SecurityGen

Telecom Security. Transcending Generations.

Edition 1, Sep 2022

5G

Decoding the ecosystem and its vulnerabilities

www.secgen.com

This paper covers the following points

1 Business Challenges

1.1 False assumptions - The security paradox

1.2 Best practices and guidance: are these enough, clear and practical?

1.3 Security still an after-thought

2 Technical Challenges

2.1 Threats and security deficiencies original to 5G that were not observed before

2.2 New and old threats brought to 5G by reused technologies and backward compatibility

3 Conclusion

The adoption of 5G is set to transform global connectivity and spark large-scale disruption in telecommunications and IoT (Internet of Things). Projected to add USD 1.3 TN to the worldwide GDP by 2030, 5G networks are making it possible for billions of different devices to connect and interact with each other at speeds that are 10x faster and with lower latency. However, with all the excitement around the many benefits that 5G offers, it is easy to forget that this ground-breaking technology requires the simultaneous management of multiple networks — 3G, 4G, and 5G, and new technologies, each with their own complexities and vulnerabilities.

As we pursue a more digitally connected future, anticipating the demands of 5G security while mitigating and managing existing threats will become critical to providing network security and ensuring customer trust. Therefore, understanding 5G security implications is crucial to our ability to secure the ecosystem of devices and applications that sprout from that network. Also, we need to know how network operators and organizations can manage these challenges and build a 5G network based on trust and security.

Over the past half year, we have worked closely with our clients as they prepared and rolled out 5G networks. And during these engagements, we identified a list of issues and possible threat vectors which could tamper with network security. In this edition, we will discuss these security challenges under two heads – business and technical issues.

BUSINESS CHALLENGES

1.1 False assumptions - The security paradox

There is a general assumption among organizations that 5G networks are cyber-resilient by default. And nothing else needs to be done once deployed as 3GPP assigned vendors, and all the expert geeks have already taken care of everything – embedding cybersecurity into the architecture of the new networks. Well, it is only partially true. There are dramatic changes, improvements and new security features in 5G compared to previous generations.

But on the other hand, the type of system complexity, the amount of technologies utilized inside (yes, 5G is not monolithic), and the way we will rely on this communication system raises potential security requirements sky high for 5G. Are all the networks able to meet these security requirements? Nobody is sure about that. So, it's not the right time for companies to feel fluffy and relaxed that somebody takes care of security – it should be each one's responsibility. This is not the time to relax and think that nothing needs to be done.

1.2 Best practices and guidance: are these enough, clear and practical ?

Previous generations of telecom networks provided practically no particular security requirements in the form of standards. Security measures were often described in a short section of protocol specifications or even just in the text of the call-flow descriptions. However, the 5G network deployment has not only made service and standardization necessary, but there is an additional need to consider the integration of virtualization elements, edge computing, front-haul, and back-haul network configurations.

Thus, there is an extensive list of available 3GPP and GSMA 5G security specifications, but a lack of mass deployment of 5G SA networks and a severe shortage of skill and expertise creates a hindrance. **This situation limits these specifications to an architectural or conceptual nature against real-life network threats and protection.**

33.310	Network Domain Security (NDS); Authentication Framework (AF)	SA3	Yes	2020-07-03	Yes
33.320	Security of Home Node B (HNB) / Home evolved Node B (HeNB)	SA3	Yes	2020-07-03	Yes
33.328	IP Multimedia Subsystem (IMS) media plane security	SA3	Yes	2020-07-03	Yes
33.401	3GPP System Architecture Evolution (SAE); Security architecture	SA3	Yes	2020-07-03	Yes
33.402	3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses	SA3	Yes	2020-07-03	Yes
33.434	Security aspects of Service Enabler Architecture Layer (SEAL) for verticals	SA3	Yes	2020-07-03	Yes
33.501	Security architecture and procedures for 5G System	SA3	Yes	2020-07-03	Yes
33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class	SA3	Yes	2020-07-03	Yes
33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)	SA3	Yes	2020-07-03	Yes
33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)	SA3	Yes	2020-07-03	Yes
33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class	SA3	Yes	2020-07-03	Yes
33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class	SA3	Yes	2020-07-03	Yes
33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class	SA3	Yes	2020-07-03	Yes
33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class	SA3	Yes	2020-07-03	Yes
33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class	SA3	Yes	2020-07-03	Yes
33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class	SA3	Yes	2020-07-03	Yes
33.536	Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services	SA3	Yes	2020-07-03	Yes
34.108	Common test environments for User Equipment (UE); Conformance testing	RAN5	Yes	2020-07-03	Yes
34.114	User Equipment (UE) / Mobile Station (MS) Over The Air (OTA) antenna performance; Conformance testing	RAN5	Yes	2020-07-03	Yes
34.131	Test Specification for C-language binding to (Universal) Subscriber Interface Module ((U)SIM) Application Programming Interface (API)	CT6	Yes	2020-07-03	Yes
34.229-1	Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification	RAN5	Yes	2020-07-03	Yes
34.229-2	Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) specification	RAN5	Yes	2020-07-03	Yes
34.229-3	Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP):	RAN5	Yes	2020-07-03	Yes

