

5G Network Technology & Security

TechRounder PDF Edition

Live article: <https://www.techrounder.com/technology/5g-network-technology-security/>

By Vipin PG | Published April 20, 2021 | Updated June 18, 2021 | Format: Article | 5 min read

In brief

5G network capabilities go beyond the highest ever speed of mobile Internet connection. The new mobile communication standard can become a universal infrastructure for interaction between people, smart devices, organizations, and even the economy's sectors.

5G network capabilities go beyond the highest ever speed of mobile Internet connection. The new mobile communication standard can become a universal infrastructure for interaction between people, smart devices, organizations, and even the economy's sectors.

Such total connectivity has a dark side as emerging cyber threats are growing to an ever-greater scale. This article discusses current 5G network security threats and the basics of ensuring their protection.

How can 5G be used?

Unlike the previous generations of mobile networks aimed at mass consumption (voice communication services, mobile Internet access), the 5G standard is being created mainly for the benefit of the corporate and public sectors. Three main scenarios for using 5G networks include:

1. Enhanced Mobile Broadband (eMBB) with peak data rates up to 25 Gbps. Application: 4K live streaming, AR/VR services, cloud gaming, and other high-traffic services.
2. Ultra-Reliable Low-Latency Communication (URLLC.) Data transmission latency reduced to 1ms. Application: self-driving vehicles, remote technologies (for example, robotic surgery).
3. Massive Machine-Type Communication (mMTC) that may support up to 1M base station connections per km². Application: development of consumer and industrial IoT (power supply, manufacturing, safe city, etc.).

Security Threat Architecture and Landscape

Let us review the key architectural features of 5G networks and the associated security challenges.

1. The radio access network (RAN) builds upon the new 5G NR (New Radio) standard that enables necessary characteristics for a given scenario to be achieved: bandwidth, minimum latency, or massive connections. According to the concept of converged architecture, other radio access networks (4G-LTE, Wi-Fi) must be connected to a single core of the 5G network. Possible risks: A large number of connections and high bandwidth increase the attack surface. IoT devices are less hack proof.
2. The backbone architecture (network core or 5G Core) is based on cloud technologies and virtualization of network functions (NFV, SDN), which allows creating many independent segments and supporting services with a different set of characteristics. Segmentation also allows providers to offer network infrastructure as a service to organizations. Possible risks: Increased impacts of failures or abuses due to the scale of use.

3. 5G involves the active use of mobile edge computing technology (MEC). These can be, in particular, corporate applications running on service provider's networks: intelligent services, financial services, multimedia, etc. It should be noted that in this case, the 5G provider's networks are integrated into the corporate infrastructure. Possible risks: New opportunities for entering corporate networks, placement of MEC equipment outside the protected perimeter of an organization.

4. Centralized network management (O&M) infrastructure is getting more complex as it supports many service segments at once. Possible risks: More serious consequences of resource abuse and/or O&M configuration errors.

Among the most significant threats to each of the main components of the 5G network are the following:

Threats to RAN

- DDoS traffic generated by terminal devices.
- Introduction of fake base stations.
- Attacks on wireless interfaces: user's data interception, spoofing.

Threats to the backbone network and operator services

- Software and hardware failures of core elements, misconfiguration.
- Malicious code Infections or exploitation of vulnerabilities of infrastructure components.
- Violation of segment isolation, unauthorized access.

Threats to MEC

- Physical access of an attacker to the equipment.
- Fake or vulnerable third-party applications.
- Infiltration into corporate or provider networks through MEC nodes.

Threats to 5G infrastructure posed by external networks

- DDoS attacks originating from the Internet
- Unauthorized access to the service provider APIs.
- Unauthorized access to the control panel.

Protection Approaches

Based on the current versions of the 5G standard, as well as on international experience in the development of complex security solutions, let me determine what measures will be necessary to counter threats inherent in 5G networks:

1. Protection at the standard level

- Splitting data transfer protocol layers into the three planes: Control Plane, User Plane, Management Plane. Isolation, encryption, and plane integrity control.
- Encryption of subscribers' and signaling traffic.
- Increasing the size of the traffic encryption key from 128 bits to 256 bits.
- Introduction of the unified subscriber authentication mechanism for various types of wireless communication.
- Support flexible security policies for segments.

2. Protection at the level of solutions, equipment, and network infrastructure

- Multi-layer isolation and protection of the integrity of SDN and VNF components, including the hypervisor, virtual machines, OS, and containers.
- Ensuring high availability of virtual machines for fast recovery from various attacks .
- Authentication of MEC applications.
- Authorization of API requests.
- Using multi-factor authentication when accessing the corporate network.
- Using whitelisting of devices and services.
- Protected communication channels between a base station, MEC, and corporate networks.
- Trusted hardware environment, secure device boot.
- Detection of attacks in real-time aimed at network nodes and virtual infrastructure components employing AI algorithms.

3. Protection at the network management level

- Multi-factor authentication and delimitation of access to segments by O&M.
- Fake base station detection tools that leverage the monitoring of service events.
- Safe management of the user data, as well as analytical and service data of the provider: encryption, anonymization, safe storage, and deletion.
- Centralized management of vulnerabilities and information security policies, big data analysis for anomaly detection, and early response to attacks.

The security of 5G networks is not to be limited to technical protection measures. It should encompass joint efforts of mutually trusting parties which include standard developers, regulators, vendors, and service providers.

The introduction of a new mobile cybersecurity scheme is underway. GSMA and 3GPP are developing it jointly with a range of cybersecurity regulators, including NESAS / SCAS (Network Equipment Security Assurance Scheme / Security Assurance Specifications).

NESAS / SCAS provides the following benefits

- Protection for the most specialized industrial access points and associated security threats that have to do with radio interface, NAS, web security, and more.
- Unified, measurable, readily available, comparable, understandable, and applicable specifications.
- Reduced fragmentation of security requirements and reduced unnecessary provider costs.

The providers, by using these solutions, save time and costs while doing vendor assessments. They will be able to define strict and uniform safety standards and ensure a high level of safety.

Wrapping up this article, it is worth promoting the idea of creating joint innovative projects (vendor-provider - OTT provider - B2B and B2G clients) aimed at testing how commercial products for 5G networks would use cybersecurity standards and the best practices. Projects like these can also demonstrate how 5G security features can be properly used and improved.

References

1. iotforall.com - enhancing-iot-security - <https://www.iotforall.com/enhancing-iot-security>
2. macsecurity.net - view / 279-remove-searchbaron-virus-from-mac - <https://macsecurity.net/view/279-remove-searchbaron-virus-from-mac>