SCTE CABLE-TEC EXPO FAST FORWARD 2021
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

5G Security & Protection Framework

Vasu Dalal
Director, Product Management
NOKIA
vasu.dalal@nokia.com

Patrick Nta
Chief Security Architect (Consulting)
NOKIA
patrick.nta@nokia.com

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

Table of Contents

List of Figures

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

List of Tables

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

1 Abstract

Cable companies offer multiple services – TV, broadband (cable, fiber, ethernet), voice, business services, home security and many others. And Cable companies now offer mobile service. They have purchased CBRS spectrum and are developing 5G service offerings for a Quad-Service play.

Mobile is an entirely new technology area for the industry and the service must be brought online in double-quick time to meet market demand, monetize CBRS spectrum purchases, and meet business commitments. At the same time, they must invest in the mobile network which is evolving to 5G. Operators must also be in position to offer these three (3) major 5G communications use cases: Ultra Reliable and Low Latency (URLLC), Massive Machine Type (mMTC), and Enhanced Mobile Broadband (eMBB).

5G is complex:

- New User Endpoints (UEs in 5G speak)
- New radios (CBRS), DOCSIS/PON backhaul and/or hybrid RAN (own & partner)
- An SDN/NFV-based Core, both centralized & distributed and/or hybrid Core
- Edge clouds and cloud-based environments (mix of bare-metal, VNF, & CNF deployments)
- A diverse network with a multitude of vendors & customers
- New, unique use cases including but not limited to Fixed Wireless Access (FWA), network "slicing", autonomous vehicles, IoT etc.
- Exposure to developer APIs (for even more app use cases) and many others
- Subscriber needs are changing, and new experiences are being created at a rapid pace

Security is critical in such a diverse, evolving, and complex 5G network while at the same time these services must be bought online faster to market with limited budgets and strained resources.

Traditional Enterprise-based security solutions will not be adequate based on the scope of the challenge, the size, diversity and scale of the network and the numerous new, unique & evolving use cases.

A 5G-based security solution requires not only adherence to traditional IT concepts of availability, integrity & confidentiality but also provide:

- A centralized, multi-vendor, end-to-end network control & management ("single pane of glass")
- Be adaptive, self-learning (AI/ML) with real-time threat updates
- Highly-scalable to support millions of diverse (UE & network) elements
- Customizable and automated (auto-discovery, audit & auto-remediation) to handle the volume of threats & scale and extent of the 5G network

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

2 5G: Key Security aspects

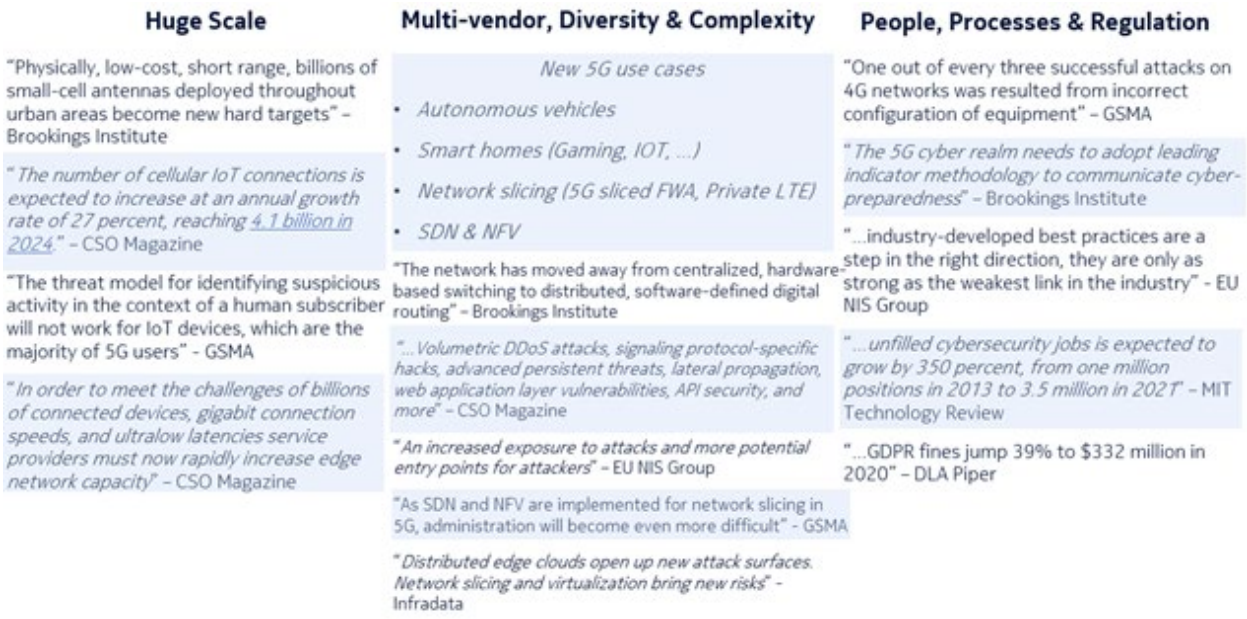

Figure 1 – 5G: Key security aspects

The key 5G security aspects can be summarized in three broad categories

1. Stringent requirements (latency, reliability & security) at high scale
2. Multi-vendor, Diversity & Complexity
3. People, Processes & Regulations