The GSMA also released a list of specifications:

FS.31 Baseline Security Controls

FS.34 Key Management for 4G and 5G inter-PLMN Security

FS.35 Security Algorithm Implementation Roadmap

FS.36 5G Interconnect Security

FS.39 5G Fraud Risks Guide

FS.40 5G Security Guide

1.3 Security still an after-thought

As the world pursues a more digitally connected future, we must focus more on cybersecurity. The greatly expanded and multi-dimensional nature of 5G networks makes them vulnerable to multiple threats (just read ENISA 5G thread scape, it is a horror story!). And when security is not included in the fabric of business development, it tends to become a patching-up and chasing exercise that is expensive and leads to much more damage and losses not just for customers but overall brand reputation and trust. It is, therefore, critical for network operators and organizations to understand and establish risk-informed cybersecurity investments upfront. **Network security must not be treated as an afterthought - the cost associated with missing a proactive 5G cybersecurity opportunity will be significantly larger than the cost of implementing cyber diligence upfront.**

TECHNICAL CHALLENGES

2.1 Threats and security deficiencies original to 5G that were not observed before

Not only are the 5G networks new for network owners and users, but a few security threats are also unique to the 5G ecosystem. Let's look at these security issues and challenges.

SBA protocols and vulnerabilities

5G networks are based on a Service Based Architecture (SBA) that allows interconnected Network Functions (NFs) to communicate with each other. This new set-up implies transitioning from the classical point-to-point messaging for the telecommunications world to the standard bus paradigm (service-based interfaces (SBIs). Traffic encryption (TLS) and the use of the protocol for authorization of network functions (OAuth2.0) are the leading measures to ensure the confidentiality, integrity, and availability of the 5G control plane. Although the support of these mechanisms is mandatory for telecom equipment vendors, mobile operators are in no hurry to implement authentication and authorization of network elements when deploying 5G networks. These results in associated challenges:

- Managing TLS keys and certificates are not trivial while deploying many network elements.
- During the implementation of monitoring tools (e.g. IDS) on SBI, the function of exchanging keys through closed channels for decrypting signal traffic needs proper management.
- Vulnerabilities within OAuth2.0 can potentially lead to DDoS attacks on the authorization service - NRF, which entails a complete denial of service of the entire operator's network.

HTTP/2 and exposure of APIs

In 5G networks, the interaction of all network elements takes place via the HTTP/2 protocol. While this helps simplify the implementation process and speeds up the overall development function. The description of services via open API attracts new players to develop the network elements and solutions. This competitive landscape created by multiple players does help reduce costs. But on the other hand, it also results in defective products due to new vendors' lack of telecom domain knowledge.

- More and more operators are moving to cloud-based deployments. This cloud-based setup helps reduce the standalone network implementation costs and enables operability and scalability. But some critical points need attention in this setup - UDR, where sensitive subscriber information (Ki, subscriber profile data) is stored, should be in a separate network security group from other network functions. This measure will help protect sensitive data from unauthorized access in the event of an outside attack on the network.

- The broad applicability of HTTP/2 in the world allows telecommunication equipment vendors to use it in developing a wide range of technologies supported everywhere by the world community. While this reduces the risk of incorrect operation in the final product and simplifies the process of introducing new features. It also opens pathways for potential attackers to develop tools for exploiting vulnerabilities.

