5G Security

Risks and Mitigation Measures

White paper

Contents

Abbreviations

Acronym/Term	Definition
3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
AMF	Core Access and Mobility Management Function
AUSF	Authentication Server Function
B20	Business 20
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
GSMA	GSM Association
ICT	*Information and Communications Technologies*
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPS	Intrusion prevention system
ISO	International Organization for Standardization
ISO27K	ISO/IEC 27000-series comprises information security standards
ITU-T	International Telecommunication Union Telecommunication Standardization
MSME	Micro, Small and Medium Enterprises
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NRF	network repository function
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PNF	Physical Network Function
RAN	Radio Access Network
SBA	Service Based Architecture
SECAM	Security Assurance Methodology
SEPP	Security Edge Protection Proxy
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
VNF	Virtual Network Function
vRAN	Virtual RAN

1 Forewords

As we have embarked on our global journey in the Industry 4.0, connectivity has become more than just a component of this future, but a critical enabler. 5G is our latest enabling tool, with features like high bandwidth, low latency and high density; Digital services will transform society and the economy. IoT, autonomous cars, wearable tech and much more devices and sensors will flood our lives and even find its way into our bodies (medical tech). Cybersecurity has never been more important and critical to our lives in the physical sense as it is in the virtual.

Saudi Arabia is leading in the adoption of 5G technology with coverage planned for almost the entire Kingdom, paving the way to becoming one of the world's leading Digital Economies. stc's 5G deployments were carefully designed with security at the core, with the goal of enabling Saudi national digital transformation via secure infrastructure, without which, no digital economy can survive in today's cyber reality. We believe that enriching the industry with what we have learned is vital to the Cybersecurity knowledge library.

This white paper, authored by Saudi Telecom Company (stc) and Nokia is an attempt to raise security awareness in our industry for a service expected to have one of the highest global impacts in economy and society in history. Security by design and taking a security first policy in software development is a vital tool in our industry's arsenal.

Eng. Yasser N. Alswailem,

Vice President of Cybersecurity,

stc.

5G is more than a radio access technology. It is a new architecture with far greater agility in all domains. The capacity, latency, agility, reliability and speeds offered by this technology makes it applicable to Communication Service Providers and all Industry Verticals. The future vision for 5G and IoT is not just about connecting individual devices; it is an enabling technology in the 4th Industrial revolution that will deliver societal change.

5G will underpin several critical use cases, from industrial automation, through public safety service, to support for utilities or connected car. As such, 5G enabled governmental networks, utilities, transportation networks, healthcare and other services relying on 5G would form new Critical Infrastructure requiring special security scrutiny. Telecommunication network infrastructures and services need to ensure appropriate safeguards are in place to protect against attacks by malicious actors attempting to sabotage or manipulate the functioning of the network or parts of it, steal or otherwise compromise the data, or hold companies to ransom. 5G high level attack vectors include Denial of Service, exploiting backdoors, exploiting flaws in operational procedures and other attacks.

Active cooperation between involved stakeholders from the private and public sectors is vital at national, regional and international levels to implement resilient and secure digital infrastructure. The B20 (Business 20) Digitalization Task Force which took place in Saudi Arabia in 2020 as a one of the key engagement groups, is an excellent example of such cooperation. The Task Force was chaired by Eng. Nasser Sulaiman Al Nasser, Group CEO of stc (Saudi Telecom Company), and included several members such as Nokia and many others. Strategic policy recommendations were outlined to develop robust and resilient cyber strategies against cyber-attacks for individuals, MSMEs, businesses and governments by establishing principles of fostering an ecosystem of trust, promoting recommended minimum cybersecurity standards and providing incentives for businesses demonstrating cybersecurity readiness.

In this white paper, Nokia joined forces with stc to provide an overview of 5G security implications, and to demystify some of the common topics around the subject. We are very grateful to stc for the opportunity to collaborate on this important topic and to share together our respective views and expertise to the wider audience.

Khalid Hussain,

Country Senior Officer,

stc Business Group Head,

Nokia.

2 Changing network paradigm

The 5G network promises to be much more capable, flexible, but also more complex than its predecessors, likely using a heterogeneous architecture comprised of multiple access and infrastructure (physical and virtual) technologies.

Many traditional network elements of 4G are replaced in 5G by Virtual Network Functions and cloud architectures. 5G delivers whole network as a service, which is enabled by service-oriented architecture, Virtual Network Functions, cloud core and dynamic network orchestration/slicing. 5G interoperates with existing wireless technologies.

