THREATS, PROBLEMS AND INFORMATION SECURITY IN 5G NETWORKS

Gafurov A.Sh.
TUIT named after Muhammad al-Khwarizmi,
Assistant of the Department of Technologies of mobile communication,
E-mail: gafurovasror686@gmail.com

Annotation: *The article analyzes information security threats in 5G data networks. The threats caused by the actions of intruders in 5G networks are considered. Problems in 5G networks are described. Formulated security in 5G networks.*

Keywords: *Providing information, 5G security issues, security threats.*

The development of cellular communication systems, comparable only to the growth in the production of personal computers and the evolution of the Internet, has not slowed down for a quarter of a century and includes several generations. The introduction of fifth generation networks (5G) will allow a wide variety of devices to work. Sensors will not only transmit the collected data to the data collection center, but also make management decisions, uniting into “smart home”, “smart quarter” or “smart city” groups, closing on themselves many of the most important processes and providing rational control of equipment. All these aspects increase the interest of attackers in such technological innovations and expose devices to a wide range of threats.

Despite the fact that fifth-generation mobile networks are positioned as secure, cybersecurity specialists managed to find a number of vulnerabilities in it.

The 5G communication network consists of the following main components:

- subscriber equipment with USIM cards;
- radio access networks (RAN), including the network
- backhaul and fronthaul1;
- network core (5GC).

However, 5G benefits not only users and businesses, but also cybercriminals. The most significant security threats facing consumers and businesses in 5G networks are:

1. Significantly larger attack surface. As 5G networks will connect more IoT devices, there will be many more entry points for targeted attacks. The number of smart devices is increasing every day, and each of them has the potential to become a target or a weapon for hackers.

2. Big consequences from cyber attacks. Businesses and infrastructures will depend on 5G significantly more than on its predecessors. Air travel, smart cars, hospitals and more will depend on 5G. With so many interconnected IoT devices and infrastructures, a security breach in one area can become a critical threat. The consequences of cyberattacks on unsecured devices could be more catastrophic than ever before, and even affect the security of society [1].

5G security issues.

5G security will become increasingly important as 5G services cover a large part of the world in the next few years.

As major network operators launch new services around the world, much of the debate surrounding the network revolves around the security risks 5G poses.

The security of telecommunications networks comes first. Security threats are a major concern for carriers in 2G, 3G, 4G and 5G networks. Among them, the Diameter signaling protocol, which is used to authenticate and authorize messages and distribute information in 4G networks, is vulnerable to a number of reasons that operators need to fix in order to effectively protect themselves from attacks. These legacy vulnerabilities in the protocol mean that 5G networks built using previous-generation networks inherit the same threats, such as tracking a user's location, obtaining sensitive information, and in some cases transferring users to insecure 3G networks.

The problem is not so much related to 5G, but the fact that new networks will work alongside legacy infrastructure. For example, an attack on a 5G network could start by exploiting vulnerabilities in 3G to obtain subscriber identities. This is why protecting legacy networks is essential to 5G security. For example, the biggest threat to IoT (Internet of Things) is DDos attacks. While the main challenges for IoT equipment are currently related to the smart home, they will move to industry and business as the use of IoT devices evolves along with 5G [2].

Distributed cloud storage is an evolution of the cloud computing architecture that allows application hosting and data processing to be moved from centralized data centers to the edge of the network, closer to where data is generated. In this new architecture, an IP connection will be terminated at the operator's edge if proper security mechanisms such as encryption and firewalls are not in place. As a result, cloud edge nodes are susceptible to spoofing, eavesdropping, and other attacks from the public Internet. It is also likely that some third-party applications will run on the same physical platforms along with Virtual Network Functions (VNFs), increasing the risk of running out of application resources required for networking functions, or worse, offering attack vectors for hackers to infiltrate the platform. .

Network partitioning is a specific form of virtualization that allows multiple logical networks to operate on top of a common physical network infrastructure [3]. With network segmentation, mobile service providers can divide their network resources for different purposes. Service providers must consider how well virtualization layers and network segments are isolated from each other. At the moment, companies are not ready to answer the following questions: if they can attack at a low level of security, can they then affect a higher level of security; if one client or one segment is compromised by malware, will other clients or segments be infected as well.

It will also increase the number of possible threats that can be exploited by attackers and increase the potential severity of the impact of such attacks. Greater reliance on a single supplier increases exposure to potential interruption of supply, for example due to a commercial failure, and its consequences. It also exacerbates the potential impact of vulnerabilities and their possible exploitation, particularly where the dependency is on a high-risk provider.