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

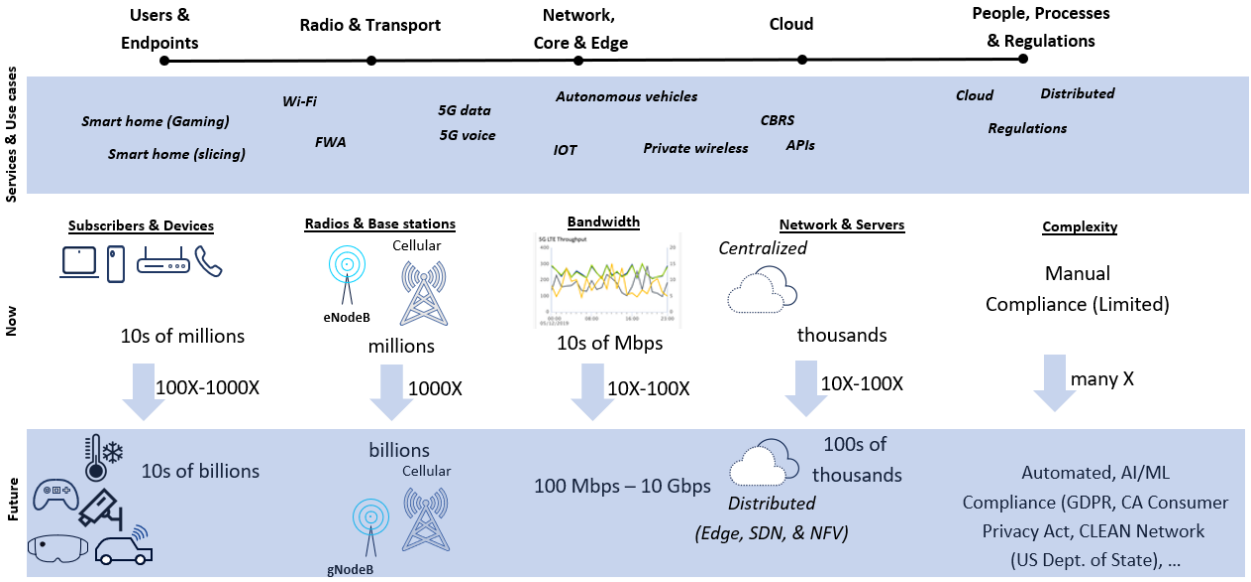

Figure 2 – Scale challenges at a glance

2.1 Stringent requirements (latency, reliability & security) at high scale

Table 1 - Speeds, Latency, Reliability requirements & Security implications

	Use-Case	DL	UL	Network Latency	Reliability	Cost Sensitivity	Security
Consumers	Mobile Broadband	100-300M	10-50M	15-25ms	Medium	Medium	Medium
	Fixed Wireless Access	1-5G	100-200M	1-20ms	High	High	Medium
	Event experience	1-100M	1-5G	1-5ms	Medium	Medium	Medium
	In-vehicle Infotainment	5-100M	1k-1M	1-20ms	Medium	Medium	Medium
Industries	Critical automation	1M	1-10M	1-5ms	Very high	Low	Very High
	Tele-operation	1M	1-10M	1-25ms	Very high	Low	Very-High
	Highly interactive AR	5-100M	1-100M	1-10ms	High	Medium	High
	Mass sensor arrays	1k-1M	1k-1M	200-500ms	Low	Very High	Medium-High

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

CBRS & 5G network requirements are in order(s) of magnitude higher in terms of # of UEs, # of radios, a software-based Edge, Core & Cloud network compared to prior networks (fixed or mobile). This compounded with the scale and new use cases leads to stringent security implications.