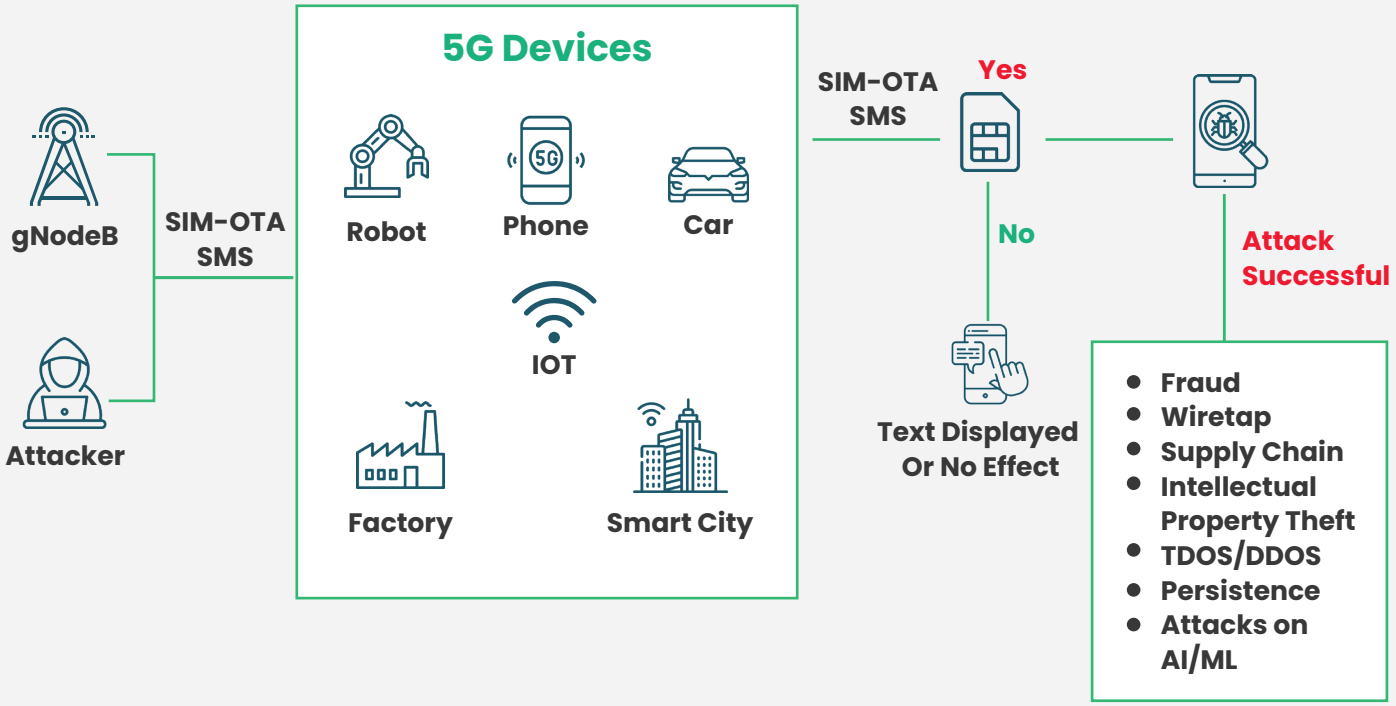
- The ability to connect third-party services to the fifth-generation network makes it more flexible and allows operators to introduce all kinds of services into their networks. Connecting these services directly to the operator's network also entails some security risks. A compromised network of even one of the partners can become a potential new attack vector for operator’s network.

