DELL Technologies

5G CYBERSECURITY

Anitha Rosely

Specialist 2, Inside Product

Dell Technologies

Anitharosely.rosely@dell.com

Haseeb Makarabbi

Senior Sales Engineer Analyst

Dell Technologies

Haseeb.makarabbi@dell.com

DELL Technologies Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Introduction

As common to all new technology, there will always be a vulnerability that will come with it. With 5G (the 5th generation of wireless data networks), people usually think about higher data speeds, but it's not the only advantage or use case 5G offers. Due to its low latency, low power consumption, and high data capacity, 5G opens several possibilities for Internet of Things (IoT) devices to be connected on a scale never seen before. It opens more use cases for smart homes, smart campuses, or even smart cities.

Most 5G networks will be managed by software, mostly using Artificial Intelligence (AI) and Machine Learning (ML) models. Software is needed because 5G is designed to handle enormous amounts and varying types of data and it will be needed for auto-scaling and properly handling the load too. Threat actors will try to take over that software to control it and manipulate the network and they can also try to target the ML and AI models by poisoning the data. Doing so would enable them to create blind spots so that they can bypass the security or fly under the radar.

High-band 5G frequencies can hold the biggest bandwidth, but it also comes with the cost of coverage. This means that the data can only travel a significantly shorter distance compared to its predecessors. Network providers are trying to address this by installing smaller cells in different spots in an area, such as lamp posts, opening a lot of attack surfaces for threat actors. For example, if they compromise one of these small cells, they can perform man-in-the-middle attacks to listen in on the network traffic and manipulate the data. This will add another problem; with more points to secure, it could only take one of these small cells to become compromised to affect the entire network. 5G is a new technology, and as is common with all new technologies, there will always be new vulnerabilities that will be discovered along with it. The best way to handle all the new vulnerabilities is to be aware of the attack scenarios and mitigations, which will be covered in this article in detail.

5G will do much more than significantly improve your network connection. It opens new opportunities, enabling us to deliver ground-breaking solutions that benefit the entire society.

5G Network Security Objective

In the 5G Network security realm, we are protecting user data and enabling network resilience which implies whatever data our network nodes are processing must be secured. In this scenario, data means the keys of the network, such as public keys, private keys, RSA key. and so on.

To protect vital personal identifiable information carried on telco networks – phone number, cell ID, etc. – all the keys as well as subscriber data that will be stored in the User Data Repository must be secured. The telco network is robust and has many components. Thus, we need to make take steps to limit or eliminate network downtime. The best approach is to target maintaining confidentiality; for example, when a message is sent from point A to Point B, no third party should be able to see the message/data. There should be data integrity that the message sent from Point A to point B should be the exact copy that point B is receiving, ensuring no data tampering between these points.

Equally important is data availability. There should always be a redundant node in the network to make sure data is not lost. Suppose there's an unexpected traffic increase; the availability of your network should not be compromised. Another consideration is traceability which means for example if anybody is accessing some nodes or escalation of privileges occurs. You should have the ability to trace it back in terms of who has done it and what command has been executed so you can reverse engineer the instance and analyze what's going on inside your network.

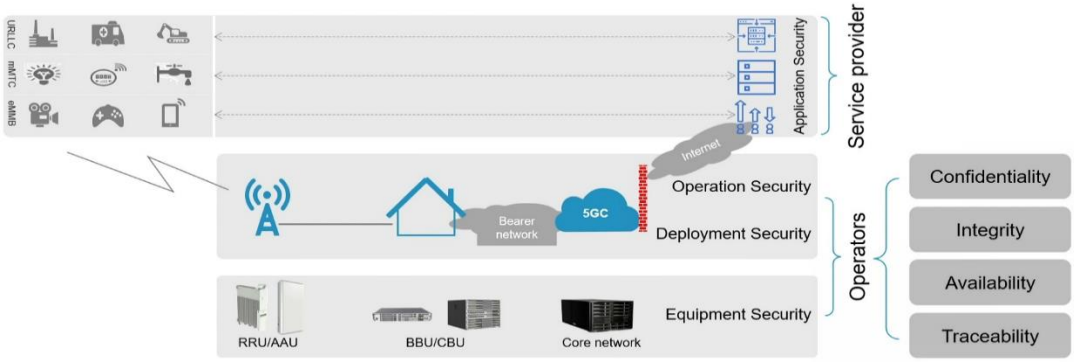

Figure 1: 5G Network Security Target

Key Assets of 5G Network

5G Networks is made up of data assets and equipment assets, which is further divided into hardware and software assets as shown in Figure 2.

