digitalpoland
Digital Poland Foundation

KIGEiT

A SHORT TALE OF SOCIETY 5.0
HOW TO LIVE AND FUNCTION IN THE TIMES OF INDUSTRY 4.0 AND 5G NETWORK

ATTACHMENT 3

SECURITY WITHIN 5G NETWORK ECOSYSTEM

The security of every telecommunications network - the 5G network is no exception - requires effective cooperation of operators, solution providers and market regulators. It also requires addressing the risks arising throughout the entire life cycle of the telecommunications network.

The operator's role in ensuring the security of the 5G network is crucial - the telecommunications operator is responsible for the security of the network and rendered services. The operator's role means in particular:

1. Determining the security requirements for 5G solution providers.
2. Designing network control mechanisms based on both solutions from 5G solution providers, as well as proprietary processes and third-party solutions.
3. Control of access to network devices and data sent over the 5G network.
4. Monitoring network security and handling incidents.
5. Ensuring the required quality parameters and business continuity.

The role of solution providers is to support network operators in ensuring its security, and above all:

– complete implementation of security mechanisms provided for in 3GPP standards in physical hardware and software solutions,
– product design taking into account best practices, standards and regulatory safety requirements,
– building products in a manner consistent with best practices - including software analysis in terms of security in a continuous process, at the product development stage, and supply chain security management,
– security verification of solutions in line with market requirements; including adequate certification, if required,
– implementation of solutions in the operator's network and transfer of the network to be maintained in accordance with security principles,
– handling vulnerabilities identified in products and providing security updates,
– in the case of providing support or monitoring services - compliance with the operator's security requirements, in particular care for data processing in accordance with the contract and the requirements of the law in force in our country.

The market regulator also has an extremely important role in ensuring the security of 5G networks in Poland. As the basic tasks of public administration it is worth pointing out:

1. Determining the security requirements that 5G networks built in Poland should meet

2. Defining the rules for verifying the security of networks and network devices, covering all market participants

3. Ensuring the operation of the security verification system and - if such a decision is made - applying an adequate certification program

1.1 THREATS RELATED TO SUPPLY CHAIN

The supply chain of all 5G network solution providers is vulnerable to the same threats associated with the international network of suppliers, and resulting from extraterritorial laws, policies implemented by non-EU countries, global trade wars and natural disasters that may disrupt supply continuity .

The level of risk present in the globalized supply chain of 5G equipment manufacturers requires special diligence in security management - telecommunications operators should require producers to comply with best practices, including certification according to relevant international standards (e.g. ISO28001).

1.2 5G NETWORK CYBERSECURITY

5G networks - thanks to the radically better technical parameters - carry the promise of opening to new applications, previously impossible to implement using earlier generations of mobile communication technologies. It is highly likely that the number of different applications of the 5G network will be significantly larger than for 3G and 4G networks - this also means that the number and variety of devices using the network will also increase significantly. These two factors result in increased "surface of attack" for 5G networks.

This effect was identified very early by 3GPP - which is why the 5G network security technical standards up to the R15 release contain significant improvements over the 4G network, addressing some key risks already at the standardization level. In addition, thanks to cooperation within the ecosystem of operators, solution providers and independent service providers, market solutions complementing the mechanisms provided in 5G technical standards appear relatively early.

It is worth highlighting four key improvements to security mechanisms compared to the fourth generation standard:

1. Unified authentication - compared to mechanisms specific to the 4G standard access technology.

2. Flexible network security policy, allowing adaptation to various network applications - in the absence of such flexibility in 4G networks.

3. Better protection of the user's privacy - by encrypting his identification number providing a higher level of security than the pseudo-anonymization mechanism used in the previous generation.

4. Introduction of an additional architecture element that allows filtering signalling messages and "hiding" the operator's network topology from the outside world - in 4G networks these functions were not required by standards.

