ALGORITHMS FOR EVALUATING THE EFFECTIVENESS OF INFORMATION SECURITY SYSTEMS IN LTE NETWORKS

https://doi.org/10.5281/zenodo.7881725

Rakhimova Sevarakhon Sanatjon kizi
Tashkent University of Information Technologies named after
Muhammad Al-Khorazmi 2nd stage graduate student

Abstract: *Fourth generation wireless broadband mobile technology is a mobile communication standard that has been continuously improved since 2010. Technological solutions have evolved that include bandwidth expansion, frequency aggregation, and advanced multipath capabilities with support for signal relaying. Every year, the number of fourth generation connections is increasing, which means that the risk of cyber attacks on user and operator equipment is increasing. The article examined the infrastructure of the fourth generation network, the components of the security architecture and their relationship. The analysis of organizational and technical measures to ensure the protection of information was carried out . Information security systembased on globally recognized LTE network security standards. The main requirements for security in fourth-generation networks are outlined, including their components, subject to their interaction. The main measures to counter the destructive impact on the objects of protection in the fourth generation networks are considered.*

Key words: *fourth generation mobile networks, security requirements, information security, LTE, technological solutions.*

INTRODUCTION

The infrastructure of fourth generation networks with LTE in terms of security is a combination of several protected components and the interconnections between them [1; 2]. The protected user equipment (UE) provides trusted applications and services to the user and is responsible for transferring data to and from the network. The UE includes a hardware- and software-secured Universal Subscriber Identity Module (USIM) that stores an International Mobile Subscriber Identity (IMSI) that uniquely identifies each user. In addition, the secret key K is stored in the USIM to obtain additional keys used during the authentication procedure in the LTE network.

Protected base stations that implement radio link layer access points to LTE networks are called eNBs or eNodeBs, with each eNB participating in the process of encrypting and protecting the integrity of radio control data, as well as encrypting user data.

The Secure Mobility Management Node (MME) in networks handles the establishment of new connections and performs the authentication process. It is designed for mobile data management where encryption and integrity protection is applied.

A secure subscriber data storage server (HSS) stores the authentication information of mobile subscribers. Thus, it plays a central role during the initial unrelated UE authentication procedure by providing the MME with user information related to information security.

MAIN PART

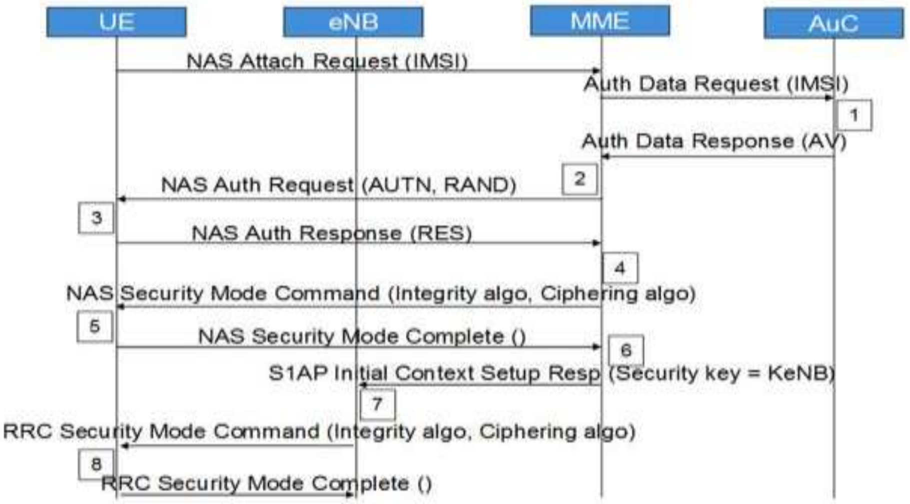
Security in LTE networks. Security in LTE networks consists of several types:

- Subscriber protection.
- Protection of transmitted messages.
- Message encryption.
- Authentication of both the subscriber and the network.
- The protection of the subscriber lies in the fact that during the service it is hidden by temporary identifiers.

To close data in LTE networks, streaming encryption is used by overlaying a pseudo-random sequence (RRP) on open information using the XOR operator (exclusive or). In these networks, the principle of tunneling connections is used to ensure security within the network. S1 and X2 packets can be encrypted using IPsec ESP, and the signaling messages of these interfaces are also encrypted.

At the moment of connecting or activating the user equipment (UE) in the network, the network starts the authentication and key agreement AKA (Authentication and Key Agreement) procedure. The purpose of this procedure is to mutually authenticate the subscriber and the network and generate an intermediate key K ASME . The operation of the AKA mechanism takes a fraction of a second, which is necessary to generate a key in the USIM application and to establish a connection with the Registration Authority (HSS). Therefore, in order to achieve the data rate of LTE networks, it is necessary to add a key information update function without initializing the AKA mechanism. To solve this problem in LTE networks, it is proposed to use a hierarchical key infrastructure. Here, as well as in 3G networks, the USIM application and the Authentication Center (AuC) pre-distribute the keys. When the AKA mechanism is initialized to perform two-way user and network authentication, an encryption key CK and a shared security key are generated, which are then transmitted from the USIM software to the Mobile Equipment (ME) and from the Authentication Center to the Registration Authority (HSS). ME and HSS, using the key pair (CK;IK) and the ID of the network used, generates the key K ASME . By establishing the dependence of the key on the network ID, the Registration Center guarantees the possibility of using the key only within this network. Next, the K ASME is transmitted from the Registration Center to the mobile management device (MME) of the current network, where it is used as a master key. Based on K ASMEa key K nas - enc is generated , which is necessary for encrypting the NAS protocol data between the mobile device (UE) and the MME, and K nas - int , which is necessary for integrity protection. When the UE joins the network, the MME generates a key KeNB and transmits it to the base stations. In turn, the Kup-enc key is generated from the KeNB key, which is used to encrypt user data of the U-Plane protocol, the Krrc-enc key for the RRC protocol (Radio Resource Control - a protocol for interaction between Mobile devices and base stations) and the Krrc-int key, designed to protect integrity.