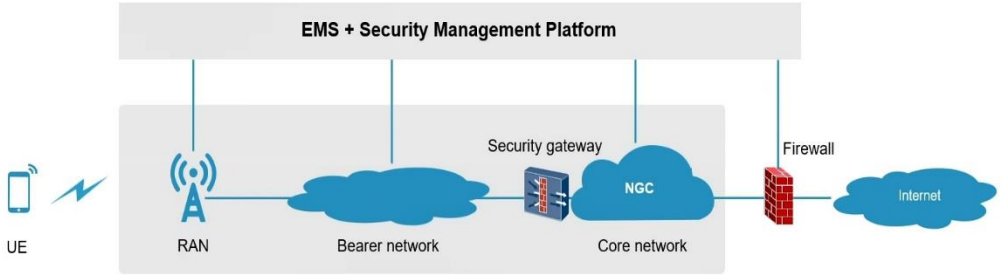

Figure 2: Assets of 5G Networks

Data assets is basically the user communication data, how the user is communicating with the network. It also has privacy information, such as subscription and location information. etc. as well as some critical reports such as measurement reports, CDRS, and key data for system operation. It also holds all the logs management data which is needed to support confidentiality and integrity of the data assets

Hardware assets hold all the data center equipment. Some are listed below:

- RAN BBU/RRU Hardware
- Cabinet
- COTS Server
- Firewall & Security gateway hardware
- Router and switch hardware

Software assets tell us what software layer is used in your network function virtualization (NFV) stack and all the software that is used in the 5G network. Some are listed below:

- RAN, core network and EMS Software
- Operating system software
- Docker software
- DB Software
- Open-Source and third-party software

5G Threats in its Network Architecture

Let's look at the 5G architecture at a high level. We have the Radio Access Network (RAN), the Emergency Management System (EMS), and the OSS platform. We also have a core network and then inside those pieces, you are connected to the internet for example having a Signaling Connection Control Part (SCCP) carrier or ISP or any third party that you can connect to. It can also be your roaming network so this is another domain you're connected to. You then have a multi-access edge computing platform, i.e. AWS, wavelength, or Hyperscalers that provide the edge computing facility. Essentially, this is how a SCCP carrier or ISP or any third party that you can connect to traditional 5G architecture looks like.