2.2 Multi-vendor, Diversity & Complexity

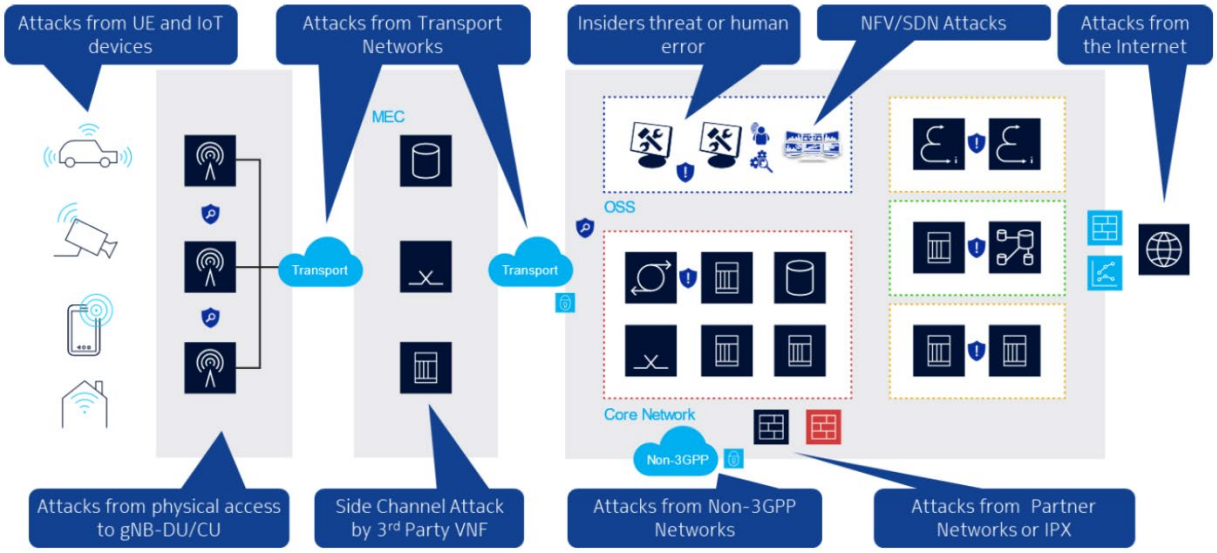

Figure 3 – Multi-vendor, diversity & complexity

Rather than having single monolithic providers controlling everything from the infrastructure up to the service layer, there are multiple stakeholders involved. The cloud, mixed edge/cloud and hybrid cloud environments have changed the notion of a perimeter. With 5G, there are many more players involved in the delivery of a service, with a much more diverse set of roles, and different understanding of risks.

Disaggregated network with lots of software solution components, new, & complex use cases (network "slicing", augmented reality, V2X, IoT & APIs).

Specific attack threat vectors for 5G networks include, but are not limited to:

- Users, Devices & Endpoints
  - Protection against eavesdropping, DOS, traffic injection, & rogue gNB attacks
  - Many times, attacks may occur without the owner of the device even being aware of it. It could be triggered by malware that has infected the device. Botnets are among the biggest threats. For example, large sets of infected devices that are controlled by an attacker and used to carry out large scale attacks, such as distributed denial of service attacks (DDoS). Such attacks can happen in 4G, too. But in 5G, we assume a different level of magnitude with higher speeds and larger device numbers. Many of them will be cheap and poorly managed IoT devices, which may easily become part of a botnet, possibly due to missing security patches, for example

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

- UE interaction is complex with DSDS-controlled handoff between CBRS <-> 5G (MNO) <-> 5G (MNO roaming)

- CBRS/5G Radio, Network and Transport
  - Network distribution & 5G services increasing the overall attack surface (DU, CU, (v)CMTS, OLT, IWF, MEC, Edge, Core, Cloud, IoT)
  - Transport technology is a mix of DOCSIS & PON backhaul for the CRBS radio sites where traffic will be backhauled over broadband (BB) networks to the Hub (or Headend). And the distributed user plane with IWF function at the interconnect point to the 5G Core network
  - Attacks may also derive from transport networks, as in 4G. Base stations are physically exposed, and therefore particularly endangered. That the base station may be split into a central unit (CU) and several distributed units (DU) is an infrastructure feature that is specific to 5G. In this case, it is mostly the DUs that will be physically exposed, but the network interconnecting CU and DUs is also at risk
- Edge, Cloud & Infrastructure Security

