NOKIA

Security challenges and opportunities for 5G mobile networks

White paper

Work on the next generation of mobile networks has gained momentum in the last two years. 5G networks will support a variety of use cases with challenging security requirements. This paper briefly summarizes the current status of 5G security and outlines the essential elements of the future 5G security architecture.

NOKIA

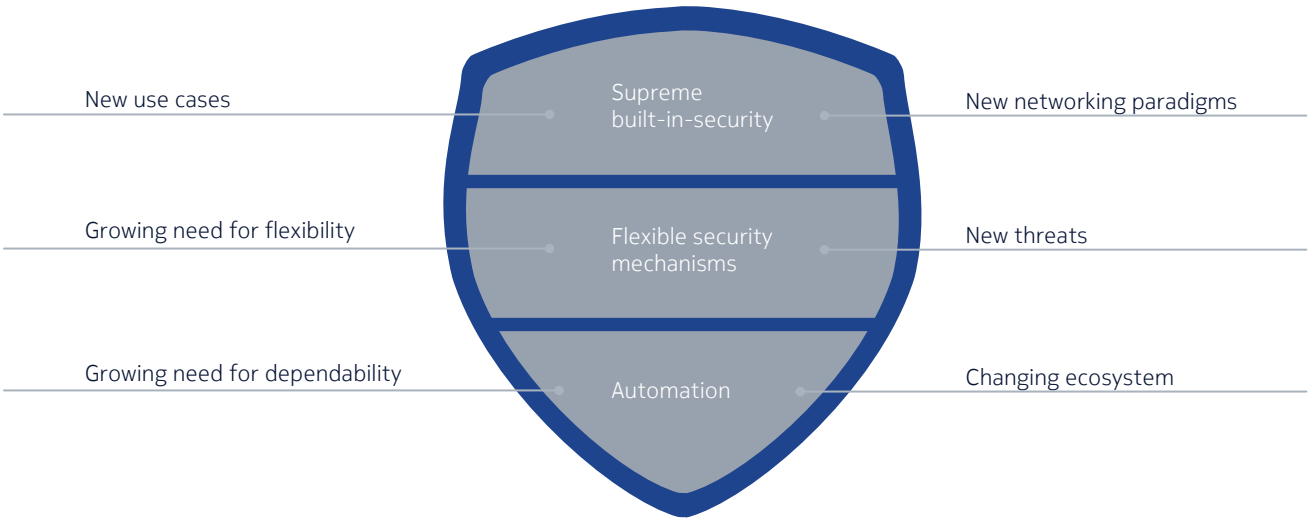
Contents

5G security drivers

Wireless communication is inherently vulnerable and needs specific protection against interception and tampering. Consequently, ever since GSM—the second generation of mobile networks—encryption has been used on the radio interface to secure the user communication. In the next two generations of mobile networks, UMTS and LTE, respectively, the security architecture was significantly enhanced. Besides encryption of user traffic, these networks have also provided mutual authentication between mobile terminals and the network, as well as integrity protection and encryption for all control and management traffic. Overall, UMTS and LTE security features ensure not only a high level of security and privacy for subscribers, but, very importantly, also assure the resilience required to combat various forms of attacks against the integrity and availability of the services these networks provide.

The LTE security concepts have not shown any major flaws since they were specified 10 years ago. This raises the question: Are new security concepts required for the next mobile network generation? The answer is yes. On the one hand, the support of a variety of new use cases and, on the other, the adoption of new networking paradigms have made it necessary to reconsider some current elements in the approach to security. Figure 1 visualizes the main drivers for 5G security.