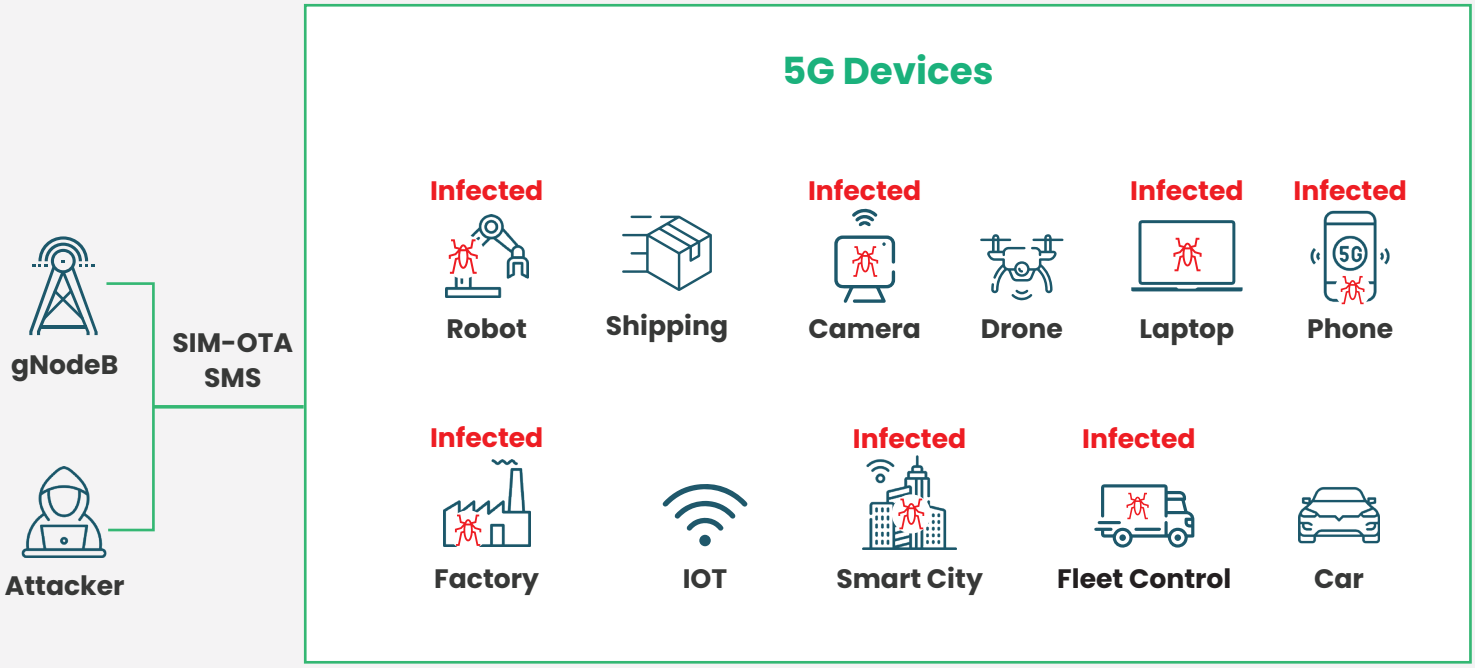
2.2 New and old threats brought to 5G by reused technologies and backward compatibility

5G networks focus on real-time data processing and act as a transport layer for different services using other technologies. Thus, the application layer is a legacy of other technologies. Additionally, the vulnerabilities of these technologies are not included in the 5G security aspect but are reused in 5G networks, which poses a challenge to network owners. One such shared aspect is the SIM cards and the associated vulnerabilities.

SIM management and STK vulnerabilities

- The most common attacks allow an attacker to steal information about the subscriber's location, their device identifier (IMEI) and cell tower (Cell ID), as well as force the phone to dial a number, send SMS, open a link in a browser, and even disable the SIM card.
- For more complex attacks, hackers can install their own SIM applets and change the settings of a compromised SIM card, thus taking a wait-and-see position in order to be ready to carry out a more complex attack at any given time.
- Many SIM cards store the current session key (Kc) in the SIM's shared memory, allowing STK applets to obtain such information in real-time and pass it on to an attacker. In the future, this information may let an attacker take control of the victim's connection.


5G Devices
gNodeB
Attacker
SIM-OTA SMS
Robot
Phone
Car
IOT
Factory
Smart City
SIM-OTA SMS
Yes
No
Text Displayed Or No Effect
Attack Successful
Fraud
Wiretap
Supply Chain
Intellectual Property Theft
TDOS/DDOS
Persistence
Attacks on AI/ML