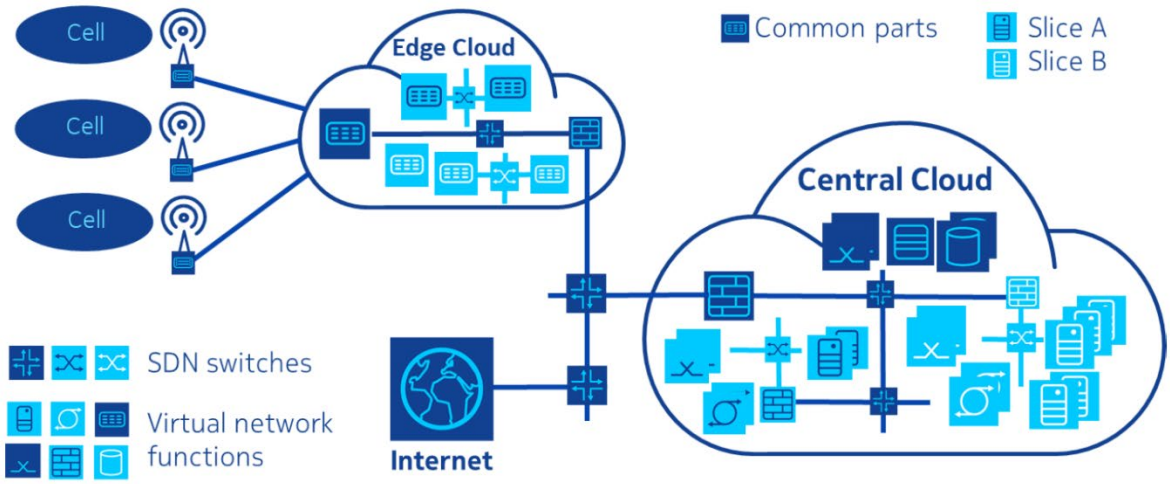

Figure 4 – Edge, cloud & infrastructure

  - 5G networks will adopt new networking paradigms. Network Function Virtualization (NFV) with both CNFs & VNFs and Software Defined Networking (SDN) will make networks much more dynamic. Cloud-centric networking is characterized by massive-scale, software-driven infrastructure and continuously shifting traffic flows, bandwidth demands, and network topologies. New attack vectors come up due to the use of Network Function Virtualization and Software Defined Networking. In particular, the sharing of infrastructure may allow so-called 'side channel attack'. When two different applications share common hardware, for example a CPU, there is always a risk that information may leak from one application to another. Other side channels may be opened by flaws in the virtualization layer. For example, a hypervisor may have a flaw that allows one virtual machine running on said hypervisor to access the memory of another virtual machine

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

running on the same hypervisor. Such side channel attacks have the potential to break the isolation between different applications or slices, and they can be very subtle and hard to detect.

If only trusted software under the control of one organization (e.g. the network operator) runs in a cloud, the risk of side channel attacks may be low. However, in 5G low-latency scenarios, third party software, such as AR/VR applications, may need to be deployed on the same edge computing infrastructure as the operator software. In this case, the side channel attack threat becomes a very real one.

- Scale
  - Discrete physical devices replaced by multiple VNFs & CNFs
  - Number of network entities under configuration management increasing dramatically
  - Expansion in the # of VNFs, CNFs & NEs requiring authenticated communications
  - Dramatic increase in volume of security information & alerts generated across the 5G network
  - Dramatic increase in the number & type of user accesses to the 5G virtualized infrastructure
  - Large increase in the amount & type of logs & data generated across the distributed network

- New, complex use cases (network “slicing”, IoT & APIs)
  - Given that more and more parts of the overall solution are accomplished in software and the "web speed" need for CI/CD, means even more attack vectors. Security must be designed in.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

2.3 People, Processes & Regulations

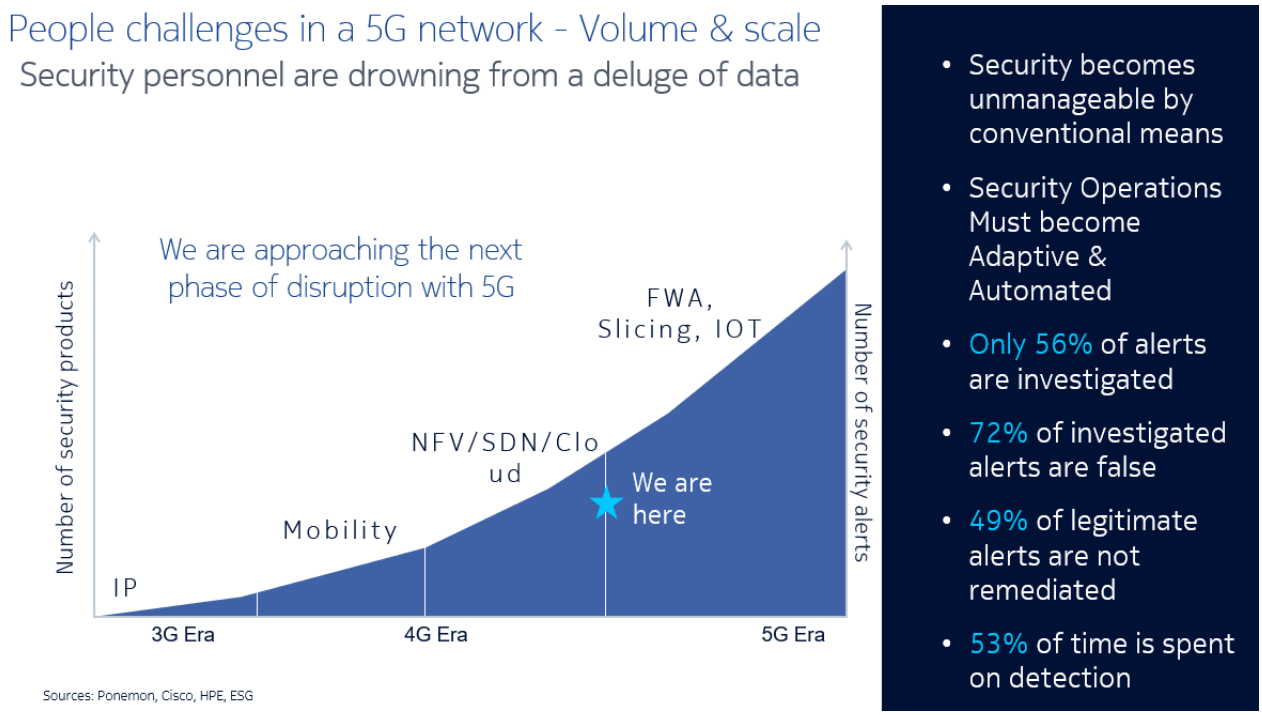

Figure 5 – People, processes & regulations

There is always the threat of security breaches by human errors or by malicious insiders. This is so in all networks, but considering mission critical 5G services, the impact of insider attacks may be even more devastating than in earlier mobile network generations.