Figure 1. 5G security drivers



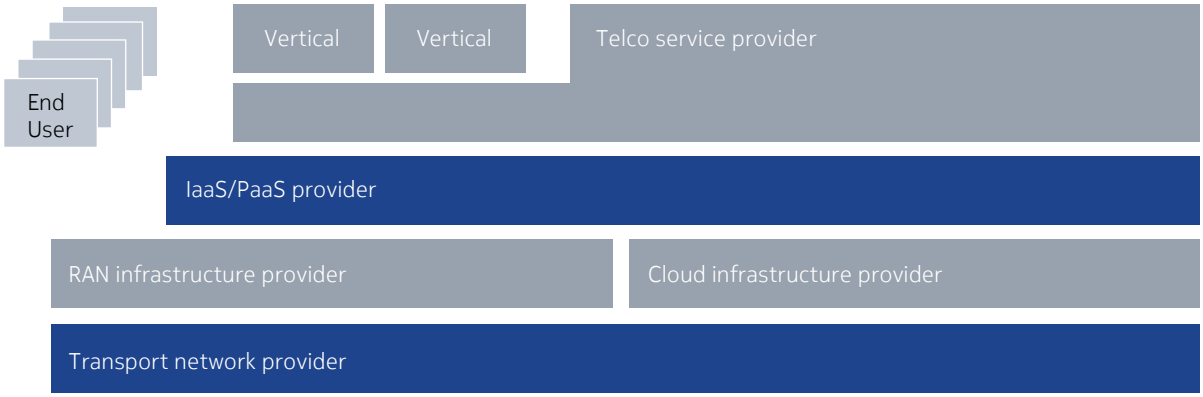
While LTE was designed primarily to support the mobile broadband use case (i.e., broadband access to the Internet), 5G targets a variety of additional use cases with a variety of specific requirements. These cases include support of an enormous density of mobile devices or the need for ultra-low latency in the user communication. Use cases, such as vehicular traffic control or industry control, place the highest demands on the dependability of the network. Indeed, human safety and even human lives depend on the availability and integrity of the network service.

To support each use case in an optimal way, security concepts will also need to be more flexible. For example, security mechanisms used for ultra-low latency, mission-critical applications may not be suitable in massive Internet of Things (IoT) deployments where mobile devices are inexpensive sensors that have a very limited energy budget and transmit data only occasionally.

To efficiently support the new levels of performance and flexibility required for 5G networks, it is understood that new networking paradigms must be adopted, such as Network Functions Virtualization (NFV) and Software Defined Networking (SDN). At the same time, though, these new techniques also bring new threats. For example, when applying NFV, the integrity of virtual network functions (VNFs) and the confidentiality of their data may depend to a larger degree on the isolation properties of a hypervisor. More generally, they will also depend on the whole cloud software stack. Vulnerabilities in such software components have surfaced in the past quite often. In fact, it remains a major challenge to provide a fully dependable, secure NFV environment. SDN, for its part, bears the threat that control applications may wreak havoc on a large scale by erroneously or maliciously interacting with a central network controller.

Another driver for 5G security is the changing ecosystem. LTE networks are dominated by large monolithic deployments—each controlled by a single network operator that owns the network infrastructure while also providing all network services. By contrast, 5G networks may see a number of specialized stakeholders providing end-user 5G network services, as illustrated in Figure 2.

Figure 2. Example of multiple stakeholders involved in providing end-user 5G network services



In particular, there may be dedicated infrastructure providers decoupled from telco service providers that host several service providers as tenants on a shared infrastructure. In another case, telco service providers may offer not only end-user communication services, but also provide complete virtual networks or "network slices" specialized for specific applications, (such as IoT applications). These may be operated by verticals. For example, a manufacturing company could run a virtual mobile network specialized for industry control applications for its own plants. The relevant security issue here is the building and maintenance of new trust relationships among all stakeholders. The aim would be to ensure a trusted and trouble-free interaction resulting in secure end-user services.

5G security requirements

When specifying a security concept, typically one of the first steps is to define the security requirements. This section does not offer a complete list of security requirements, but rather highlights some exemplary requirements and their sources.

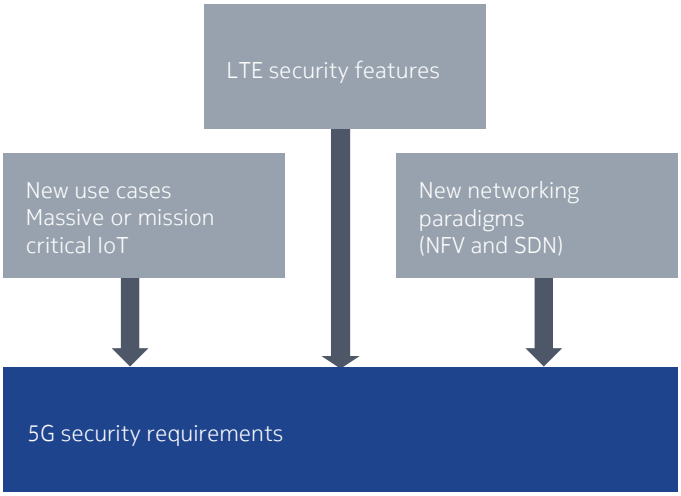
An early, major source of 5G requirements is the NGMN Alliance's 5G White Paper. This paper emphasizes the point that in 5G networks, the "enhanced performance is expected to be provided along with the capability to control a highly heterogeneous environment, and capability to, among others, ensure security and trust, identity, and privacy."[1] So, on the one hand, the security mechanisms need to comply with the overall 5G requirements, including extremely fast control plane procedures, extremely low user plane latency, and the highest degree of energy efficiency.

