PROBLEMS OF INFORMATION SECURITY IN 5G NETWORK TECHNOLOGY

Makhmudjonov Shokhrukhbek Maksujon o'g'li
Master of Tashkent University of Information Technologies named after Muhammad Khwarizmi
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

Annotation: The article describes the new wireless standards inevitably lead to digital transformation. In addition to significantly outperforming previous generations in terms of capacity and bandwidth, 5G networks and systems will provide the infrastructure to support a wide variety of services: industrial Internet of Things and intelligent control systems, autonomous vehicles and drones, vital e-health and remote surgery, virtual and augmented reality, remote diagnostics and preventive maintenance, etc. The number of Internet devices is growing rapidly, so the old standards inevitably have to be upgraded. To work properly, many devices need higher network bandwidth. 5G works on other frequencies, gives Internet access to more devices, has ultra-fast speed and minimizes data transmission delays. Such network improvements require a radically new approach to the security model, unlike that used in cellular systems until the last fourth generation.

Keywords: Information security, 5G network, technology, wireless standards, digital transformation, wide variety of services.

The problem of security in cellular systems arose initially to solve a very specific problem: how to authenticate users connecting to the network and protect the relevant data in transit from intruders who can eavesdrop on the radio channel. This has all been properly addressed in previous generations of cellular systems. Technologies have been created that have gradually reached such a level of protection that it is difficult to find any breakthrough improvements in this area in recent years.

1G and 2G system (not)security: While the first-generation systems did not provide any communication security solution, GSM (second-generation) implemented user authentication and encryption at the radio interface level. However, the GSM security model has proven to be extremely unreliable. The cryptographic algorithm

adopted in GSM authentication (later called COMP-128) has not been validated by the cryptographic community. The idea, which later proved disastrous, was that security could be provided by the secrecy of the algorithm itself ("security through obscurity"). Unfortunately, this did not happen. Around 1998, details of the COMP-128 algorithm were leaked, and it took the cryptographic community several weeks to completely crack it and prove its complete failure.

Although the cryptographic algorithm is the most noticeable weakness of second-generation systems, the GSM security flaws are not limited to this. In particular, it does not provide mutual authentication. In GSM systems, the user was required to authenticate before being allowed access to the network; however, the reverse is not true – the user is not given the option to authenticate the radio station. The technological revolution that took place in the late 90s with the advent of software-defined radio (SDR), made not only possible, but even quite cheap attacks based on "fraudulent base stations", that is, fictitious radio stations controlled by an attacker, who, thus, was able to intercept and interfere with the messages of end users.

Finally, no security solution in the core network part has been standardized in GSM. The encryption of the radio interface was completed in the access network - the information was transmitted in clear form over a fixed network, as a result of which any attacker with access to the transport infrastructure could violate the confidentiality and integrity of the transmitted data.

3G: Security generation: The next third generation, UMTS, was the generation that made the most progress in security. First, 3G systems have completely abandoned "security through obscurity" by adopting publicly validated cryptographic algorithms of the AES (Advanced Encryption Standard) family, which are much more secure than the previous ones. The use of cryptographic techniques has also been significantly improved, both by explicitly separating ciphers and corresponding keys from data integrity, and by introducing privacy features and protecting users from end-user location-tracking attacks (location privacy). 3G systems also eliminated the problem of unauthorized base stations by providing an extremely effective method of mutual authentication.

Systematization of security and 4G: In line with the progress made in 3G systems, the fourth generation has made several improvements. First of all, this is "security by design" (SBD), that is, solving security issues from the very beginning of the LTE architecture standardization stage. The overall 4G security architecture was divided into five areas:

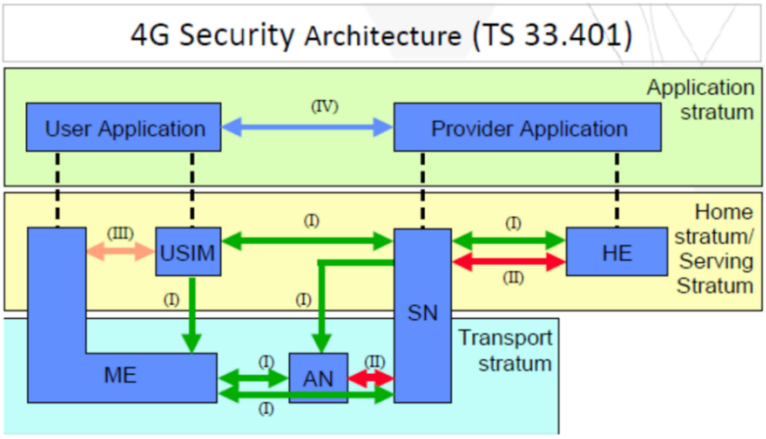
I -network access security: radio interface security and secure user access to the service;

II- network domain security: protection of network elements and the corresponding exchange of data traffic and signaling messages;

III- user Domain Security: Protecting the mobile device and its interaction with USIM;

IV- application Domain security: secure communication at the application level;

V- visibility: the ability to check whether (and what) security features are working, as well as how they are configured.



In addition, 4G systems have undergone many improvements (or fixes) in the algorithms and methods used: improved authentication and key management, improved cryptographic algorithms (including support for a new stream cipher called ZUC), end-to-end security, integration with IP security technologies, etc.;

5G Security. Security of non-autonomous networks: The first step, 3GPP towards full 5G coverage, was non-autonomous mode (Non-Standalone - NSA), also known as EN-DC (E-UTRA-NR Dual Connectivity). A key feature of the non-autonomous mode is the ability to use the existing LTE infrastructure, which makes the new radio technology available without replacing the network. EN-DC uses LTE as the primary radio access technology, while the New Radio Access technology (New Radio - NR) serves as the secondary radio access technology with User Equipment (UE) connected to both radio stations. The security procedures for EN-DC are mainly in line with the dual-connection security standards for 4G.

The main base station of the LTE eNB network checks whether the UE has 5G NR capabilities to access the secondary gNB, i.e. the 5G base station, and access rights to the gNB. The eNB creates and sends a key that will be used by the gNB for secure communication over the NR; the UE also receives the same key. Unlike dual connectivity in 4G networks, Radio Resource Control (RRC) messages can be exchanged between the UE and the gNB, thus obtaining keys used to protect the integrity and confidentiality of RRC messages, as well as User Plane - UP data.