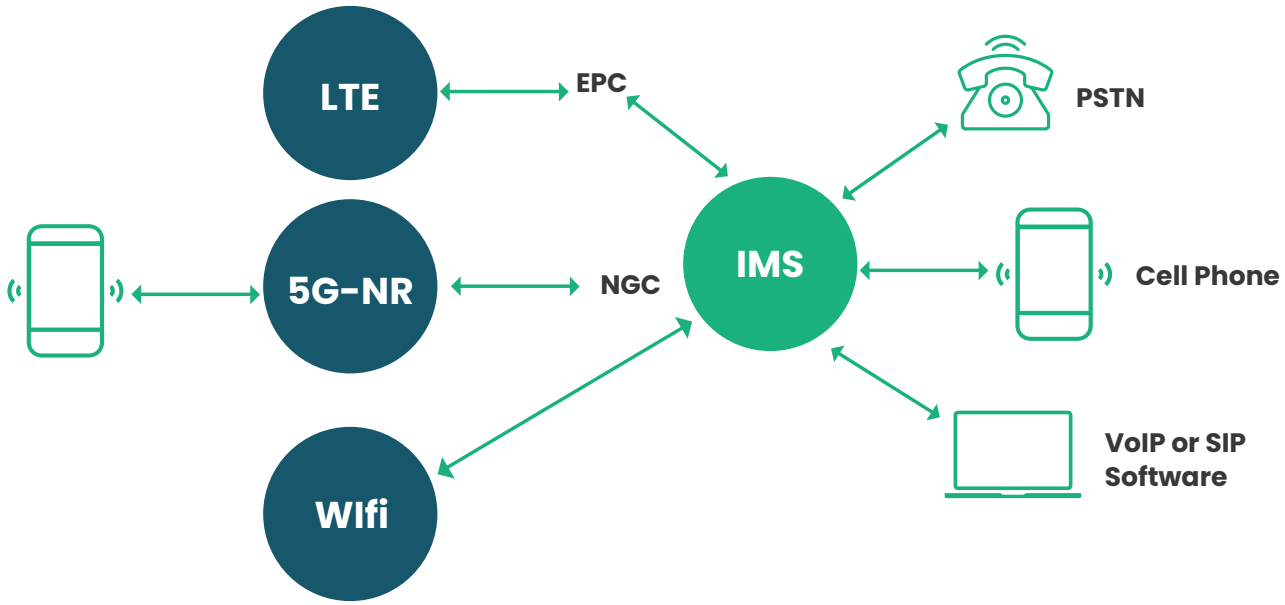

5G Devices
gNodeB
Attacker
SIM-OTA SMS
Infected
Robot
Shipping
Infected
Camera
Drone
Infected
Laptop
Infected
Phone
Infected
Factory
IOT
Infected
Smart City
Infected
Fleet Control
Car

5G networks do not have built-in security controls for SIM cards, enabling attackers to gradually establish their own rules inside the 5G domain, using captured SIM cards to steal funds, create authorised approvals, install malware, and conduct other illegal activities.

In the context of 5G networks, this vulnerability of SIM cards has become a serious problem, especially considering the increasing number of connected devices. Although the SIM alliance has developed new 5G SIM standards for increased security, some network operators continue to use "old" SIM cards in fifth-generation networks, which is a cause of concern while ensuring security.

Threats of IMS and VoNR

Another example of inherited vulnerability related to all Voice service – the origin of telephony.



5G networks will use Voice over New Radio (VoNR) – as part of their new architecture to offer significantly better sound quality and lower latency. VoLTE, VoWiFI and Vo5G are just technologies which describe the technical aspect of the connection between UE (user equipment) and IMS core. All IMS threats will also be present in any of these technologies. Below are common IMS threats.

- **Disclosure of the network data**
  Information about functional roles, vendors and models, software versions, and IP addresses. Also, it is possible to obtain information about the DNS names of some network nodes. With this data, an intruder can attack network elements and subscribers via network scans and eavesdropping on signalling traffic.

- **Disclosure of subscriber data**
  It was possible to obtain subscriber information such as IMEI (phone model or OS model), subscriber location, mobile device network status, subscriber account status, and list of enabled services via IMS procedures. With this information, any subscriber in the customer's network can get information of another subscriber via short call (without the answer).

- **Denial of Service (DoS)**
  Caused by attacks on individual subscribers or network elements. The consequences can range from reputational damage, subscriber churn and a negative impact on profitability.

- **Fraud**
  Can be committed by bypassing online charging systems, making calls and sending SMS at the expense of another subscriber, illegally activating services or disabling limitations set by the operator. These attacks initiated via call & IP address spoofing, call interception, supplementary services manipulation, and unauthorized use of operator resources might bring reputational and financial losses caused by unpaid calls and potential legal actions.

CONCLUSION

Firstly, the above examples do not cover the entire industry spectrum. Nor is it a summary of common trends. They are a quick compilation of challenges you may witness while deploying 5G networks. We faced similar obstacles and discussed workarounds with several global security teams spanning different network operators. Interestingly, we found that organisations worldwide struggle to find appropriate solutions and specific, actionable guidelines.

Every 5G network rollout will experience challenges, given that individual networks are unique. Would it be difficult to define cybersecurity best practices that are easy to follow and get satisfactory results? We believe it is possible and will try to address each potential challenge and share inputs on our learnings and experience of resolving them successfully. We hope this will be helpful to you and your organisation as you prepare to roll out 5G networks.

Stay Tuned!

In our next Edition, we will explain a few best practices and protocols to protect against these threat vectors within the 5G ecosystem.