1 Next Generation Mobile Network Alliance, "5G White Paper", p. 9. Version 1.0, Feb 17, 2015. Available at https://www.ngmn.org/5g-white-paper/5g-white-paper.html.

On the other hand, the NGMN Alliance's 5G White Paper explicitly specifies a number of security improvements compared to today's networks, including the requirements to:

- "Improve resilience and availability of the network against signalling based threats"
- "Improve system robustness against smart jamming attacks of the radio signals and channels."[2]
- "Improve security of 5G small cell nodes".

Figure 3. Sources of 5G security requirements



Subsequent to these challenges, the NGMN Alliance has driven a working group on 5G security, which has delivered three dedicated documents (called "packages") with 5G security recommendations. These consider topics, such as potential security improvements of the access network, Denial-of-Service (DoS) protection, network slicing, mobile edge computing, low latency and consistent user experience.[3]

Clearly, the LTE security concepts are a starting point, as well as a benchmark for 5G security.[4] This is particularly true with respect to mobile broadband use cases, which will remain of major importance. Obviously 5G must be able to provide at least the same level of protection where needed, so LTE security features are a natural security baseline for 5G networks. On top of this, it is rewarding to revisit security features that have been discussed but were not adopted for LTE. This discussion is captured in 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System

2 Ibid, p. 33
3 These documents are available at https://www.ngmn.org/de/publications/technical.html.
4 For a comprehensive description, see D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi: "LTE Security," 2nd ed., Wiley, 2013.

Architecture Evolution (SAE)".[5] This document comprises features, such as International Mobile Subscriber Identity (IMSI) catching protection,[6] user plane integrity protection, or ensuring non-repudiation of service requests.[7]

More formally, the 3GPP[8] whose 5G or next-generation work is described in greater detail in the section on standardization below, has conducted a feasibility study titled "New Services and Markets Technology Enablers", referring to 5G or the "next generation". This study has produced potential security requirements that are documented in several technical reports and summarized in section 6.2 of 3GPP TR 22.861, "Feasibility Study on New Services and Markets Technology Enablers".[9] The 3GPP has also started work on a respective technical specification (i.e., a normative document).[10] These security considerations take into account future 5G features, such as network slices. The considerations require that network slices need to be isolated in order to confine any effects of a potential cyber-attack to a single network slice, or that individual slices need to conform to individual security requirements. The case of network slices owned by verticals is also considered, where the system is required to support network access authentication under the full control of the vertical. The system must assure full flexibility in the use of identifiers, credentials, and authentication methods. Other potential security requirements relate to:

- Protection against active IMSI catching
- Minimization of security-related signalling overhead
- Secure remote credential provisioning to devices
- Enhanced authentication and authorization mechanisms for various types of connectivity (e.g., connectivity without the presence of operator credentials in the device)
- Group authentication
- End-to-end user plane integrity protection, and many more.[11]

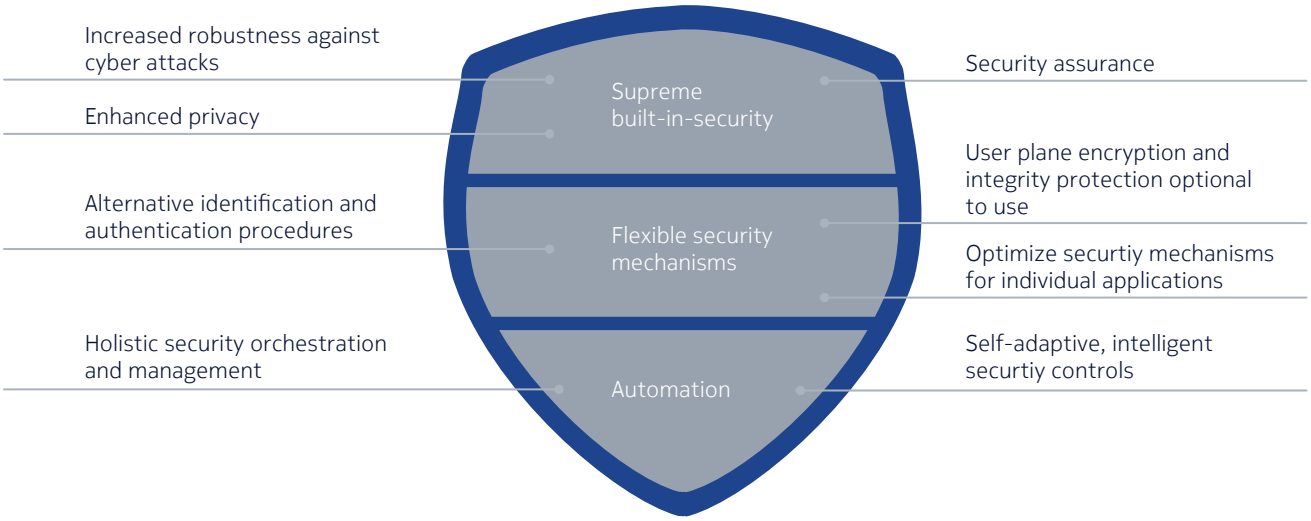
Although this overview on security requirements focuses solely on the NGMN Alliance and 3GPP as sources of requirements, it clearly shows that there is already a significant body of diverse and somewhat challenging 5G security requirements to help guide next steps towards the 5G security architecture.