These improvements already mean that the fifth generation standard provides the highest level of security among existing public mobile communication systems. Of course, the security mechanisms themselves provided for by 3GPP standards are not a sufficient response to the threats that may occur in 5G networks - that's why both operators and suppliers use solutions that go beyond the security provided by the standards.

It should also be emphasized that the provider of applications using 5G networks should not rely solely on network security mechanisms if they do not meet the requirements of its clients (e.g. they do not ensure end-to-end confidentiality). In this case, the application layer mechanisms should ensure the level of protection required by the service.

1.2.1 SENSITIVE FEATURES OF 5G NETWORK

The basic assumption adopted during the design of 5G security mechanisms was the division of network elements into trust domains, however, the further from the network core, the lower the trust level may be. This concept is explained in the diagram below - network functions such as UDM or ARPF require the highest level of trust, and gNB (presented in the form of DU / CU) is considered to be a much less sensitive element of network architecture. It is worth emphasizing at this point that due to the evolutionary approach to the implementation of 5G networks, elements of the fifth generation core network will not appear in our country earlier than in a few years - in the first phase of construction of 5G, operators will simply expand existing 4G networks with new transmitters compliant with the 5G standard (gNodeB). It also means that the threats related to the 5G core network discussed below are currently theoretical risk analysis.

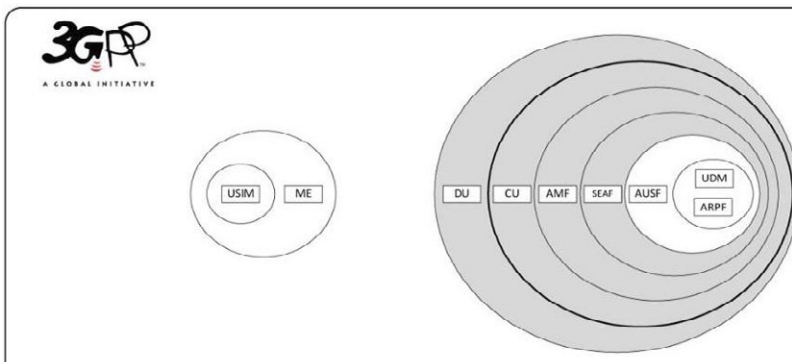


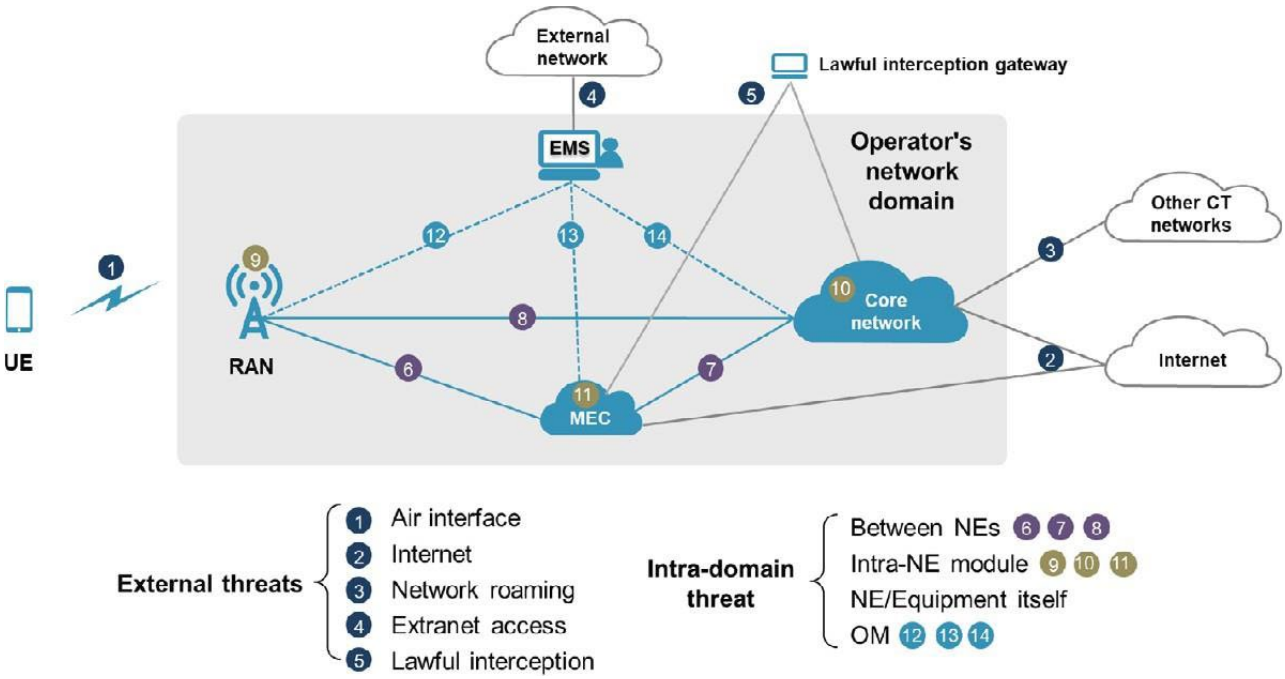
Figure 1 Trust model of non-roaming scenario