Threats to the availability and integrity of networks will become major security concerns. 5G networks are expected to be the backbone of many mission-critical IT applications, and the integrity and availability of these networks will be major security concerns. Although 5G is subject to the Authentication and Key Agreement (AKA), a system designed to establish trust between networks, it is currently possible to track people nearby using their phones. You can even eavesdrop on phone calls in real time [4].

The SS7 protocol, also known as Signaling System No. 7, refers to a data network and a set of technical protocols or rules that govern the exchange of data over them. Despite being several decades old, it is still heavily used in 2G and 3G networks. The flaws in the protocol are not new, but the problems have continued to worsen in recent years [5]. Not only that, but even LTE-only networks using the Diameter protocol instead of SS7 connect to previous generation networks. This means that even 4G networks that use Diameter are vulnerable to some attacks through SS7 networks [6].

Operators have become so focused on 5G that they are taking less action on 2G and 3G networks, a blind spot they cannot afford given the potential threats it poses to both the network and its subscribers. The gaps in the network mean that hackers can track a customer's every move, listen in on calls, and even disconnect them from service.

The heterogeneity and complexity of 5G infrastructure will require the application of security at multiple levels, across multiple domains, with a mix of centralized and distributed, physical and virtual deployment. For previous generations, manual intervention to mitigate threats may be normal. But given the speed of the network with the transition to 5G and the fact that the possible threats and their complexity only continue to grow, manual operations are not enough. Security must be completely automated - automatic detection and elimination of threats with holistic visibility is required.

5G has developed security controls to address many of the threats faced by today's 4G/3G/2G networks. These controls include new mutual authentication capabilities, improved subscriber identity protection, and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to improve network and service security.

5G provides proactive measures to limit the impact of known threats, but the introduction of new network technologies creates new potential threats for the industry.

When developing 5G standards, the principles of Secure by Design were adopted, which led to:

- using mutual authentication. Confirming the trust of the sender and recipient and ensuring the security of end-to-end relationships;

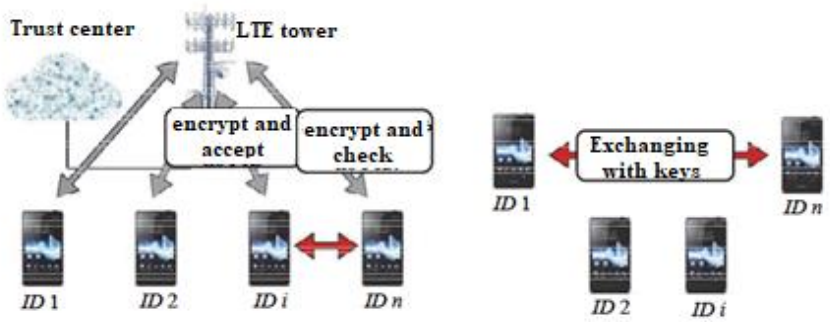
- the alleged "open" network. Removing any security assumptions from the overlay products or processes;

-confirmation that all links can be intercepted.

Ensuring information security in 5G networks.

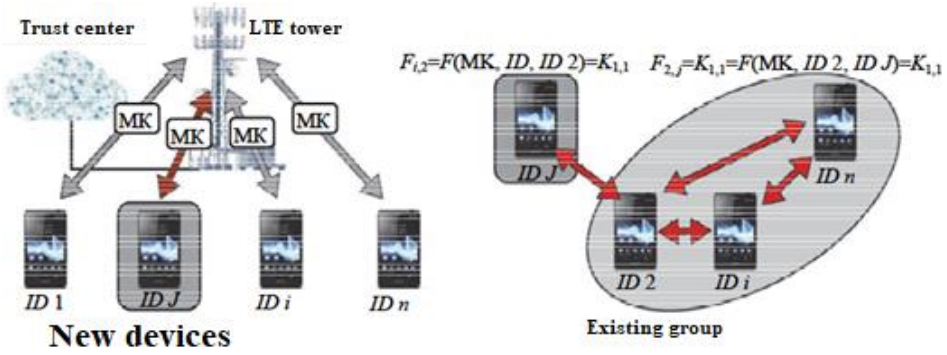
Overview of current solutions. The key requirements for systems without permanent centralized control can be defined as follows [7]: a reliable communication control algorithm; an adaptive mechanism for quick response to topology changes and failures of individual network nodes; possibility of wireless relay communication; the possibility of continuous secure communication even if the infrastructure network is unavailable.

