SYSTEMATIZATION OF SECURITY OF MOBILE NETWORKS

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

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.

Key Hierarchy: The 5G hierarchy reflects changes in the overall architecture and trust model using the key-sharing security principle. One of the main differences between 5G and 4G is the ability to protect the integrity of the user's plane.

Mobility: Mobility in 5G is similar to mobility in 4G with the difference that in 5G, the mobility binding in the underlying network can be separated from the security binding.

The main use case for 5G Phase 1 was mobile broadband. Phase 2 5G will provide solutions for the Internet of Things (IoT), massive Machine-to-machine mMTC (massive Machine Type Communication), and highly reliable, Very Low-Latency URLLC (Ultra-Reliable and Low-Latency Communication). mMTC refers to a very large number of devices that transmit a relatively small amount of data and are not sensitive to latency, while URLLC refers to services with strict requirements for bandwidth, latency, and availability.

For mMTC very low data rates, dropping to a few bits per day, we will have to consider the degree of security (authentication, privacy, integrity, etc.) that can be provided. Examples are temperature sensors that provide hourly updates, farm animal sensors that provide vital status information a couple of times a day, and so on. Such devices will also have limited battery, computing, and memory resources. The requirement for security will be to reduce the overhead associated with bit security.

On the other hand, URLLC devices will require high data rates with potentially more capacious batteries and computing resources. Examples of such devices are automobiles, industrial Internet of Things (IIoT) devices such as factory equipment, virtual or augmented reality (VR or AR) devices used for real-time games or services. Providing higher data rates also means that the bandwidth of the security features must be taken into account to avoid processing delays.

Reference:

1. Lyashkov A. A. Geometric and computer modeling of the main objects for shaping of technical products // Omsk Scientific Bulletin. Series Aviation-Rocket and Power Engineering. 2017. Vol. 1, no. 2. P. 9–16.

2. N. Sedova, V. Sedov, R. Bazhenov, A. Karavka, S.Beknazarova. Automated Stationary Obstacle Avoidance When Navigating a Marine Craft //2019 International Multi-Conference on Engineering, Computer and Information Sciences, SIBIRCON 2019; Novosibirsk; Russian Federation; 21 October 2019

3. Beknazarova S., Mukhamadiyev A.Sh. Jaumitbayeva M.K.Processing color images, brightness and color conversion//International Conference on Information Science and Communications Technologies ICISCT 2019 Applications, Trends and Opportunities. Tashkent 2019.