Both the architecture and the 5G business ecosystem contain elements important for security, and not included in the above trust model - for example, applications running in Multi-access Edge Computing (MEC) can be provided by partners or clients of operators, which requires operator for additional security analysis.

1.2.2 TECHNOLOGICAL THREATS

As a rule, the main technological threats to the security of the fifth generation networks do not differ from those already present in the 4G network and from threats known from other key applications for the implementation of 5G technology (virtualization, Software Defined Networking, micro services, etc.). It can be said with a high degree of probability that with the emergence of 5G networks in Poland, there will be no new, previously unknown types of cybersecurity threats. Moreover, contrary to information appearing in the public space, even technologies specific to the fifth generation Core network (Core) are already being used by Polish operators - for example, the network function virtualization (NFV) technology is already used in virtualized 4G core networks.

The diagram below presents the main categories of technical threats that may occur in 5G networks. Threat scenarios are in principle divided into two groups: related to 5G network interfaces with the outside world (extra-domain threats), and related to the internal 5G architecture itself, or its incorrect implementation (intra-domain threats).

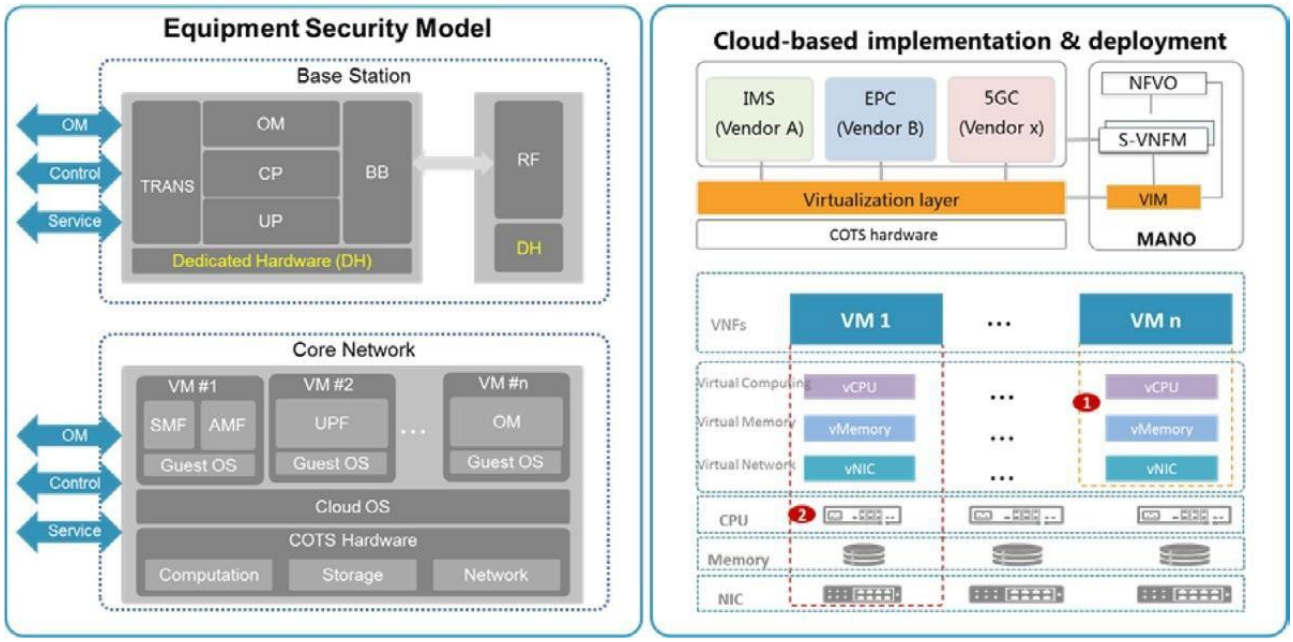


External threats to 5G networks are identical to those of previous generations - they are summarized in the table below. Security mechanisms introduced in 5G standards address external threats better than in 4G networks - which means that the level of associated risk is lower.

Threat scenario type	Main threat scenarios	Description
Extra-domain	Air Interface Threats related to the radio interface - wiretapping, DdoS attacks from IoT devices	5G security mechanisms better protect the privacy and user data transmitted in the radio interface - eavesdropping and obtaining metadata (e.g. location information) is significantly impeded. Risk mitigation mechanisms related to Denial of Service attacks from Internet of Things devices are not directly related to 5G, so they are not standardized - however, some 5G solution providers are introducing their own solutions in gNB to detect and limit redundant traffic.
	Internet Connection threats with packet networks, in particular the Internet	Threats of this kind are known and present in current mobile networks.
	Network roaming Connection threats with other operators' networks	Threats related to signalling attacks and threats related to user authentication in "visited" networks occur in every previous generation - the 5G standard introduces in this case additional security mechanisms that reduce the risk.