5 http://www.3gpp.org/ftp/Specs/archive/33_series/33.821/33821-900.zip
6 "IMSI (International Mobile Subscriber Identity) catching" means tricking mobile devices into revealing the subscriber's identity by carrying out an active attack involving the use of a fake base station.
7 Non-repudiation of service requests means that users cannot reasonably deny that they made a service request. This is because it can be proven who made each service request, typically by use of digital signatures.
8 http://www.3gpp.org/
9 3GPP TR 22.861, "Feasibility Study on New Services and Markets Technology Enablers – Network Operation", Available at http://www.3gpp.org/DynaReport/22861.htm
10 3GPP TR 22.261, "Service requirements for next generation new services and markets", (work in progress). Available at http://www.3gpp.org/DynaReport/22261.htm
11 For more information, refer to 3GPP TR 22.861, "Feasibility Study on New Services and Markets Technology Enablers – Network Operation", Available at http://www.3gpp.org/DynaReport/22861.htm and 3GPP TR 22.261, "Service requirements for next generation new services and markets", (work in progress). Available at http://www.3gpp.org/DynaReport/22261.htm

High-level 5G security vision

Based on the high-level security requirements visible so far, this section discusses a high-level 5G security vision comprising supreme built-in security, flexible security mechanisms, and a high degree of security automation. Figure 4 illustrates this vision.

Figure 4. Basic elements of a high-level 5G security vision



Obviously 5G networks must support a very high level of security and privacy for their users (not restricted to humans) and their traffic. At the same time, networks must be highly resistant to all kinds of cyber-attacks. To address this two-fold challenge, security cannot be regarded as an add-on only; instead, security must be considered as part of the overall architecture and built into the architecture right from the start. Based on a secure architecture, secure network function implementations are also essential in order to ensure a high security network. Security assurance methods are therefore essential so that operators can ensure the required security level for different network functions.

5G security must be flexible. Instead of a one-size-fits-all approach, the security setup must optimally support each application. This entails the use of individual virtual networks or network slices for individual applications, as well as the adjustment of the security configuration per network slice. Security features subject to this flexibility may comprise the mechanisms for identifying and authenticating mobile devices and/or their subscriptions, or for determining the way that user traffic is protected. For example, some applications may rely on security mechanisms offered by the network. These applications may require not only encryption, as in LTE, but also user plane integrity protection. However, other applications may use end-to-end security

on the application layer. They may opt out of network-terminated, user-plane security because it does not provide additional security in this case (but rather increases the energy consumption of mobile devices).

Another key element of this vision is security automation, which combines automated holistic security orchestration and management with automated, intelligent security controls:

- 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 infrastructure domains, and that comprises a plethora of VNFs that may be allocated dynamically in these different domains. The holistic security management includes the task of specifying and distributing security policies to virtual and physical security functions and maintaining their consistency in a dynamic network setup.
- Automated, intelligent security controls will be needed to detect and mitigate the yet unknown threats – those that will try to exploit any weaknesses and flaws that may be found in spite of all efforts to rule them out. These kind of predictive security controls should act autonomously and have the capability to adapt themselves to cope with ever changing and evolving security threats.

5G security research

With Nokia being one of the main drivers, research on 5G security has gained a lot of momentum in the last two years. It is beyond the scope of this paper to give a comprehensive overview of this momentum but a few examples can be highlighted.

In 2015 and 2016, Nokia organized the 1st and 2nd IEEE International Workshop on 5G Security,[12,13] which received a lot of attention. The workshop solicited interesting papers, such as "Towards 5G Security",[14] on possible next steps towards 5G security in addition to making visible many 5G security research activities being conducted already.