The algorithm for authentication and key generation is shown in fig. 1:


UE
eNB
MME
AuC
NAS Attach Request (IMSI)
Auth Data Request (IMSI)
1
Auth Data Response (AV)
NAS Auth Request (AUTN, RAND)
2
3
NAS Auth Response (RES)
4
NAS Security Mode Command (Integrity algo, Ciphering algo)
5
NAS Security Mode Complete ()
6
S1AP Initial Context Setup Resp (Security key = KeNB)
7
RRC Security Mode Command (Integrity algo, Ciphering algo)
8
RRC Security Mode Complete ()

Rice. 1 Authentication and key generation diagram

Here:

Step 1: Network connection request from a mobile station (UE). The MME requests authentication data related to a particular IMSI by sending an Authentication Data Request. The AuC/HSS selects the PSK related to the particular IMSI and calculates the authentication data from the PSK. AuC/HSS sends back AV with Authentication Data Response.

Step 2. MME receives IK, CK, XRES, RAND and AUTH from AV. The MME sends AUTH and RAND with an Authentication Request to the UE.

Step 3: The UE authenticates the NW by verifying the received AUTH. Then it calculates IK, CK, RES, XMAC from its security key, AMF, (OP), AUTH and RAND. It sends RES with an Authentication response.

Step 4. After receiving the RES, the MME compares it with the XRES and if they match, then the authentication was successful, otherwise, the MME sends an Authentication failure to the UE. The MME resets the DL NAS counter. Calculates KASME, KeNB, Knas-int, Knas-enc. Sends a security mode command (integrity algorithm, encryption algorithm, NAS keyset ID, UE security function) to the NAS with integrity guarded but not encrypted using Knas-inc.

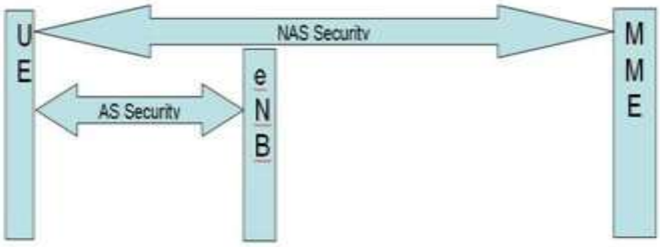
Step 5: After the NAS receives the security mode command, the UE calculates KASME, KeNB, Knas-int, Knas-enc. The UE sends the security mode to the NAS with integrity, secure and encrypted.

Step 6. After the NAS receives the security mode command from the UE, the MME sends the KeNB to the eNB with the S1AP initial context setup (secure key).

Step 7. After receiving KeNB, eNB calculates Krrc-int, Krrc-enc, Kup-enc. It then sends an RRC security key command with an AS integrity algorithm and an AS encryption algorithm.

Step 8: After receiving the RRC security key command, the UE calculates Krrc-int, Krrc-enc, Kup-enc. The UE sends the completed encryption key to the eNB by RRC.

After all the described actions, all NAS and AS messages will be securely protected and encrypted, unlike user data, which will only be encrypted. [4]



Rice. 2. Layers of security

The LTE security architecture defines the security mechanism for both the NAS layer and the AS layer.

NAS (Non-Access Stratum) security:

Made for NAS messages and belongs to the domain of UE and MME.

In this case, it is necessary when transferring NAS messages between UE and MME - integrity protected and encrypted with an additional NAS security header.

CONCLUSION

In general, protected LTE traffic can be divided into two types: user data and control data. Particular attention is paid to the encryption of user data. Encryption is activated by the "Security Mode" RRC command, which defines the message encryption algorithm. The telecom operator can also choose which integrity algorithm will be used when transmitting messages.

To establish a secure communication channel with the LTE network, mutual authentication between the UE and the network is used, which is a mandatory requirement of the security standard. Without authentication, no part of the link can fully trust the other side.

While LTE continues to improve, there are several security concerns. First of all, this is the lack of flexibility and scalability of the LTE architecture, which is why vulnerabilities and loopholes appear in networks. It is also difficult to detect and effectively counteract DoS attacks that disrupt IP access over wireless networks, while attackers are constantly creating new attacks on eNB base stations, including through user equipment UE. Counteracting these and other destructive influences is a direction for further research.

REFERENCES:

1. Threats to the security of the 4G packet network core [Electronic resource] / Positive Technologies Company. - Electron. text data. and Count. Dan. -M.: official. site, 2017. - Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/?sphrase_id=74511, free. - Zagl. from the screen.

2. Belyankov, D.A., Tsvetkov V.Yu. Security and privacy in 4G/4G/LTE networks [Text] / D.A. Belyankov, V.Yu. Tsvetkov - 56th scientific. conf. graduate students, undergraduates and students of BSUIR: tr. conf. - Minsk, 2020. - S. 122-124.

3. Analysis of the security of the 4G / LTE-A security system from the directed impact of DOS attacks [Electronic resource] / N.V. Kormiltsev, A.D. Uvarov, I.I. Khamatnurov, M.V. Tumbinskaya. - Electron. text data. and Count. Dan. - M .: official. website, 2019. - Access mode: https://www.fin-izdat.com/joumal/national/detaü.php?ro=74026, free. -Title from the screen.

4. A.N. Steputin, A.D. Nikolaev. 6G mobile communication. In 2 volumes. - 2nd edition. - Moscow-Vologda: Infra-engineering, 2018. - 804 p.