Particular attention in this work is focused on the tasks of ensuring information security in terms of establishing a secure connection between "unfamiliar" or "untrusted" devices. Despite the innovative formulation of the problem, due to the developing peer-to-peer communication technology “device-to-device” in the context of cellular assistance, the history of the issue is quite extensive and is partially considered in [8–10]. For example, the well-known Diffie-Hellman key exchange algorithm [11] provides a zero-knowledge property for each side, but requires a reliable channel for its successful application. Taking into account more recent developments, today, traditionally, a public key infrastructure (PKI) is used as a center of trust (i.e., a certification representative) for distributing public keys and ensuring communication of end devices [12]. A simplified diagram of the PKI is shown in fig. one.



Rice. 1. Secure data transfer in the presence/absence of a public key infrastructure: PKi, PKn - public keys, ID - unique device identifier, i, n - serial numbers of devices

If the network under consideration does not provide for a centralized control device, a paired key can be used to establish a direct connection [13]. It is important to note that when using this method, devices will not be able to obtain information about their paired devices other than their ID. Therefore, it will be necessary to use cryptography based only on public identifiers [14, 15] and verify the device signature based on a unique identifier. However, in this case, a personal secret key is needed for decryption. The corresponding service can be implemented using a private key generator (PKG), which will only be used if it is available in the system.



Rice. 2. Distribution of keys, where MK is the master key, and J is the serial number of the new device

It should also be noted that in case of temporary unavailability of the SPC, a group of users connected to the SPC earlier can generate (or use an existing) master key (MC) [16, 17]. Accordingly, a new device can access the network, as shown in fig. 2. A new paired key can be generated as a function of MK and a set of identifiers ($F_{i,j}$ = $F(MK,ID_i,ID_j)$) and obtained as follows:$F_{i,1} = F(MK,ID_i,ID_1)$

$F_{i,2} = F(MK,ID_i,ID_2)$

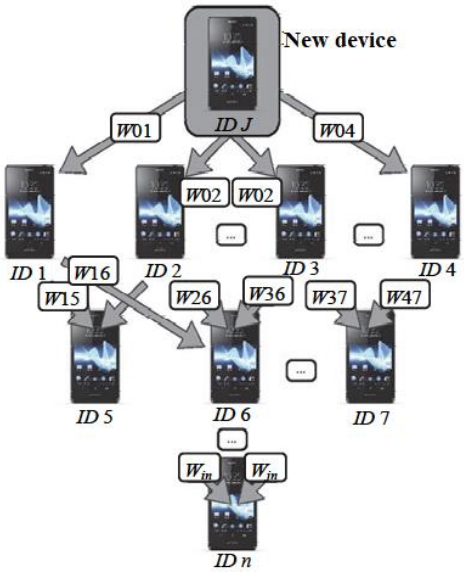
…

$F_{i,i} = F(MK,ID_i,ID_i)$

$F_{i,n} = F(MK,ID_i,ID_n)$

In sensor networks, devices usually do not use the MC after generating a paired key [18], i.e.

MK is disposable. This approach is used mainly due to the static topology of most networks of this type. In the considered device-to-device architecture, MC continues to be used in order to ensure the continuous connectivity of new devices to the peer-to-peer network, even in the absence of a connection to the cellular network. In addition, a new MC can be generated in case of restoration of communication with the base station.



Rice. 3. Trust policy based on Pretty Good Privacy: Wij is the level of trust between nodes i and j

Notably, the device can store the paired key $\mathbf{F_{i,i}}$ with itself. This is done mainly for cases where a new user happens to be nearby, i.e. when the target device is connected to the cellular network and requests the MK directly from the network coordinator in order to obtain a new key and connect to the neighboring device

Another important issue in cellular-assisted peer-to-peer networks based on geographic proximity is the issue of trust. For example, consider the popular solution based on the Pretty Good Privacy (PGP) trust system [19]. The trust level can take values from zero to one and is defined as the sum of the products of the trust levels of already known users $t = w01w11 + w02w12$, as shown in Fig. 3. If the result of the trust function is close to or equal to 1, then a decision can be made to trust the user. Otherwise, the user may be denied connection.

Conclusion

The functioning of the considered systems "device-device" is similar to the operation of self-organizing networks, but has a key difference - in the case of "device-device" systems, all communication devices (were) associated with a cellular base station, at least for some time, which sufficient to distribute initial security-related information (master keys, certificates, etc.). Therefore, classical distributed security solutions (for example, sensor networks) can be significantly improved in the case of device-to-device communication by exploiting the possibility of (periodic) access to a trusted cellular infrastructure.

