ARTICLE HISTORY: Received: September 20, 2021 Accepted: November 13, 2021 Published: November 19, 2021

5G NETWORK THREAT ANALYSIS

Kononova N.V., Grobova S.K.,
Azarova E.R., Kononov M.N., Palashchenko V.N.

Abstract. This article is about analyzing threats in the network 5G.
Keywords: network, threats, 5G

In the coming era of the massive 5G Internet of Things (mIoT), we are expected to have 1000 devices connected to each person, and these devices will be components of the "5G operating system" for our smart cities, smart homes, smart transportation, smart healthcare, Industry 4.0, and more [1]. To ensure this, we will need complex systems, mechanisms to maintain these devices, corporate and telecommunications data centers, public clouds. They all play a role in each of the most use cases, rotate dynamically and are accessible via virtualized networks. And the solution to these multi-criteria tasks will, of course, be complex artificial intelligence systems. This promising new world is already here, and it creates unique cybersecurity challenges that will make our past cybersecurity paradigms obsolete. 5G is not just a next-generation network, but the potential for new ways of being, new technologies and new industries. What recently existed solely in the realm of science fiction, with 5G will become possible in the real world. This technology offers a platform for integrating many different aspects of 21st-century life in creative and exciting ways [2]. It is necessary to carry out this integration correctly and in a timely manner, taking into account the issues of comprehensive security. On the one hand, the population is more globalized and integrated than before, but on the other hand, people seem to be more polarized and compressed. Finding a balance between these forces is key. Realizing 5G's full potential will require collaboration, but also smart security. There may be value in the fact that any government cares about security and privacy, but this can do more harm than good. It's time consuming, costly and distracting from the much more serious challenges inherent in 5G adoption. In 2020, many countries associated the transition to the fifth generation with the spread of the coronavirus COVID-19. There is a widespread belief that network of bots has been established in the UK and the US to promote a conspiracy theory that 5G towers are contributing to coronavirus infection, which has contributed to the massive arson of 5G towers. This absurdity has led many people to believe that 5G networks negatively affect the body and suppress the immune system, which makes it harder for a person to resist viruses.

As it rolls out, 5G is rapidly becoming the backbone for the functioning of national critical infrastructures. Previously, this was not possible with 3G or 4G, but today 5G will reallocate resources, transportation, medical services, agriculture, water supply and sanitation systems, energy, defense and many other vital sectors [3]. This network will quickly become the infrastructure on which virtually all areas of life depend - the most critical of critical infrastructures. The progress will be incredible, we will be able to experience previously unimaginable levels of efficiency. We will see the strengthening of new technologies such as autonomous vehicles and remote surgery. But as systems become more unified on critical 5G infrastructure, risks are transforming and increasing. Instead of critical infrastructure, 5G itself will become a prime target for cyberattacks.

Therefore, today it is necessary to pay close attention to 5G security, when the network is still in its infancy and the problems may not be so catastrophic.

5G networks are the next step in the evolution of mobile communications, which will provide completely new possibilities for a variety of uses on various devices in many industries. In the near future, everything will work on 5G, it will change market relations, affect the processing of information in the world in real-time. Now we can only imagine how medical procedures, financial transactions, remote industrial automation, military operations or the work of emergency services will take place. Therefore, it should come as no surprise that 5G is expected to become the most important infrastructure.

Artificial intelligence in the form of machine learning has dramatically improved internet and security and has potential for 5G. This will optimize investments and reduce costs through accurate 5G network planning, predicting capacity expansion, access to automatic coverage optimization, enabling dynamic scheduling of cloud network resources, and enabling intelligent 5G network slicing. In the coming years, artificial intelligence will help move from the existing human-based management model to a self-directed automatic management model. With this evolution, a reasonable transition will be achieved in the operation and maintenance of the network. Of course, new challenges will arise that telecommunications and cybersecurity professionals have never encountered, such as artificial intelligence black boxes, the inability to test it for deliberate backdoors, or adversarial learning, which is remote reprogramming of neural network algorithms. In 5G, the security system becomes more complex, with a network architecture more flexible, logically separated and connected to the Internet. There will be a need for a secure, integrated system that includes applications, cloud, data center, network and endpoints.

