

[3] TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture", 2014

[4] A.N. Bikos, N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks", IEEE Security and Privacy Magazine, 2013.

[5] S. F. Mjølsnes, J.-K. Tsay. "Computational security analysis of the UMTS and LTE authentication and key agreement protocols", CoRR, abs/1203.3866, 2012.

[6] L. Xiehua, W. Yongjun, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network, *The 7th International Conference on Wireless Communications, Networking and Mobile Computing,* 2011.

[7] K. Ahmad, "Protocoles, gestion et transmission securise par chaos des cles secretes. Applications aux standards: TCP/IP via DVB-S, UMTS, EPS", PhD thesis of the University of Nantes, France, 2013.

[8] J. Bou Abdo, K. Ahmad, J. Demerjian, H. Chaouchi, G. Pujolle, "EPS mutual authentication and cryptanalyzing SPAKA", *IEEE International Conference on Computing, Management and Telecommunications*, 2013.

[9] 3GPP TS 35.206, "3rd Generation Partnership Project; Technical Specifications Group Services and System Aspects; 3G Security; Specifications of the Mileange Algorithm Set: An example algorithm set for the 3GPP Authentication and Key Generation Functions, f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specifications "

[10] J. Cao, M. Ma, H. Li, Y. Z et al. "A survey on security aspects for LTE and LTE-A networks", IEEE Communications Surveys and Tutorials, 2014.