- 65% of cyberattacks exploit configuration-related vulnerabilities
- 62% of causes of downtime are configuration errors (user error)

As the security threat landscape of mobile network is evolving very fast, it creates a lot of concerns on industries and governments and drives need to impose stricter security regulation on critical information infrastructures (CII) including mobile networks.

Many countries have passed cybersecurity or privacy laws which have important implications on the design, implementation, and operation of mobile networks. Examples include:

- EU issued a report on 5G risk assessment in Q3 2019 which identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities, and strategic risks Mitigating measures will be announced end 2019 to address the identified cybersecurity risks at national and union level
- General Data Protection Regulation (GDPR) in EU is passed in April 2016 and implemented in May 2018. GDPR has global significance as it governs not only EU companies but also all companies that process EU resident's data

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

- In France, law has been issued in August 2019 to preserve the interests of defense and national security in connection with the operation of mobile radio networks (5G and further) It modifies the Posts and Electronic Communications Code to introduce an authorization request for the operation of radio network equipment (BTS and core).
- China Internet Security Law enacted in November 2016 and in force in June 2017.
- Canada's Personal Information and Electronic Documents Act (PIPEDA)
- In USA, if government project is involved, contractors need to comply with Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) requirement FIPS 200 and SP 800-53
- California Consumer Privacy Act (CCPA)
- Clean Network (US Department of State) and many others

Finally, there is a geo-political and nationalistic aspect to 5G, and supply-chain provenance must be evaluated in depth.

Before 5G, mobile network was primarily focusing on voice and internet services. Moving toward 5G, mobile network operators will unavoidably get into other business segments such as banking, energy, healthcare, public safety or even military. Network operators must be ready to comply with all industry specific and government regulatory security requirements.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3 5G Security Framework

3.1 Vision

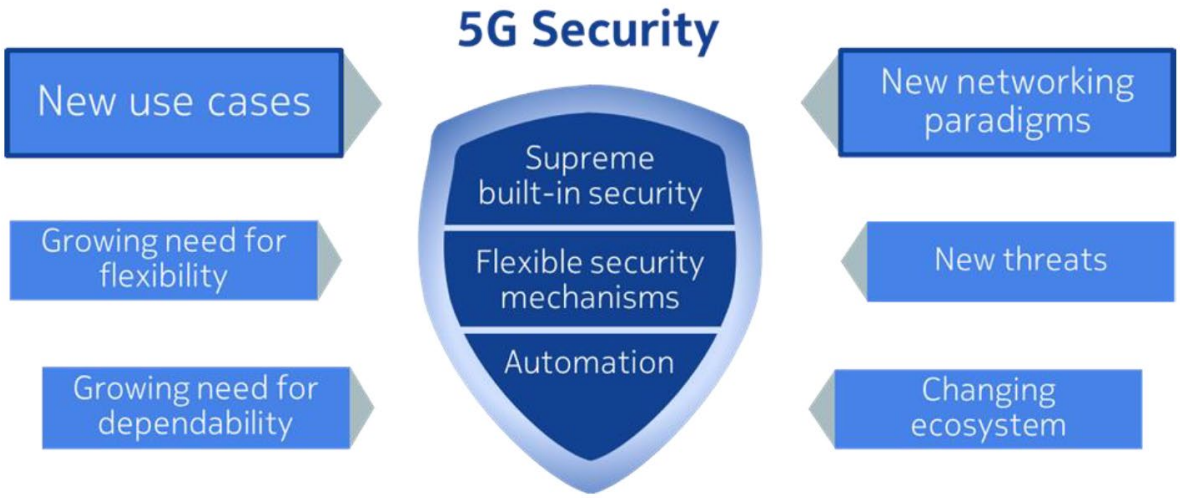

Figure 6 – 5G Security framework

Mobile networks are moving into a post-perimeter world where the network boundaries have disappeared, and the difference between insiders and outsiders has been eradicated. Given this situation there is pressing need to gain total visibility and intelligence on what is happening within service provider infrastructures, services, applications, data and people, to detect security breaches and respond to them.