Even more visible are the large international collaborative projects with the 5G PPP and the 5G Infrastructure Public Private Partnership,[15] which are taking a leading role to boost 5G research in Europe. A first wave of two-to-three year projects was kicked off in 2015, with more waves to follow. These projects

12,13 Ibid, p. 33
14 G.Horn, P.Schneider, "Towards 5G Security", Trustcom/BigDataSE/ISPA, 2015 IEEE, Volume 1, pp. 1165-1170. Available at https://www.bell-labs.com/newsroom/publications/294923/
15 https://5g-ppp.eu/
16 http://www.5gensure.eu/
17 An online article on the first face-to-face meeting of this group can be found here: http://www.5gensure.eu/news/5g-ppp-security-work-group-takeaways-1st-f2f-meeting

cover all aspects of future 5G networks with some of them covering specific aspects of security. One project, 5G-ENSURE,[16] is dedicated to security, and plans to deliver a 5G reference security architecture supported by an initial set of building blocks—so-called security enablers. This project has also initiated horizontal activity, the 5G PPP Security Working Group, where many 5G PPP projects meet to discuss 5G security questions and to develop a common view on 5G security.

Relevant in this context is the Nokia-led project 5G NORMA,[18] which will deliver a novel radio multiservice adaptive network architecture for the 5G era. This architecture takes the approach of creating a new architecture with security in mind from the very beginning. For this purpose, a dedicated security task in 5G NORMA analyses security threats associated with new concepts and procedures specified by the project, and sets up architectural guidelines in order to mitigate these risks.

Also, outside the 5G PPP framework, notable internationally funded and cooperative research on security is being carried out. One example is the Nokia coordinated EUREKA/Celtic-Plus project SENDATE (Secure Networking for a Data Centre Cloud in Europe).[19] SENDATE's goal is to pave the way to a new global network infrastructure topology. The topology will consider the needs of future services, as well as the convergence of telecommunication and IT networks backboned by securely connected, distributed data centers partly located at the network edge. These cloud data centers will be connected through enhanced transport networks and improved networking concepts, such as SDN. This will reinforce overall internet security with better control of data flows and new security concepts. Although not targeted at 5G explicitly, the future network security concepts developed in this project are also highly relevant for 5G mobile networks.

5G security standardization

The obvious standardization organization for 5G mobile networks is the 3GPP, which has already specified UMTS and LTE. As described, the 3GPP has specified a comprehensive set of potential requirements, including security requirements, for what it calls the "next generation system". In the context of 3GPP Release 14, studies are being carried out on all important aspects, particularly on the Radio Access Network (RAN) and Service and System Aspects (SA) specification groups. This work is in progress and is being captured in various technical reports.[20]

18 https://5gnorma.5g-ppp.eu/
19 http://www.sendate.eu/
20 For example, 3GPP TR 23.799, "Study on Architecture for Next Generation System", (work in progress). Available at http://www.3gpp.org/DynaReport/23799.htm

Security work in the 3GPP is carried out in the technical specification group SA3. In the group's latest meetings, numerous contributions on next generation security have been discussed. In its "Study on the security aspects of the next generation system,"[21] the SA3 has captured many so-called "key issues", grouped according to security areas, including architectural aspects, authentication, security context and key management, as well as subscriber privacy or network slicing security. Solutions proposed for a variety of key security issues have already been captured. Such solutions provide the input for the normative SA3 work to be started in 2017.

NFV will play a major role in 5G networks, and consequently, also the standards developed by the ETSI ISG NFV.[22] In this specification group, security issues are covered by a dedicated security group, which works on topics, such as Security Management and Monitoring for NFV, Certificate Management Guidance, Trust/-Attestation Technologies and Practices for Secure Deployment, Specifications for Execution of Sensitive NFV Components, and Maintenance/Multilayer Host Administration, to name a few. In addition, security specifications are being worked out that identify the essential threats for the management and orchestration (MANO) components, as well as for the reference points between them. The work of the security group will have an impact on the overall NFV architecture — for example, architectural enhancements are likely to be introduced for security management.

Besides the 3GPP and the ETSI ISG NFV, other organizations are expected to develop standards relevant for 5G. These include the Open Networking Foundation (ONF)[23] for software defined networking, or the Internet Engineering Task Force (IETF)[24] for multiple kinds of protocols. In general, standardization activities outside of the 3GPP will become more relevant for 5G than for previous mobile network generations. It is beyond the scope of this document to elaborate on this further.