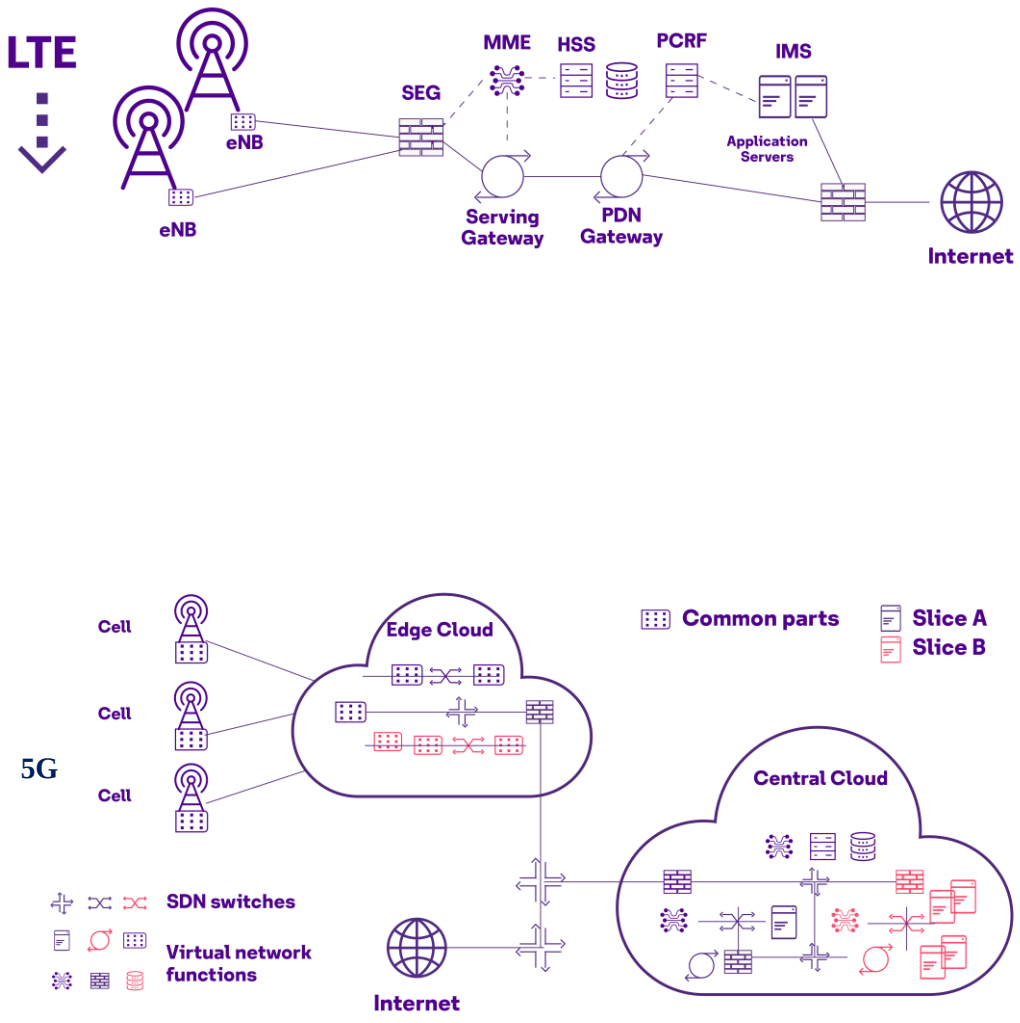

Figure 1. Evolution of the mobile network architecture

It is estimated that billions of devices will be connected to the 5G network over the coming years. Many of these devices will be low power sensors, wearables, and small devices used in industry. 5G increases wireless capacity by 1000 times, connects 7 Billion people & 7 Trillion IoT with zero perceived down time.

Realizing network as a service and the diversity of 5G use cases will make securing the network more complex. Availability, confidentiality and integrity of all user, management and control functions need to evolve to cater to: dynamic networks, multiple players involved in service delivery, wide variety of devices (including IoT), users, and applications. In particular, multiple logical networks, so called network slices, will be running on the shared 5G infrastructure. This complexity leads to a large attack surface. Moreover, the huge number of connected devices also means that the network may be exposed to massive attacks by such devices, if they become infected by malware and are abused by an attacker as a botnet for carrying out attacks such as distributed denial of service (DDoS) attacks. The Mirai Botnet attack gives just a preview of such attacks with the potential to cripple ICT infrastructures all over the world.[1]

With 5G, vulnerabilities in the network may have more serious consequences than was the case with previous telecom generations due to diversity of use cases. In Addition, the convergence of Telecom and IT infrastructures, services, and operations, require a holistic and broader look at 5G security than before.

