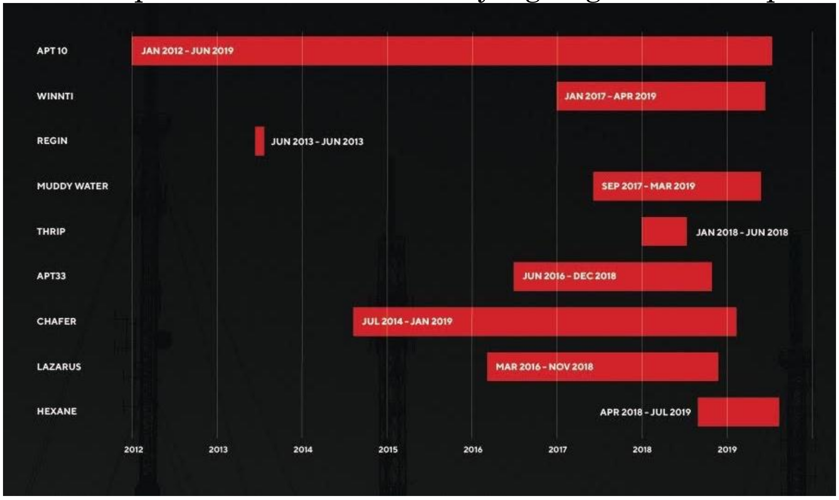
INFORMATION SECURITY PROBLEMS IN 5G NETWORK TECHNOLOGIES AND WAYS OF ELIMINATE

Makhmudjonov Shokhrukhbek Maksujon o'g'li
Master 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

5G network security Experts pay special attention to the fifth-generation mobile networks in the context of the lawsuit. On the one hand, 5G is now at the center of everyone's interest. States are interested, because this topic is at the intersection of two major factors, and corporations are trying to get ahead of each other and are fighting over, who exactly will set the technological standards. The benefit is obvious: the ability to force the entire market to play by its own rules is a significant prize. It is quite natural that hype events attract intruders, since everything new and popular gives access to a large audience. Users who rush to join the new technology will already be waiting for cybercriminals who have learned about its vulnerabilities in advance. On the other hand, the fifth-generation network differs from all the previous ones architecturally: many of its features are implemented in software, not hardware. The concerns of security experts are related to this: mobile communication is turning into a function that works on an ordinary server in an ordinary data center.

Consequently, the entire set of threats to which such an infrastructure is exposed immediately hangs over it. With a degree of conditionality, we can say this: if earlier, for example, a radio station was required to intercept traffic, now there are prospects to do with a malicious program. We can distinguish, in particular, the technology for logical network slicing (Network Slicing). In fifth-generation mobile communications, there are tools that allow you to "slice" a single pool of network addresses into subsets. If we assume that an attacker gets access to this pool, then all logical segments (each of which may belong to different companies) are at risk. The front of a potential attack expands dramatically, and as a result, the entire infrastructure may be compromised. Not surprisingly, over the past year, several scientific and expert studies have emerged about the security flaws of 5G. Teams from around the world described potential attacks of varying degrees of complexity.



In particular, it was possible to detect problems with the AKA (Authentication and Key Agreement) security protocol, identify vulnerabilities in LTE data transmission standards that allow a potential attacker to intercept the victim's calls and monitor her, and find a way to link the international mobile id IMSI to a specific phone number. The most dangerous attack can be called the ToRPEDO (TRacking via Paging mEssage DistributiOn) method, which makes it possible to fake paging messages and arrange denial-of-service (DoS) attacks. In general, the conclusions of Group-IB are as follows: the spread of fifth-generation networks will lead not so much to the emergence of new threats, but to an increase in the scale of already known ones. For example, high-speed data transmission combined with the spread of poorly protected devices will allow for unprecedented powerful DDoS attacks. IoT gadgets will give cybercriminals new opportunities to confuse their tracks: acting through a hacked smart device, the attacker will effectively hide their location. It will not do without the "classics" in the form of malware that will be distributed through compromised devices. Attacks on protocols and routing One of the main telecommunications threats that Group-IB analysts consider in several parts of the report is the manipulation of traffic by spoofing routing tables. The BGP protocol, which allows connections to be made in the shortest and most efficient way possible, is based on the following assumption: it is assumed that autonomous systems report correct information about the IP prefixes that belong to them. If an attacker gains control of a router that stands on the border of such an autonomous system and announces prefixes, then he thereby gains the ability to distort the routing. As a result, the traffic of users working with a particular site will go through the equipment that belongs to the attackers. The report lists and describes some incidents of this kind: traffic interception by the Chinese provider China Telecom, suspicious activity of the Portuguese Internet service provider Bitcanal, which was subsequently disconnected from international data transit, an attempt to attack public DNS servers in Taiwan, which was also carried out through manipulation with BGP (but worked only for a few minutes and, it seems, did not bring its authors noticeable success). Internet service providers from Southeast Asia were particularly noted. During one week in July 2018, the Indonesian organization Digital Wireless Indonesia and the Malaysian provider Extreme Broadband broadcast fake prefixes several times for Savvis, Vantiv, Q9 Networks, Mercury Payment Systems and some others. It is assumed that in this way, cybercriminals wanted to intercept traffic containing financial data and information about bank payments. In addition to routing on the Internet, the attackers ' target in 2019 was the SS7 cellular protocol (ACS-7). It solves similar problems, but in relation to mobile communication networks — and has, by the way, a similar flaw of excessive trust in data coming from a communication service provider. If the operator has a weakly protected part of the infrastructure, the cybercriminal will be able to access the protocol and control the communication of the desired subscriber. In practice, this is usually expressed in redirecting SMS messages with codes for two-factor authentication to someone else's device. Group-IB cites the example of the credit institution Metro Bank, whose customers in January 2019 suffered from such a scheme, and does not exclude that there were other similar incidents — just the British bank was the only one who announced the incident publicly. Although, as noted above, financially oriented Trojan programs for all types of devices are gradually losing popularity, this does not mean that there are fewer threats in the relevant area. Attackers actively and willingly work with ATMs, payment gateways on the Internet, systems for processing money transfers and card transactions. Bypassing two-factor authentication through imperfect communication protocols is just one of the possible techniques in this area. Conclusions Telecom is one of the priority targets for politically motivated cybercriminals who seek to use high-tech tools for espionage and targeted attacks. Many aspects of cyberwarfare are somehow related to the stability of communications, the authenticity of software, and the reliability of network protocols. Unfortunately, most of the malicious techniques and methods discussed in the report are beyond the control of an ordinary user or business. It is hoped that technology and its security will evolve, closing old gaps and avoiding new ones. Of course, telecommunications service providers themselves will have to play a significant role in this process: at the very least, they can improve the security of routers and reduce the risks of manipulating traffic.

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.