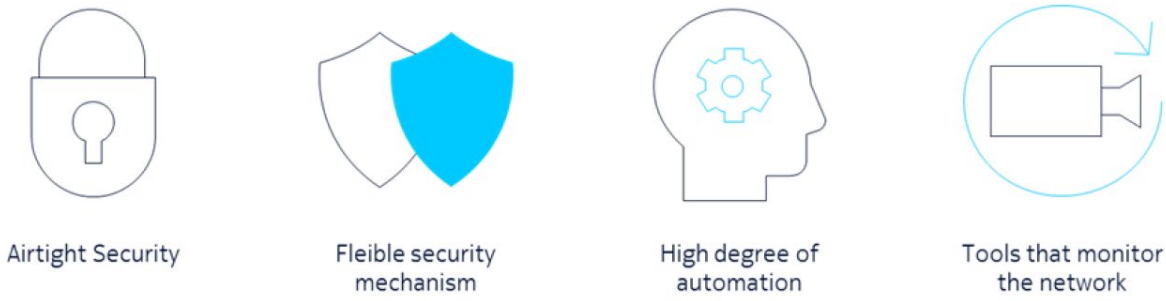

Figure 7 – 5G Security vision

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

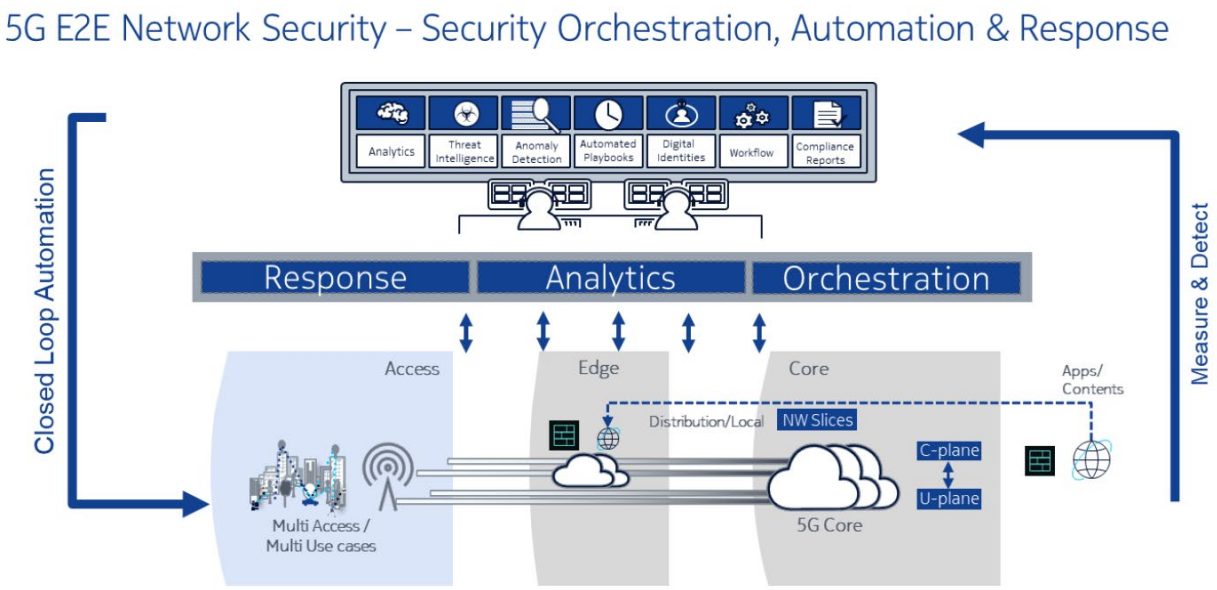

Figure 8 - SOAR

A Security Orchestration, Automation & Response (SOAR) strategy provides a centralized security command-and-control structure to protect the network from the most advanced persistent attack with the fusion of threat intelligence, analytics, machine learning & automated response.

Security must limit attack vectors, detect all threats when they do occur and respond faster to eliminate time between detection and mitigation.

Some of the key themes include:

- Constantly measure your security posture and risk levels. This is more than compliance auditing, but rather an ongoing near real time assessment of your network security posture. To do this effectively requires automated software security systems
- Control and limit access to key operational systems and assets. In addition to perimeter security defenses, this includes access governance and management
- Detecting threats earlier in the kill chain requires an ability to perform multi-dimensional analytics across a variety of systems and resources in order to identify threats that may be otherwise missed. The goal is to identify anomalies from normal behavior, and this is where data analytics and machine learning (ML) for security are emerging. Analytics and machine learning (ML) are needed to spot indicators of compromise, proactively identify harmful actors, help security analysts prioritize risk and initiates the appropriate rapid response

Rapid response is key to minimize the impact of cyber-attacks. The time between detection and mitigation needs to be eliminated. One of the big challenges security teams face is the inability to keep pace with the diversity and velocity of threats.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

Combined with a global cyber skillset shortage, traditional incident response strategies rely on too many manual processes performed by limited security expert resources. This is where security process automation or orchestration plays a key role.

Adaptive security is about transforming security operations to be predictive & automated by using machine learning and multi-dimensional analytics and threat intelligence in order to drive rapid, automated, and predictive responses to threats.