2.1 Evolving understanding of Critical Infrastructure

When selecting criticality of telecom elements that should undergo special scrutiny, focus should be on critical infrastructure, defined as:

- Government networks and data centres.
- Infrastructure used by providers of basic products and services: energy, food, raw materials, railways, airports, telecoms, banks, internet exchanges, water utilities, hospitals.
- Infrastructure critical for high value enterprises or of key strategic importance for the nation's economy.

It must be understood that criticality of networks and specific networks elements should be evaluated based on (potentially disrupted) applications underpinned by those networks. Even a short failure in connectivity in a limited geographic area or an impact on latency requirements for a critical service could result in a deadly consequence (consider disruptions of connected car services). As such, undisrupted access to connectivity becomes as crucial as access to electricity.

3 What do we want to protect (ASSETS)?

3.1 Physical telecom infrastructure

5G networks will be cloud-based, i.e. their infrastructure consists of interconnected data centres, or "clouds". These provide a virtualization environment, where network functions are running as virtual network functions on a shared infrastructure that provides virtualized compute, networking and storage

[1] (https://en.wikipedia.org/wiki/Mirai_(malware)#Use_in_DDoS_attacks)

resources. There are different deployment options, but it can be assumed that a typical network will use some more central data centres and even more distributed data centres, possibly including “far edge” deployments that are widely spread throughout a covered geographical area.

The data centres will be interconnected by transport networks, consisting of the transport network nodes (e.g. optical switches) and the actual links (e.g. fibre networks). Transport networks will also provide interconnection between data centres belonging to different mobile networks, thus facilitating roaming and communication between subscribers of different networks. These so called “interconnection” or “IPX” networks may also comprise of mobile-network-specific functions above the mere transport layer, e.g. specific routing functions for the control plane traffic and similarly if applicable for the user plane traffic between different PLMNs. Additionally, there needs to exist established mutual agreements and security related policies between the different PLMNs and the IPX (entity) providers, for example, covering X.509 PKI solution for using TLS when securing the 5G inter-domain SBA control plane traffic between the IPX entities and the Security Edge Protection Proxy SEPPs in different PLMNs.

Mobile access (RAN) is composed of antennas, radio frequency and base band equipment. In 5G, the RAN can be realized in a variety of topologies, ranging from the “classical” distributed networks based on specific HW Physical Network Function (PNF), to virtualized architectures (vRAN/VNF) based on large numbers of Edge Cloud. The Edge Cloud will not be dedicated to the RAN but will also host part of the Core, mainly gateways, and applications to implement the low latency use cases that are supported with 5G. This is why the distinction between mobile access and core becomes ever more blurred.

While the devices using the network are typically not assets of the mobile network operators, they may still contain, according to 3GPP specifications, a secure hardware, commonly known as the “SIM card” but called UICC (Universal Integrated Circuit Card) in the specifications. The UICC is under control of the network operator and holds data and software called the USIM (Universal Subscriber Identity Module) application. The USIM application on the UICC is essential for secure communication between the device and the network and can be considered as part of the mobile network operators’ assets. For IoT devices the UICC might be embedded and only the USIM part of it under control of an operator.

A Summary of the list of 5G infrastructure assets are listed below. Classification of criticality is based on the geographical reach/number of subscribers affected in case of disruption. However, the actual risk level depends on the applications that could be compromised. Even small area disruption may have critical consequences (see chapter on critical infrastructure).

Table 1.Criticality classification of 5G infrastructure assets

5G function/network element	Classification	Comment
Data Centres	Critical	- Data centres host: Critical 5G network functions, sensitive network and user data and interfaces to other networks. - towards the edge (DC) the risk may decrease as the impact of successful attacks is regional.
Transport networks **(nodes and links, e.g. optical switches and fibres; SDN switches)**	High	- physically exposed, disruption of network operation possible, - threat of wiretapping can be mitigated by encryption, - redundancy can overcome attacks against single transport nodes and links
IPX entities	High	- similar to transport networks, traffic can be protected using the 3GPP specified mechanisms or those specified by other entities such as the GSMA.
Non-virtualized base stations	Medium	- Attacks have usually local impact, redundant coverage from other base stations possible, sensitive data protected in the base station's secure environment; however injection of a DoS attack into the core is also a risk
Antenna	Low	- Low impact; only localized DoS attacks
UICC/USIM	Low	- high hardware security, very local impact when hacking or cloning a USIM

3.2 Virtualization and Logical Network Layer of telecom networks

In data centres, virtualization software provides virtualized resources that are used to implement the logical network layer that consists of virtualized network functions. Considering the virtualization and logical layer allows a more fine-grained distinction of assets, which could form the basis of a fine-grained threat and risk analysis, where for example each 3GPP-specified network function is assessed, taking into account, its functionality, its interfaces and the data it accesses.