In addition, 5G subscribers are recognized in various use cases such as M2M, industrial automation, IoT, etc. These devices use different radio access technologies and are equipped with different security features. Such devices are susceptible to MitM attacks, hacking of the firmware and operating system, tracking attacks, botnets, etc [4].

5G architecture requires the introduction of new network concepts and the adaptation of some existing ones. Architectural evolution is recognized primarily as an adaptation to cloud operations and network virtualization.

5G will facilitate the work of edge computing, which removes computation from the "core" of the network and puts it at or near the data source. Mobile Edge Computing (MEC) reuses the CUPS architecture to allow user plane functions and applications closer to the edge of the network. This is partly what makes 5G latency possible below 5ms. Computing will be hosted between the devices themselves, corporate data centers or near-edge computing, device vendor data centers, public cloud, all owned and operated by different service providers. All this means that specialists will struggle to maintain the same level of security as when all major processes are concentrated near the computing core that they control. Perimeter security will go away with the arrival of 5G and mIoT [5].

Network slicing, another 5G networking feature that will allow multiple virtual networks to be built on top of a shared physical infrastructure, will become a fundamental architectural component of a 5G network to suit most 5G use cases. Portions of the network can be assigned to specific domains or use cases, such as specific critical infrastructures, so that the network can operate more efficiently and reliably. But this will create new security challenges, as each piece of the virtual network may require unique security capabilities that need to be managed in a coordinated manner. It is necessary to isolate network slices to prevent malicious attacks and the propagation of vulnerabilities or failures to other components within and between slices.

The challenge is proving the risks of missing critical virtual machines for a network slice - a completely virtual slice of the network and compute that can pass through the public cloud, through the main, transport, and accessible networks, all the way to your peripherals, and which is mostly outside your control.

In the digital world, encryption has become the main mechanism for protecting information, and will also affect the security of 5G, and vice versa [6].

However, while encryption methods were developed to provide corporate security over the Internet, they are currently being co-opted into cyber attacks.

Network visibility is becoming more complex. Where encryption is used, the network operator's ability to analyze traffic and infer whether it is malicious is limited. Security solutions must be able to assess secure and unsecured traffic using encryption while assessing which traffic is contaminated and which is not. Since deep packet analysis is no longer viable due to encryption and data volume and speed, other technical solutions such as Encrypted Traffic Analytics should be investigated.

In previous generations of networks, mobile operators had direct access and control over all system components. However, 5G mobile operators do not have full control over the system, as it is logically and physically dislocated. User and data privacy is severely compromised in shared environments where the same infrastructure is available to different stakeholders. In addition, there are no physical boundaries of the 5G network as cloud storage and NFV functions are implemented.

Effective 5G security cannot be achieved with a one-size-fits-all approach. Different 5G system facilities will have different security needs - understanding this will be fundamental to building secure network operations.

References

[1] Schneider P, Mannweiler C, Kerboeuf S 2018 Providing strong 5G mobile network slice isolation for highly sensitive third-party services (Barselona: IEEE WCNC)

[2] Kumar T, Liyanage M, Ahmad I, Braeken A, Ylianttila M 2018 User privacy, identity and trust in 5G (Is Part of: A Comprehensive Guide to 5G Security) pp 267-279

[3] Frascolla V, Englisch J, Takinami K, Chiaraviglio L 2018 Strinati Millimeter-waves, MEC, and network softwarization as enablers of new 5G business opportunities (Barselona: IEEE WCNC)

[4] Ahmad A, Atzori L 2020 MNO-OTT collaborative video streaming in 5G: The zero-rated qoe approach for quality and resource management IEEE Trans. Netw. Serv. Manag. 17 (1) pp 361-374

[5] Ahokangas P, Matinmikko-Blue M 2018 Novel context and platform driven business models via 5G networks (Bologna: IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications)

[6] Zhou X, Li R, Chen T, Zhang H 2016 Network slicing as a service: enabling enterprises' own software-defined cellular networks IEEE Commun. Mag. 54 (7) pp 146-153