3.2 Security Orchestration Analytics and Response (SOAR)

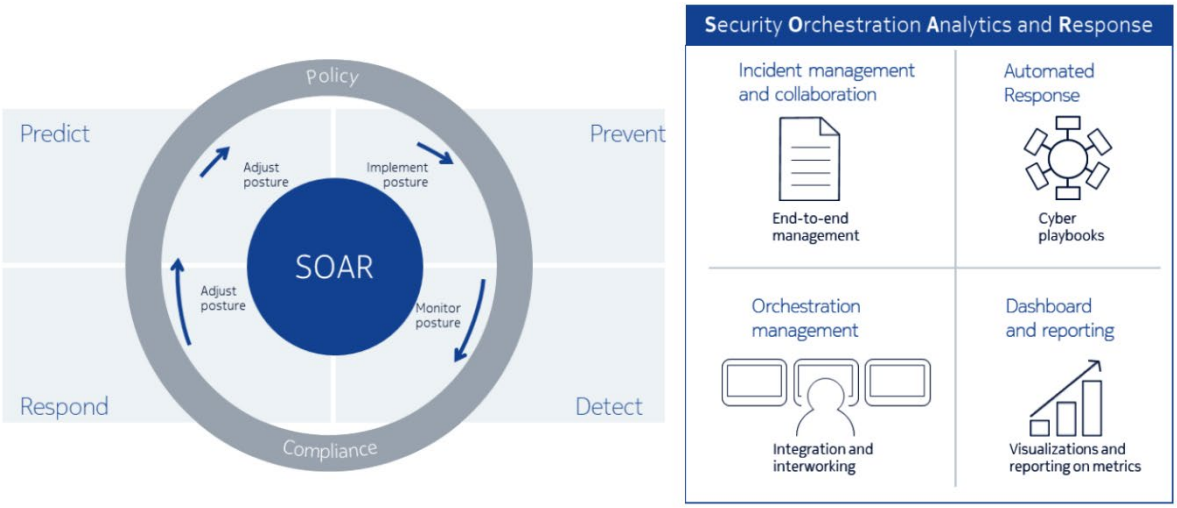

Figure 9 – SOAR in action

An "optimized" state cannot be achieved using conventional approaches to security operations. The priority for any digital strategy is to build an adaptive security architecture that automates security driven by intelligence and analytics.

These are the basic principles of Security Orchestration, Analytics and Response (SOAR): using security analytics in order to drive an orchestrated automated response.

SOAR systems aggregate, correlate, and analyze data from disparate point tools into cohesive and enriched security intelligence with business-specific context.

By analyzing user behavior to identify bad actors and providing threat indicators to potential insider threats. These capabilities help security professionals prioritize risks and automate security operations activities in the context of the attack surface and business and improves alert management by correlating and consolidating alerts from existing systems.

Security operations workflow automation and orchestration are at the heart of the transition from static defense to agile and adaptive response. Security automation involves more than just operations; it must be aware of and encode business processes, regulations, and customer-specific policies. Automation is the

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

process executing repeatable actions without human intervention while orchestration is the concept chaining these automated tasks into executed playbooks to perform workflows to accelerate both investigation and mitigation.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.3 5G Security Architecture

3.3.1 Defense in Depth

Below is how the 5G architecture is depicted by 3GPP in its Technical Specification TS 23.501.

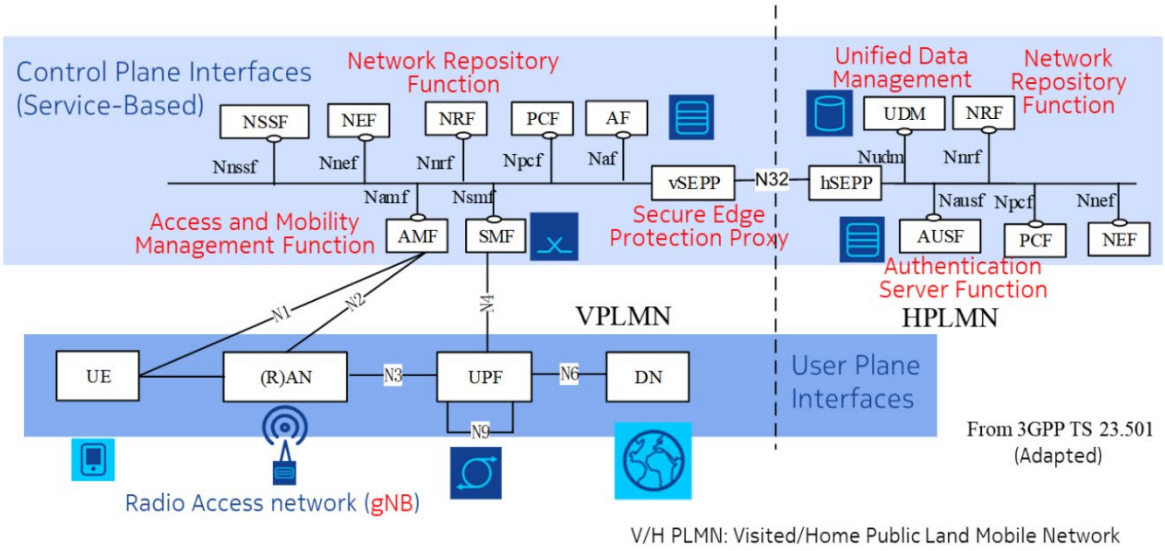

Figure 10 – 3GPP specifications

The basic concept of 5G Mobile Network Security is known as “Defense in Depth”. This describes multiple layers of overlapping security measures protecting the valuable assets, preventing from potential attack, and causing impact to the important asset of the network.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