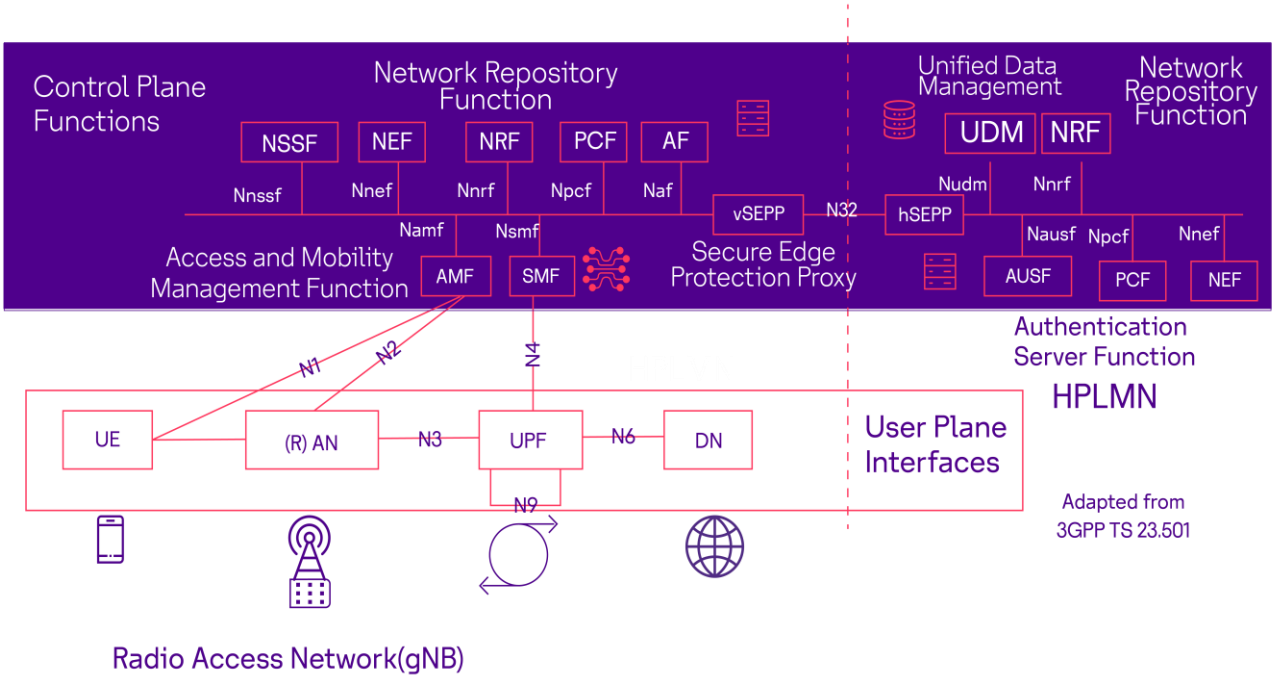

Figure 2. 3GPP 5G network architecture for inter-PLMN interworking (5G roaming)

The picture above shows the 5G network architecture for inter-PLMN interworking (5G roaming) as specified by 3GPP, highlighting the network functions that are critical for the 3GPP security architecture. The most critical of them may be those in the so-called home environment:

- The UDM (unified data management) provides access to the data held by the network, in particular, the subscription and policy data.
- The AUSF (authentication server function) has a central role in performing the authentication procedure between UE (User Equipment, i.e. mobile devices like smart phones or IoT devices) and the network.
- The NRF (network repository function) has a central role in enforcing the policies of how network functions communicate with each other, in particular inter-PLMN communication.

Other security-relevant functions include:

- The SEPP (secure edge protection proxy) protects the network at its edge (e.g. by hiding the internal topology to outside networks) and secures all inter-PLMN traffic.
- The AMF (access and mobility management function) maintains security associations to all UEs to secure the signalling between UEs and the core network.
- The gNB's (i.e. the 5G base stations) have a crucial role in protecting the radio interface. A single gNB may support a large number of radio cells, but clearly it has a much more local scope than the core functions.