Elements of a 5G security architecture

As the specification work for the overall 5G mobile network architecture is still in an early stage, a 5G security architecture can obviously not yet be given. However, a number of possible elements of this architecture can be anticipated, and are discussed in this section.

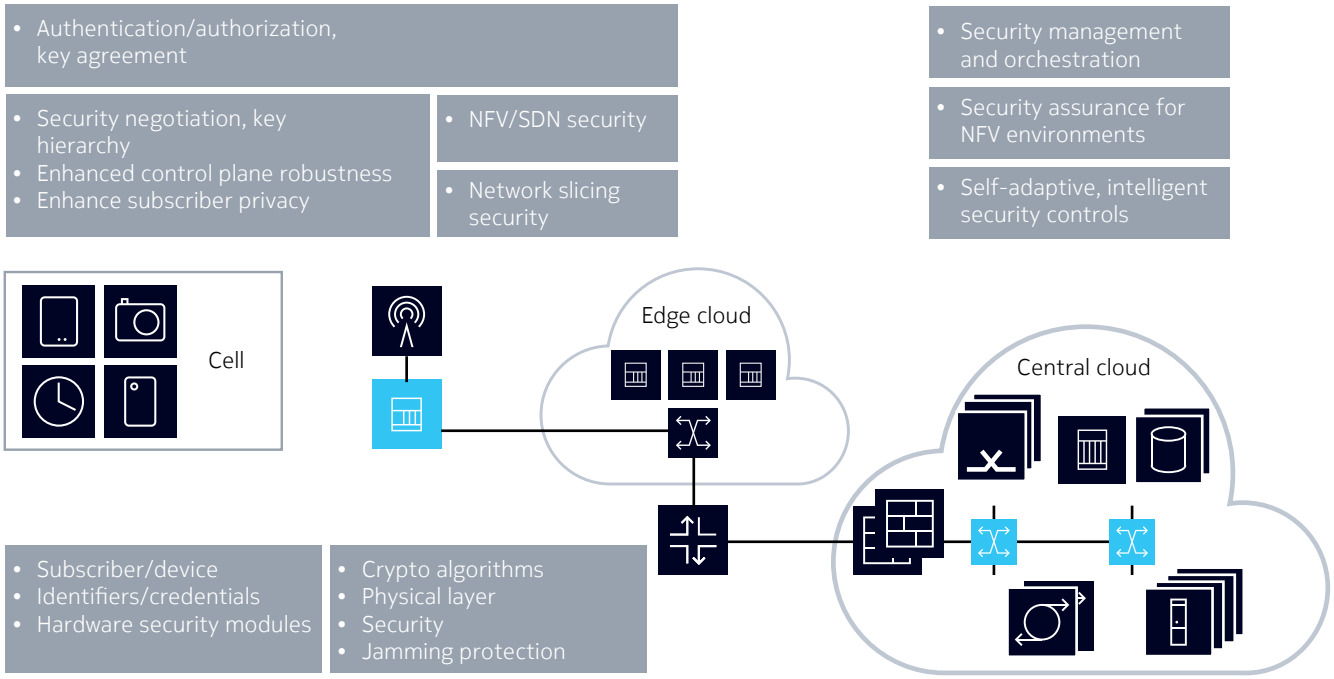
As a basis, a 5G mobile network architecture is assumed where most of the network functions run in cloud environments. These cloud environments are not restricted to central clouds, but will comprise a number of highly

21 3GPP TR33.899, "Study on the security aspects of the next generation system", (work in progress). Available at http://www.3gpp.org/DynaReport/33899.htm
22 http://www.etsi.org/technologies-clusters/technologies/nfv
23 https://www.opennetworking.org/
24 https://www.ietf.org/

distributed edge cloud deployments in order to facilitate mobile edge computing close to the mobile devices. Outside the clouds, "5G Access Points" will be deployed to provide radio coverage to mobile devices. It is assumed that only lower layer functions will be implemented in the 5G Access Points. Using LTE terminology, "lower layer" here means that the Packet Data Convergence Protocol (PDCP) layer that provides the radio interface security will no longer run in a "base station device," but in the edge cloud.

Figure 5 provides a schematic view of this architecture and depicts possible security architecture elements that are discussed below.