	External Access to EMS Threats related to access to the network management system	The threat consists in remote access to the network management system - if the operator provides such a possibility. Mitigation of this risk requires an appropriate infrastructure for remote access on the operator's side, authorization management and meeting the security standard of workstations accessing the management server. The above threat exists in functioning networks.
	Lawful Interception Security Threats Threats related to access to functionality authorized monitoring	The threat is related to unauthorized access to the authorized monitoring function, used under appropriate control by authorized state services. This type of threat exists and is also limited in current networks.

Threats within the network are associated with communication between network elements - implemented basically based on the IP protocol, technologies used to meet the functional requirements of the 5G network (e.g. NFV, SDN, SBA) or the location of individual elements (playing a role, e.g. in Multi-access Edge Computing).

The network core implemented in cloud computing technology can be based on a commercially available hardware platform (Commercial-Off-The-Shelf - COTS) or use a dedicated platform using specialized electronic systems (FPGA, ASIC). Both solutions have their advantages and disadvantages, in the case of COTS equipment, the risk associated with greater heterogeneity of the entire solution, including the probable use of open-source solutions should be taken into account.



It is worth noting that 5G, by introducing to the world of mobile telecommunications the threats typical of the Internet and IT environments in enterprises, also allows the use of best practices and proven organizational and technical security measures developed in the IT industry.

The following table summarizes the main categories of 5G threats that occur inside the network:

Threat scenario type	Main threat scenarios	Description
Intra-domain	Between NEs Threats located between network elements (including communication between micro services), threats between 5GC / MEC / gNodeB	– The 5G (5GC) core network introduces microservice-based architecture (SBA), which causes threats in the event of poor communication security between services – gNodeB and 5GC / MEC are located in other security domains (levels of trust) - threats relate to the transmission of signalling and user data between gNodeB and 5GC / MEC – There are threats to the clock interface: time server spoofing, clock information modification, GPS signal manipulation – Transmission threats - spoofing, eavesdropping, information modification, DoS attacks.