Note that not all functions required in an operational network are specified by 3GPP. For example, the logical network layer may comprise DNS servers, DHCP servers, SDN controllers or virtual firewalls. Such functions are also of significant relevance for the secure operation of the network.

3.3 Network and Service Management Layer of telecoms

Management systems are a crucial asset of mobile networks. – The compromise of such systems can have a huge impact on the overall network. With control over the management systems, attackers with the appropriate privileges will be able to shut down the network or access all its sensitive data. Also, selective compromise of management systems can have huge impact. For example, being able to delete a system log file may allow an attacker to destroy evidence of its malicious activity. Management systems are somewhat less standardized than the 3GPP network functions. In addition to generic attacks against management systems, there can be a variety of individual attacks to individual mechanisms of management systems.

4 What do we want to protect against (THREATS)?

Note: These threats are not 5G-specific, but their severity may be particularly high in 5G networks, due to the fact the 5G networks are supposed to support a wider range of use cases including mission critical services.

- **Loss of availability** of the network or a communication service: This may be restricted to certain parts of the network (e.g. a set of radio cells, or a set of subscriptions, core network, RAN, management/control), but it may also impact the network as a whole. Loss of a mission critical service, that is expected to be run over 5G networks, can obviously have severe impact on the "real world" beyond the network. Even a localized loss of availability can be devastating, for example terroristic activities at critical locations such as a powerplant or an airport.
- **Leak of confidential information**: In a 5G network, leakage of confidential information in user plane traffic and any data stored in the network, in particular subscription data or tenant data (assuming a business model where tenants such as industry verticals can rent and operate network slices). An example of notable user-related confidential information available in the network is a user's geographical location. Depending on the sensitive information, loss of its confidentiality can obviously have various kinds of severe negative impacts.

  Loss of the integrity is often listed as the third of the high-level information security threats. On the one hand, compromising the integrity of the network can be used as a step towards the first two threats mentioned above. On the other hand, it may lead to undesired behaviour of the network that may have various impacts reaching outside the confines of the network itself. For example, loss of integrity of the network's authentication function may allow attackers to impersonate other service users, and abuse this to deliver wrong information to these service users' communication peers, potentially with huge negative impact. As another example, loss of integrity of charging and billing systems may lead to theft of service and the network operator losing revenue.

5 Why do we need to protect (RISKS)?

5.1 High level attack vectors

Note: These attack vectors are not 5G-specific. However, due to the huge variety of applications to be supported by the network, and the rich set of functions required, the attack surface of future 5G networks may become substantially larger with respect to these attacks.

- **Denial of Service (DoS) attacks by flooding the network** with requests (in the control plane) or simply with traffic (in the user plane) in a way that the network becomes partly or completely unavailable for regular users. A specific variant of this kind of DoS against mobile networks is radio interface jamming, i.e. making radio resources unavailable by transmitting noise. Flooding attacks may come in the flavour of distributed DoS attacks, where a huge number of sources may be orchestrated to generate the message floods. These sources could for example be the members of a botnet, e.g. a collection of devices infected with malware to the point that they can all be controlled by an attacker to execute the attack. Flooding attacks may affect all kinds of external interfaces the network provides, including the radio interface, interfaces to external networks like the Internet or other mobile networks.
- **Exploiting flaws in the design, implementation or configuration of the network**: It is assumed that such flaws cannot easily be completely avoided, in particular in the software implementing the network functions, and in the configuration of complex network elements. Design flaws may be much rarer, in particular in 3GPP-specified mobile networks, where specifications are created with a high amount of scrutiny. All external interfaces of the network may become subject to such attacks. In addition, flawed network configuration can lead to erroneously exposing network functions to external attacks, creating additional interfaces that may be attacked. Potential vulnerabilities may be also introduced by insufficient control over software design processes.
- **Creating and exploiting backdoors or malicious functions within networks**: Such functions may be inserted by “malicious insiders” into network elements at different parts of the supply chain. Sophisticated malware that operates stealthily may be very hard to detect.
- **Exploiting flaws in the operational procedures used for managing the network**: It is assumed that such flaws will always exist, due to humans involved in these procedures. In a broader sense, this attack category also is meant to cover attacks by malicious insiders in the network operation staff and others with knowledge of and access to the network.

6 How do we protect against threats (MITIGATION)

It is extremely important to be mindful of the cybersecurity risks and to take all appropriate steps to minimize such risks relying on standardized security features and additional solutions available on the market.