Figure 5. Elements of a 5G security architecture



Security between mobile devices and the network

The security features shown in the left-hand side of Figure 6 concern the interface between mobiles and the network. These features are therefore subject to standardization in 3GPP SA3. Some of these features might be contentious among different players in the telco industry. These features might include the types of identities (for subscriptions, devices, or even human users), the credentials that can be used, as well as the options available to store them on mobile devices. It appears that the current approach with the Universal Subscriber Identity Module (USIM) application on a Universal Integrated Circuit Card (UICC), commonly called a SIM card, will continue to play a major role, particularly for the mobile use case. In addition,

other mechanisms may be added to optimally support other use cases, such as massive IoT deployment. The authentication procedures are also under discussion. Currently the Extensible Authentication Protocol (EAP) is appearing as the main candidate because of the need to provide a unified authentication framework for various kinds of access networks, including those not specified by 3GPP.

To support more flexibility in the security setup, the security negotiation between the mobile device and network may need to be modified (compared to LTE). For example, this would allow a mobile device to opt out of network terminated user traffic security, as discussed already. More flexibility is also required with respect to crypto algorithms. While the algorithms used in LTE are still very sound and not endangered by known attacks, new algorithms may need to be added, particularly so-called lightweight crypto algorithms. These refer to algorithms that minimize energy consumption for crypto operations without sacrificing security. They are thus very important for massive IoT use cases.

We will likely see the same or similar backhaul security solutions in 5G as we now see in LTE, including IPSec tunnels that protect the data between the base stations and the core network. By tunneling all data on this link, the need is removed to set up individual security associations for different sessions. Using the established standards, network elements can be securely bootstrapped by means of operator-run Public Key Infrastructure (PKI), allowing them to reliably authenticate their link peers.

In contrast to user traffic, control traffic needs vital integrity protection. Encryption is also important here as a method to protect user privacy. In addition, means may be specified that protect the privacy of the user location even against active attacks (IMSI catching). Furthermore, the control plane protocols must be designed and implemented to anticipate all kinds of malicious behaviour from connected devices—even those that have been authenticated as legal network devices. Reliance on standard conformant behaviour of connected devices is not an option. That is because these devices, often without the owner's knowledge, can be corrupted by malware and attack the network. At its most dangerous, many corrupted devices may form a mobile botnet that carries out large-scale attacks against the network. Future networks will suffer due to a continuous increase of botnets, such as Mirai, which has recently been used to attack web services and network infrastructure. Network-based detection of suspicious device behaviour on Internet Protocol (IP), as well as application layer protocols, is therefore imperative as it protects not only subscribers and the data on their devices, but also the networks themselves.

In LTE, security on the radio interface relies on crypto protocols located on top of the Layer 2 protocol stack. It is an interesting field of research. For example, to what degree physical layer security mechanisms can enhance the security architecture is an important question. This might be done by providing additional security for communication on the lowest layers[25] whereas there is no cryptographic protection available in current mobile networks.

Security in the telco cloud

As most network functions are expected to run in NFV environments, NFV security mechanisms, as discussed in the Nokia white paper "Building Secure Telco Clouds",[26] will play a major role in the 5G mobile network security architecture.

In the context of network slicing, security mechanisms must ensure a strict isolation between different network slices running on shared infrastructures. This is necessary to prevent virtual machines in one slice from impacting those in other slices. It is also required to prevent information from leaking between slices on side channels (e.g., via physical memory sequentially used by different slices).

When network functions are no longer bound to specific hardware but may be instantiated on different hardware platforms, it might be harder to ensure their proper, secure operation. In this sense, NFV may have a significant impact on security assurance methods that will need to take this dynamic allocation of software functions to different hardware infrastructures into account.

Automated security

As discussed in the context of this security vision, automated holistic security orchestration and management will become crucial in large, cloud-based 5G mobile network deployments. End-to-end security needs will have to be managed through a central point of control. This allows the set up and maintenance of effective security mechanisms as the network is continuously adapting and dynamically reconfiguring for the best performance and user experience. For example, virtual machines providing VNFs need to be brought up in the right security zones of the virtualization environment—protected from each other by virtual and physical security appliances. Once set up, the network's security architecture needs to be automatically maintained as VNFs migrate from one infrastructure zone to another.

25 In LTE, for example, this communication comprises control messages on the MAC layer. By such messages, mobile devices inform the base station of the amount of data they want to transmit at a given time. Conversely, base stations inform mobile devices which radio resource blocks they must use to transmit the data.