	Intra-NE module Threats occurring inside network elements and inside the MEC, threats related to cloud computing, threats of network layering (slicing)	– Mobile Edge Computing is not defined in 3GPP's Release 15 standards, but the use of this subsystem in the future is very likely. MEC locations will be closer to the edge of the network, so they will not be as well protected as central server rooms - in addition, these environments will include third-party applications. – Virtualization of network functions (NFV) is already used in 4G networks, but only in 5G will the core of the network be fully implemented in a private cloud. This means that all known threats related to cloud computing will also apply to 5G. – 5G introduces end-to-end network stratification, which causes threats in the event of insufficient separation between layers with different properties and made available to different recipients, and poor management of service access.
	NE/equipment Threats related to software, hardware and data processing	The types of threats related to software and hardware are identical to those in previous generation networks and in Enterprise class solutions.
	O&M Security Threats related to interface management	Insufficiently secured management interfaces can cause loss of control over the telecommunications network.

RECOMMENDATIONS REGARDING 5G NETWORK SECURITY

The practice of building secure 5G networks in Poland - and thus any regulations - should take into account the following principles:

1. Support for standards-based solutions (GSMA / 3GPP):

– From a security point of view, the 5G network uses a layered and domain-separated model in accordance with ISO 19249. According to this model, all stakeholders - application / service providers, end device suppliers, suppliers and network operators - should be responsible for secure the network in its own scope.
– Network security must be based on open standards defined by organizations such as 3GPP and IETF. An open approach should also be used during public-private cooperation to improve the security of Polish 5G networks, including risk analysis or defining security requirements.
– Network security standards in force in Poland should ensure that 5G networks are designed, built and maintained in a way that maximally makes their level of security independent of the choice of a specific supplier (s) of 5G network elements.

2. Independent verification /certification of 5G network solutions

– – Verification and certification of network equipment security is a key tool to ensure that solutions meet specific cybersecurity standards. Verification or certification should be carried out by independent

laboratories.
– An example of an approach that ensures cost-effectiveness and consistency of security requirements are the verification scheme defined by 3GPP and GSMA covering the security requirements for SCAS (Security Assurance Specification) network devices and the process accreditation scheme and NESAS (Network Equipment Security Assurance Scheme solutions)). Pilot tests have now been completed and NESAS is expected to be available later this year.
– SCAS requirements are defined by 3GPP for each network function (e.g. gNB) of the system. NESAS defines the process of testing and accreditation of processes related to the safe life cycle of 5G products - their design, development, testing and maintenance. This approach allows operators to obtain information not only about the security of hardware and software, but also about the supplier's competence in the field of change, configuration, updates and vulnerability management.
– NESAS and SCAS are prepared by organizations not associated with any of the suppliers, and the tests will be carried out by independent laboratories.
– Currently, according to the plan outlined by the Cybersecurity Act, work is underway in the European Union on certification schemes and programs, including also Common Criteria-based approaches. There are also analyzes verifying the possibility of adapting NESAS to the requirements of certification programs in accordance with the Cybersecurity Act.

3. Using best practices, also from outside the telecommunications industry.

– The Coordinated Vulnerability Disclosure (CVD) mechanism should be used to exchange information on identified vulnerabilities, verify them by suppliers, GSMA and 3GPP, and provide appropriate updates.
– Handling vulnerabilities and incidents requires the existence of specialized teams on the side of suppliers, affiliated with relevant industry organizations (e.g. FIRST). Requirements regarding the existence and competence of rapid response teams should be part of the expectations of operators of solution manufacturers.

digitalpoland
Digital Poland Foundation

KIGEiT
Polish Chamber
of Commerce for Electronics
and Telecommunications