6.1 3GPP Security Architecture

5G networks complying with the 3GPP security architecture will provide multiple protection measures, including:

- authentication and authorization mechanisms between network and devices and between network elements of a single or different networks;
- cryptographic protection of traffic on the various network interfaces;
- temporary identities and concealed identities to hide the subscribers' permanent identities in the communication over the radio interface;
- secure environment inside the (physically exposed) base stations to ensure a secure boot and protect sensitive data.

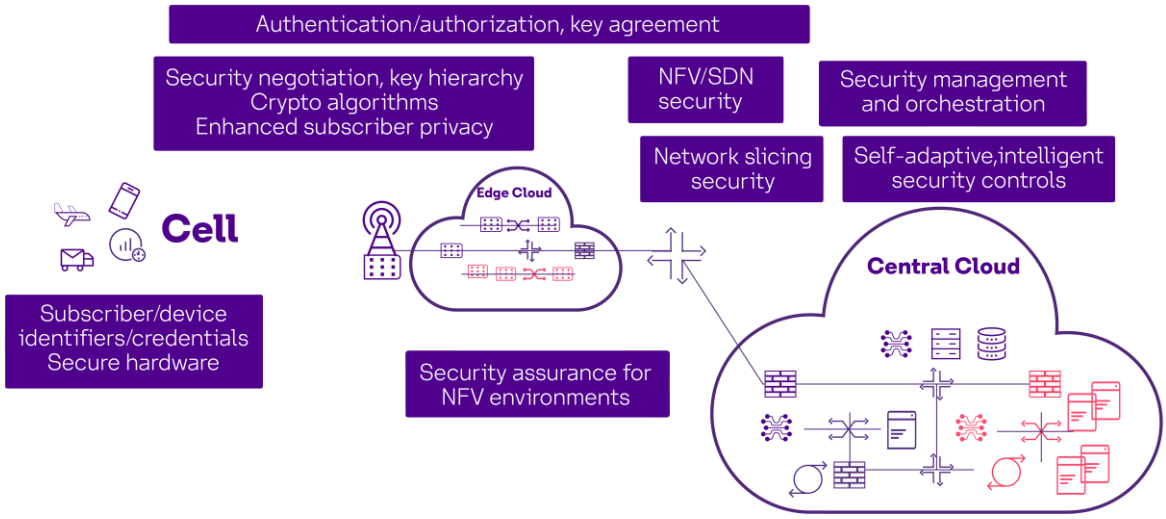

Figure 3. Security architecture

For 4G networks, 3GPP has also specified security assurance methods and security assurance specifications for various network elements that describe the steps that need to be taken during implementation to avoid vulnerabilities. For 5G, assurance specifications are still in the process of being specified.

Network elements are required to be compliant with the 3GPP security architecture and security features specified therein. More broadly and depending on the overall network architecture, a combination of different mitigation scenarios and frameworks are required as indicated in Figure 4 below.