The known problems of the communication protocols of the previous generation networks were taken into account when developing the 5G network architecture. However, new 5G technologies such as virtualization and new use cases bring new kinds of security threats to network operators. Despite all the security mechanisms in 5G networks, achieving long-term security will require ongoing efforts by telecommunications service providers responsible for implementing standards, and

operators themselves responsible for the correct configuration and compliance with recommendations.

The most important thing that companies and IT professionals need to know is that some of the current understanding of data security needs to be adapted to the requirements of 5G technology, as the introduction of 5G will expand the possible threats.

Advanced security measures, such as encryption applied to data stored or in transit, will need to be applied to the selected 5G service at every point on the network.

Data encryption is an important first step, but not the only one, as companies must ensure that they remain in control and fully protect the entire lifecycle of their encryption keys, creating a truly perfect security strategy for their 5G services.

REFERENCE:

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: учебник для ВУЗов. – СПб.: БХВ- Петербург, 2014. – 400 с.
2. Джефер Г.П. Архитектура и процедуры обеспечения безопасности для систем 5G. 2021. С. 254.
3. Самойлов А.С. 5G-стандарт сотовой связи. 2020. С. 196.
4. Тихвинский В.О., Коваль В.А. Сети мобильной связи 5G. 2021. С 401.
5. Тинцзинь Д. Развитие сетей 5G в России. 2021. С. 184.
6. Стефан П. 5G Пятое поколение мобильной связи. 2021. С.290.
7. Омётов А.Я., Кучерявый Е.А., Андреев С.Д. О роли беспроводных технологий связи в развитии "Интернета Вещей" // Информационные технологии и телекоммуникации. 2014. № 3(7). С. 31–40.
8. Lu Q., Miao Q., Fodor G., Brahmi N. Clustering schemes for D2D communications under partial/no network coverage // IEEE 79th Vehicular Technology Conference (VTC Spring). 2014. P. 1–5. doi: 10.1109/vtcspring.2014.7022860
9. Perrig A., Stankovic J., Wagner D. Security in wireless sensor networks // Communications of the ACM. 2004. V. 47. N 6. P. 53–57. doi: 10.1145/990680.990707
10. McDaniel P., McLaughin S. Security and privacy challenges in the smart grid // IEEE Security & Privacy Magazine. 2009. V. 7. N 3. P. 75–77. doi: 10.1109/msp.2009.76
11. Hubaux J.-P., Capkun S., Luo J. The security and privacy of smart vehicles // IEEE Security & Privacy Magazine, 2004. V. 2. N 3. P. 49–55. doi: 10.1109/msp.2004.26
12. Diffie W., Hellman M.E. New directions in cryptography // IEEE Transactions on Information Theory. 1976. V. 22. N 6. P. 644–654. doi: 10.1109/tit.1976.1055638

13. Liu D., Ning P., Li R., Establishing pairwise keys in distributed sensor networks // ACM Transactions on Information and System Security (TISSEC). 2005. V. 8. N 1. P. 41–77. doi: 10.1145/1053283.1053287

14. Shamir A. How to share a secret // Communications of the ACM. 1979. V. 22. N 11. P. 612–613. doi: 10.1145/359168.359176

15. Shamir A. Identity-based cryptosystems and signature schemes // Lecture Notes in Computer Science. 1985. V. 196. P. 47–53. doi: 10.1007/3-540-39568-7_5

16. Perrig A., Szewczyk R., Tygar J., Wen V., Culler D.E. SPINS: security protocols for sensor networks // Wireless Networks. 2002. V. 8. N 5. P. 521–534. doi: 10.1023/a:1016598314198

17. Du W., Deng J., Han Y.S., Varshney P.K., Katz J., Khalili A. A pairwise key predistribution scheme for wireless sensor networks // ACM Transactions on Information and System Security (TISSEC). 2005. V. 8. N 2. P. 228–258. doi: 10.1145/1065545.1065548

18. Zhu S., Setia S., Jajodia S. LEAP+: efficient security mechanisms for large-scale distributed sensor networks // ACM Transactions on Sensor Networks. 2006. V. 2. N 4. P. 500–528. doi: 10.1145/1218556.1218559

19. Zimmermann P. Why I wrote PGP // Part of the Original PGP User's Guide. 1991.