26 "Building Secure Telco Clouds". Available at https://resources.nokia.com/asset/200289

Finally, in order to cope with unpredictable threats that try to exploit weaknesses that may be present despite the care involved in designing and implementing the network, smart security controls are required. Most network breaches, even those preparing for an eventual and very visible denial-of-service (DoS), aim to stay undetected for as long as possible. Attackers want to keep their activities under the radar of a network's security operation centre or aim to become part of the information noise caused by minor and relatively harmless attacks. Making use of the industry's continuously evolving analytics capabilities will help network operators to disclose such activities at an early stage, thus reducing greater harm. This can be achieved by correlating data from systems across the network, paired with automated workflows for triggering countermeasures.

Maintaining control of all operations activities is crucial in a world with an increasing number of stakeholders involved in providing end-to-end services to humans and things. In operations, the stakeholders are represented by human administrative personnel, and also increasingly by automated scripts. No matter whether operations are executed by humans or machines, service and infrastructure providers need to be able to enforce policy for all administrative actions. Should anything go wrong, any misconfiguration must be detected as soon as possible and the cause identified.

In future networks, interconnect between networks will become even more important than it is today. A significant number of cellular-connected things will actually consist of roaming subscribers in order to receive the best possible global network coverage. This will result not only in an increased amount of inter-network signalling, but also raise the economic value of the interconnect interface. While it is unlikely that the rather flat trust hierarchy in an international interconnect will change significantly, the number of stakeholders will increase. As a result, operators will need to closely monitor the user and control traffic entering their networks, and drop anything that could harm individual subscribers or the network. Last but not least, for business reasons every possible effort must be taken to ensure that the interconnect interfaces remain operational. Care must be taken that they are not overloaded by a Distributed Denial-of-Service (DDoS) attack or have to be purposively cut off in order to block an attack on crucial network equipment.

NOKIA

Conclusion

This paper has provided a high-level examination of the security threats associated with 5G networks. As observed by 3GPP today, 5G networks will require complex security requirements at different layers within the system. Moreover, with standardization at an early stage, innovative security solutions proportionate to the threats will have to be built into the network from the very start. This approach will protect subscribers, devices and their communications, as well as the integrity of the network itself—whatever the use case.

Investing in 5G security now is also a wise insurance policy to avoid unexpected costs that might arise later from countering attacks or from suffering the consequences of insufficiently protected high-value data. The wrong decision about security today will only prove to be false economy in the future.

Leadership in network security

Nokia technologies and expertise can help you protect your network and services. We have worked as a security system integrator for many years. Today, we are involved in more than 500 security projects worldwide, offering capabilities that range from design to support. We also lead the industry in securing commercial LTE networks. We leverage our work in security standards forums to design solutions that fully address the security requirements of complex networks.

Abbreviations

3GPP	Third Generation Partnership Project
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IOT	Internet of Things
LTE	Long-Term Evolution
MANO	Management & Orchestration
NFV	Network Functions Virtualization
ONF	Open Networking Foundation

PDCP	Packet Data Convergence Protocol
PKI	Public Key Infrastructure
RAN	Radio Access Network
SA	Service and System Aspects
SDN	Software Defined Networking
SENDATE	Secure Networking for a Data Centre Cloud in Europe
USIM	Universal Subscriber Identity Module
SIM	Subscriber Identity Module
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System

NOKIA

References

3GPP TR 22.261, “Service requirements for next generation new services and markets”, (work in progress). Available at http://www.3gpp.org/DynaReport/22261.htm

3GPP TR 22.861, “Feasibility Study on New Services and Markets Technology Enablers – Network Operation”. Available at http://www.3gpp.org/DynaReport/22861.htm

3GPP TR 23.799, “Study on Architecture for Next Generation System”, (work in progress). Available at http://www.3gpp.org/DynaReport/23799.htm

3GPP TR 33.821: “Rationale and track of security decisions in Long Term Evolved (LTE) RAN/ 3GPP System Architecture Evolution (SAE)”. Available at http://www.3gpp.org/ftp/Specs/archive/33_series/33.821/33821-900.zip

3GPP TR33.899, “Study on the security aspects of the next generation system”, (work in progress). Available at http://www.3gpp.org/DynaReport/33899.htm

D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi: “LTE Security”, 2nd ed., Wiley, 2013.

G. Horn, P. Schneider, “Towards 5G Security”, Trustcom/BigDataSE/ISPA, 2015 IEEE, Volume 1, pp. 1165-1170. Available at http://resources.alcatel-lucent.com/asset/200292

Next Generation Mobile Network Alliance, “5G White Paper”, Version 1.0, Feb 17, 2015. Available at https://www.ngmn.org/5g-white-paper/5g-white-paper.html

“Building Secure Telco Clouds”. Available at https://resources.nokia.com/asset/200289

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1612004464EN (February)