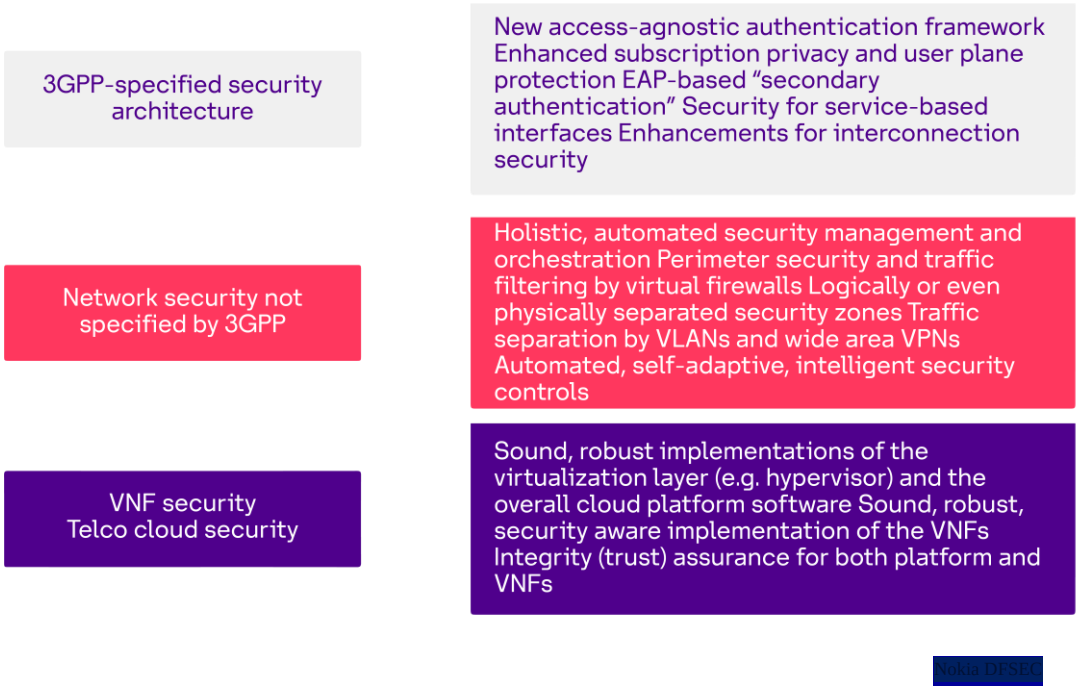

Figure 4. Network architecture implications

Most of the new security functions that are defined in the standards are 'mandatory to support, optional to use'. Vendors are required to implement mandatory 3GPP defined security features. However due to a variety of reasons (e.g. operator budget restrictions, different legislations in different countries, risk acceptance exercises) some network operators are not using or configuring the security functions available to them thus weakening network security. This can expose the network and its users to unnecessary risks. Operators should conduct a risk assessment justifying the adopted security decisions. Reporting of such decisions may also be part a regulatory requirement.

6.2 Other SDOs providing security measures for mobile networks

3GPP security architecture mandates the use of many security mechanisms specified by other SDOs, in particular the IETF, ITU-T or ETSI.

- The ETSI Industry Specification Group for Network Function Virtualization (ETSI ISG NFV) has its own security group, which has provided a number of technical reports and specifications that discuss the specific threats in virtualized environments and provide recommendations how to secure them properly.
- The ITU-T security specification group has addressed many SDN and cloud computing security aspects by a number of specifications.
- The ETSI ISG MEC (Multi-Access Edge Computing) addresses the specific challenges of edge clouds, including security aspects.

- The industrial representative organization for operators, GSMA, has guidelines for practical operational aspects of the network security and these include detailed guidelines for network security monitoring, interaction with partners, security filtering for messages and configurations.

All these specifications are of value and should be implemented in the 5G networks.

6.3 Network security not specified by 3GPP

Advanced attacks and pervasive threats to the 5G network will often rely on compromised credentials which have likely been acquired through a “spearfishing” attack or through malicious internal users the result of which can cause extreme damage and in case of 5G networks even endanger lives. Bad certificate authorities and insecure DNS have been problems for a long time, but with 5G, these flaws are about to become even more serious. For 5G operations the use of a multi-vendor system that provides single-sign-on, privileged identity management, user-behavior analytics and compliance-logging capabilities with the scalability, resiliency, and extensibility required in 5G networks should be table-stakes and can help, for example, in the detection of bad actors use of compromised credentials.

5G network elements are usually very complex to integrate and their security even more complex to maintain over time. Therefore, it is recommended to carry a continuous security audit and monitoring of the security configurations / security policies. 5G Security Management systems should also advise actions to improve security as well as to reduce the risk of network infrastructure attacks. Strong security operation systems shall also trigger possible risk mitigations via security playbooks that could be either manual steps and automatic workflows impacting the change in security configurations.

Secure orchestration and management of virtualization, general forms of security management (e.g. monitoring) are absolutely fundamental for 5G to operate robustly. Security automation is a key element in the operations of the 5G network supporting multitude of use cases and tenants, that increases significantly the complexity to be managed. Security automation combines automated holistic security orchestration and management with automated, intelligent security controls. The automated holistic security orchestration and management will be required to cope with the complexity of managing security efficiently and consistently throughout a network that spans multiple, possibly independent infra domains. The automated, intelligent security controls will be needed to detect and mitigate the yet unknown threats.

Security teams need a better way to not only gather the supporting information about the security state from a wider range of sources, but also to automate security processes. Security Operations, Analytics and Reporting (SOAR) can automate response workflow to gather and analyze security data from various sources and to make them available and consumable by different stakeholders. A platform that uses intelligent analytics, artificial intelligence and machine learning would continuously evaluate the risk posture and the state of the environment to enable informed decision making, formalize and automate responsive actions in real time. Such cognitive analytical and automated technologies measure rather than monitor to provide formalized workflows and enable informed remediation prioritization.

In the world of cyber security, Automation and predictive intelligent analysis will also play more and more a pivotal role in remediation. For instance, EUBA (Entity and User Behavior Analytics) is a statistical analysis which tries to study changes in regular patterns which may have the possibility of becoming a threat in the future. By monitoring different devices and tracking security events, this advanced system works by focusing on identifying and preventing suspicious behavior patterns.