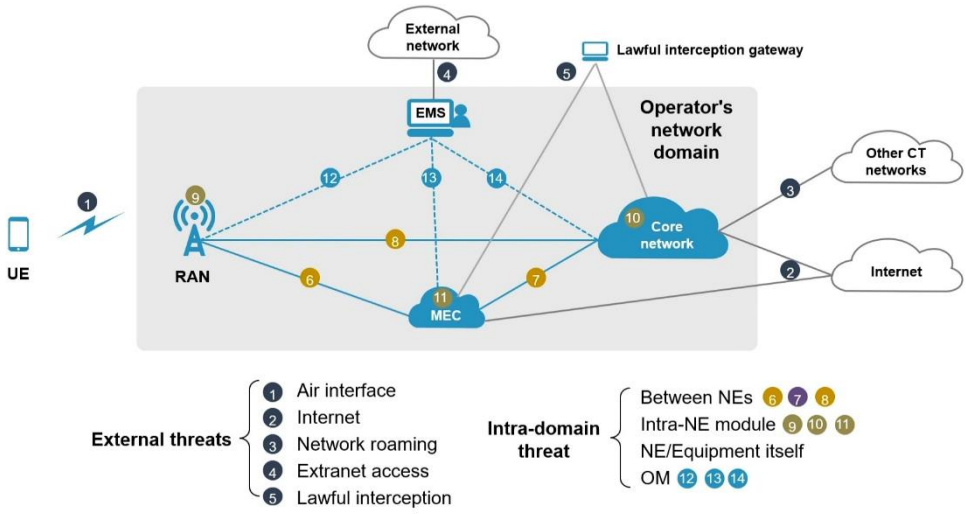

Figure 3: 5G Network Security Threats

In Figure 3, we can easily divide this into external threats which are posing threats to us externally, for example UE, internet, Extranet access and network roaming.

We also have intra-domain threats which are internally to the domain, for example between RAN and Core network, OSS and the multi-access edge computing (MEC) domain or all the things that are happening inside this network.

Threats from Outside the Operator's Network

There are five possible external threats that can happen. Let's have a quick look at all of these:

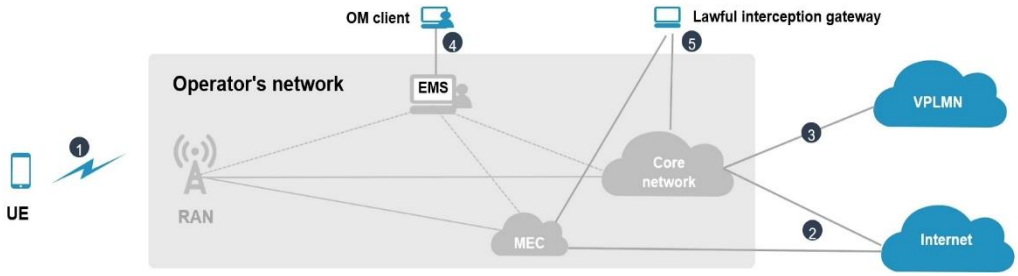

Figure 4: Threats from Outside the Operator's Network

1) **Air Interface Security Threats**

- Theft/Tampering of user data and Information
- Deny user access due to DDoS (Distributed Denial of Service)
- Illegal access to the network by unauthorized terminals
- Pseudo base station
- Trigger terminal fallback to 2G
- Malicious interference

2) **Internet Security Threats**

- Leakage or tampering of user data during transmission
- Spoofing network applications
- Denying data services due to DDoS on the Internet
- Unauthorized access to exposure APIs

3) **Roaming Security Threats**

- Forgery transfer operator and service rejection
- Leakage or tampering of user data during transmission

4) **Security Threats of External Access to EMS**

- Leakage of sensitive user information during transmission
- Unauthorized operation by Unauthorized users
- Malicious operations by Unauthorized users
- Breakdown O&M functions due to DDoS
- Web attack (SQL Injection)

5) **Lawful Interception Security Threats**

- Illegal interception gateway access
- Leakage of intercepted target ID
- Interception data leakage due to attacks from interception port

Intra-domain: Threats Among Network Equipment's (NEs) and within NE

Under the Threats among NEs & within NE, we have 3 types of threats:

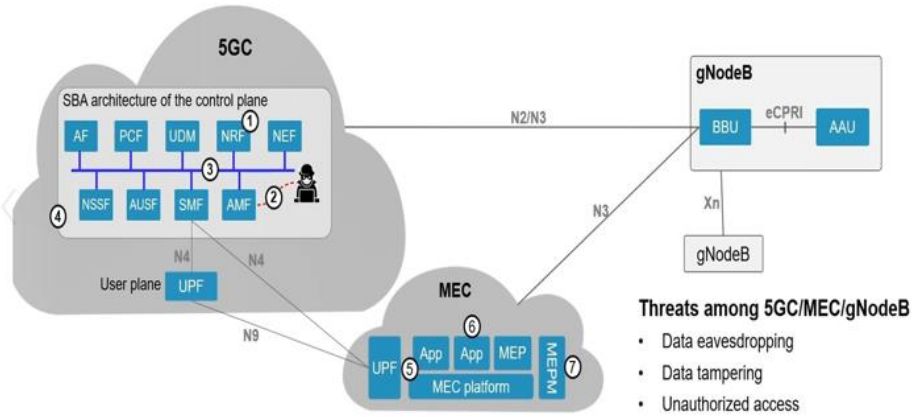

Figure 5: Threats Among NEs and Within NE

A) **Service-Based Architecture threats within 5GC**

1. Attacks occur on Network Repository Function (NRF). As a result, services cannot be registered or discovered.
2. Attackers imitate Network Functions to access unauthorized data.
3. Eavesdrop and tamper of data occurs among the Network Functions
4. These attacks usually happen based on the existing Hypertext Transfer Protocol Secure (HTTPS) vulnerabilities

B) **Threats within MEC (Multi-access edge computing)**

1. Malicious apps attack the MEC, User Plane Function (UPF) or Virtual Network Functions (VNFs)
2. This attack creates competition for resources among apps which, in turn, affect performance of other apps.
3. Unauthorized third-party application management and O&M.

C) **Threats among 5GC/MEC/gNodeB**

1. Data eavesdropping: Attackers can employ a variety of tactics to launch eavesdropping attacks, which often involve the use of a range of eavesdropping equipment to listen in on conversations and monitor network activity.
2. Data tampering: Web applications are vulnerable to data tampering, which is one of the most serious security risks they face. It's utilized to update or edit files in online applications, which are typically employed by multibillion-dollar businesses all over the world.

3. Unauthorized access: Unauthorized access can also happen if a user tries to access a part of the system that they shouldn't. They would be refused access and potentially receive an unauthorized access message if they tried to enter that location.

Intra-domain: Key Threat Analysis for NEs and Equipment

Under the Threats for NEs & Equipment, we have four possible types of threats:

A) **Threats to Hardware and Software security**

1. Unauthorized access to equipment via a physical interface.
2. Unauthorized operations on NEs.
3. Unauthorized software replacement or malicious software implantation.

B) **Threats to Data Security**

1. Locally stored confidential information is stolen or tampered with, such as keys and user context information.
2. User privacy information is stolen or tampered with, including subscription data and CDRs.
3. Unauthorized access to user-Plane data from other Planes.

C) **Threats to Cloud Security**

1. Exploitation of open resource software vulnerabilities.
2. Unauthorized resource use and data reading.
3. Difficult to find problems with multi-vendor integration.
4. Eavesdropping or tampering with application layer communication context via virtual network.

D) **Threats to Slice Security**

1. Unauthorized access between slices or UE access to unauthorized slices.
2. Resource preemption between slices leads to resource overconsumption.
3. Unauthorized slice O&M.

Intra-domain: O&M Security Threat Analysis

In Figure 6, client is connected to EMS. The EMS is in turn connected to both gNodeB and 5GC. This is an environment where there is possibility of O&M security threats.

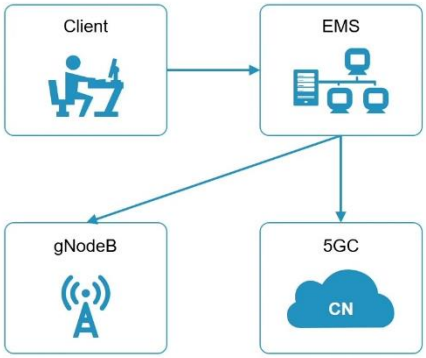

Figure 6: O&M Security Threat

From the client side, some threats may arise due to Unauthorized access, Password cracking/Leakage and Malicious operations by authorized users while the gNodeB can face issues when there is a Malware implantation.

The EMS could face a user privacy leakage and on occasion, log deletion/Tampering could also happen. Threats for the 5GC happens when the sensitive O&M data is tampered or leaked to the attackers.

None of these threats suggests that we should halt our progress toward 5G's benefits. It does, however, suggest that our current 5G strategy should be reconsidered.

How can the world win the 5G race?