In addition, special care is required for non-standardized security measures such as network perimeter protection, network zoning, traffic separation and secure network topologies, certificate management (e.g. Public Key Infrastructure), secure operations and maintenance, etc.

6.4 Technical assurance schemes and security life-cycle certification

Globally or at least regionally accepted certification schemes are preferred. This will promote innovation and reduce overhead. The GSMA NESAS (Network Equipment Security Assurance Scheme) is a promising scheme that has potential to become one such global certification scheme using 3GPP standards.

Cybersecurity is a combination of awareness, policies and procedures and technology. Developments in cybersecurity are evolving at such a speed that in order to deal with this dynamic environment a process-based approach to cybersecurity is essential. Many organizations have developed internal security by design programs. Externally, standards like ISO27K, NIST SP 800-160, TL9000 and NESAS Vendor Development and Product Lifecycle are developed to address secure development lifecycle process.

Advantages of product security life-cycle evaluation:

- Ensures that security is central to all stages of product design and development up to delivery.
- From a security point of view this approach facilitates faster remediation of security faults.

Operators and vendors of the mobile networks industry defined the Security Assurance Methodology (SECAM) in 3GPP standards organization. On this basis NESAS was developed within the GSMA. Some national cybersecurity authorities are involved in the process as well. NESAS is the most suitably global security assurance scheme, and adopting it brings benefits for

- Operators: reduced effort for tender with security by default and measurable security
- Vendors: uniform security requirements for network equipment and demonstration of commitment to secure product development and maintenance
- Governments: developed scheme, supported by the industry, introducing basic cybersecurity “hygiene”.

7 Summary

5G is one of the key enabling technologies for the future, and along with cloud, AI, and robotics it will make it possible to interconnect the physical, virtual and biological worlds. These are exciting times, and with this opportunity ahead of us, we must ensure we can keep pace (literally) and leverage the full benefits of the 5G.

Network paradigms are shifting, and the 5G network heterogeneous architecture will comprise of multiple access and infrastructure (physical and virtual) technologies that will require special attention from a cybersecurity perspective.

This paper is the fruit of a fruitful collaborative effort between the Saudi Telecom Company (STC) and Nokia, to provide a general overview of 5G security implications regarding the assets that need to be

protected, the threats and risks that we need to protect against, and most importantly, the most common mitigation steps to minimize those risks.

We believe regulators and policy makers wishing to improve cybersecurity of the 5G networks need to consider the following actions:

- Encouraging the use and appropriate configuration of the security functions specified by 3GPP.
- Encouraging implementation of additional solutions available on the market that improve the security of networks:
    - A continuous security audit and monitoring of the security configurations / security policies,
    - A multi-vendor system that provides single-sign-on with privileged identity management, user-behavior analytics and compliance-logging capabilities,
    - Automated holistic security orchestration and management combined with automated, intelligent security controls.

It is also of primary importance to Adopt a global security assurance scheme and avoid cumbersome and duplicated processes and procedures. for this purpose, it was explained how the Network Element Security Assurance Scheme (NESAS) is the most suitable scheme since it was developed within the GSMA on the basis of the mobile networks industry Security Assurance Methodology (SECAM) in 3GPP standards. It is understood however, that from a broader security approach, there are other bodies and organizations addressing cybersecurity frameworks that are not specific to 3GPP networks that can or may be of relevance in the future. These would require to be reviewed per market, per solution, and per product on a case per case to possibly include improvements they would introduce.

8 Additional references

1. Cybersecurity in the age of 5G technology. Reducing risk and complying with security frameworks and toolboxes, Nokia.
2. 5G security – a new approach to build digital trust, Nokia.
3. The triangle of trust: What security means to 5G operations, Nokia.
4. Use case: Cloud robotics. Building trust in the n the 5G industrial IoT ecosystem. Nokia.

9 Authors

Eng. Yasser N. Alswailem,

Vice President of Cybersecurity,

stc.

Dr. Mohsin S. Alhilal,

Cybersecurity GRC General Manager,

stc.

Eng. Alwaleed A. Alghothami,

Senior Cybersecurity Consultant,

stc.

Khalid Hussain,

Country Senior Officer,

stc Business Group Head, Nokia.

Dr. Brahim Ghribi,

Head of Middle East & Africa Government and Policy Affairs, Nokia.

Henrique Vale

Vice President of Middle East & Africa

Cloud & Network Services, Nokia.