- **Reverse underinvestment in cyber risk reduction**: The necessity of making proactive cybersecurity investments cannot be overstated. A constantly changing environment requires enterprises to make significant expenditures in new technology, procedures, and compliance with increasing rules, even in older network topologies. Cyber investments are frequently directed from corporate board levels all the way down to management for most public organizations and large private corporations. Small and medium-sized businesses, on the other hand, lack the means and capacity to invest in IT security, making them the preferred entrance point for cybercriminals. 5G technologies demand significant security investments because they introduce new dangers that cannot be addressed with present security measures. SMEs, smart homeowners, and other firms involved in supplying critical infrastructure products or services must spend extensively in new systems to proactively address recognized cybersecurity vulnerabilities.

- **The market for DevSecOps is increasing**: Most software developers today must incorporate DevSecOps into their development processes to create safe solutions. Rather than putting security into an already created product, this is the approach of building security into every phase of the production lifecycle. It requires including cybersecurity as a design element in the development phase, as well as deploying all new projects. Because 5G is based on software, it's

more critical than ever to incorporate security not only in software but also in hardware and firmware development. This could result in new laws requiring regulatory bodies to impose baseline security requirements in all 5G hardware and software development environments and centers.

- **Using AI and machine learning in security**: The crucial role of AI and ML in the development of 5G is an established reality. Driverless vehicles, for example, rely on 5G networks for real-time communication, but they also need AI and ML capabilities. They navigate a smart city using a combination of AI, sensors, radars, and cameras, rather than human operators. From a security standpoint, the majority of 5G network threats target software that controls critical processes. They require countermeasures that are software-based and sophisticated. People should not be used as defenses against machine-based attacks. The benefit of employing AI-powered security solutions is that they effectively self-learn and update to fit in any scenario.

- **Emerging best practices**: As new technologies develop, best security practices must evolve. Because 5G technologies have whole new infrastructures and dangers, most earlier network security standards are inapplicable. The best security measures, according to the National Institute of Standards and Technology (NIST) () Cybersecurity Framework, are to identify, protect, detect, respond, and recover. These may be appropriate for protecting enterprises from external and internal threats, but they are ineffective for developing 5G IoT systems and devices. While industry-specific best practices can be useful, they can only be as strong as their weakest link. They impose the greatest burden on users who are ill-informed and may not realize if they are following best practices.

- **Using lead indicators instead of log indicators**: To communicate cyber-preparedness between government agencies responsible for oversight responsibilities and interdependent commercial enterprises, 5G networks demand the use of a leading indicator mechanism. Prioritizing shared cybersecurity risk assessments as a best practice for organizations and their supply chain partners is one example that will be made achievable. Observing a regular programme in which government regulators and company boards routinely engage using leading indicators builds trust, accelerates the closing of the 5G gap, and leans more toward positive outcomes in the event that attackers succeed.

Conclusion

To address the difficulties of huge connectivity, flexibility, and cost, 5G will leverage mobile clouds, SDN, and NFV. With all their advantages, these technologies also come with security risks. As a result, in this article, we've highlighted the primary security concerns that, if not addressed effectively, could become more dangerous in 5G. The security threat vectors cannot be completely realized at this moment due to limited standalone and integrated deployment of these technologies in 5G. Similarly, as more user devices, such as IoT, are connected and more diversified sets of services are offered in 5G, communication security and privacy problems will become more visible.

It is likely that when new 5G technology and services are deployed, new forms of security threats and issues will emerge. However, addressing these issues from the beginning of the design process through deployment will reduce the risk of security and privacy breaches.

References

- https://learn.g2.com/advantages-of-5g-technology
- https://www.facebook.com/CyberVisionptyltd/videos/is-5g-a-cyber-security-threatnew-technology-always-brings-new-challenges-will-5g/2869151699968394/
- https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/07/24/tk-bijlage-5g-toolbox-implementation-report/tk-bijlage-5g-toolbox-implementation-report.pdf
- https://www.forbes.com/sites/arthurherman/2019/03/26/how-america-can-still-win-the-battle-for-5g/
- https://cybersguards.com/5g-cybersecurity/