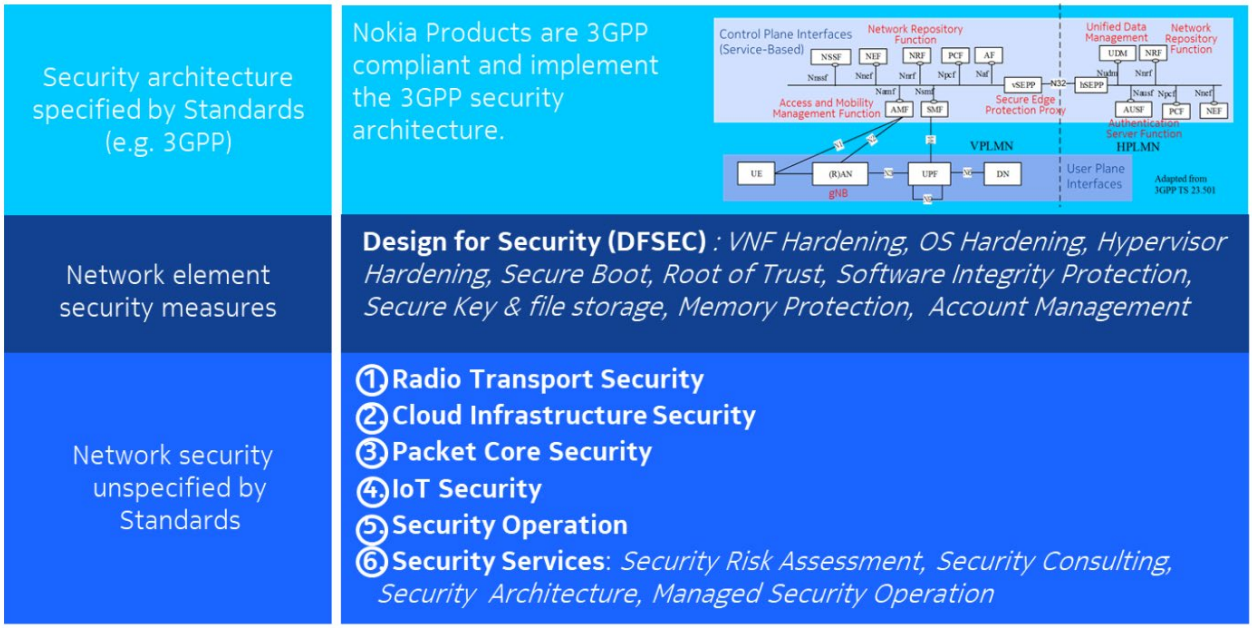

Figure 11 – Defense in Depth

The 1st layer is the 3GPP specified security architecture. Security features are implemented in most 5G solutions and products, supporting 3GPP-recommended security architecture.

The 2nd layer is the hardening of the Virtual Network Function & cloud infrastructure and is vendor and network dependent. Vendors require well-defined security management processes built into their Design & Development. This ensures all products in the portfolio are implementing a baseline set of security features and hardening according to best practice within the industry. Examples include secure key and file storage, secure boot, root-of-trust, account management, and Software Integrity Protection.

The 3rd layer is also vendor and operator dependent. Vendors must identify gaps that are not covered by 3GPP and standard VNF & CNF hardening steps and fill the gaps by offering comprehensive security solutions and services.

The diagram below illustrates the essential elements of a security architecture for a 5G network implemented on distributed service provider networks:

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

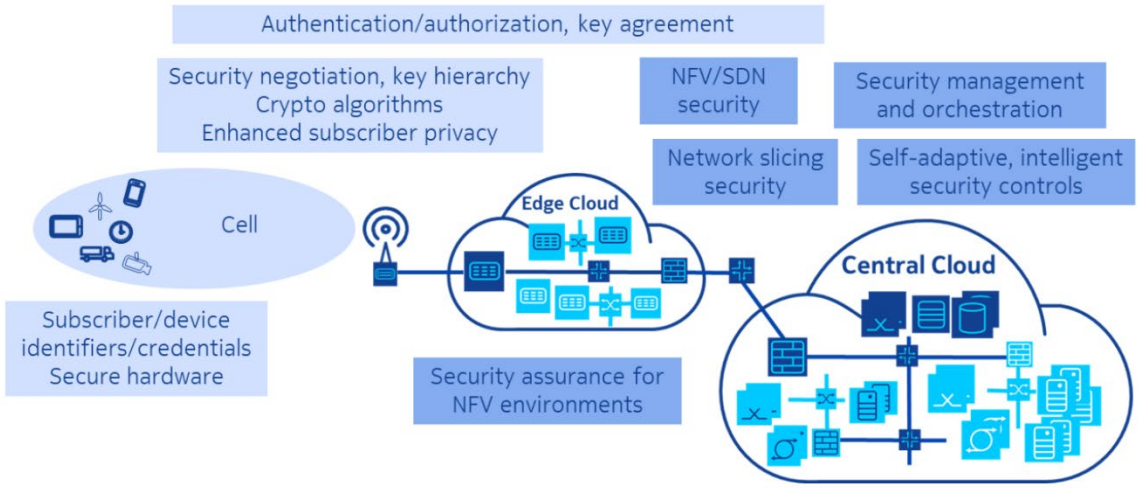

Figure 12 – Edge, infrastructure & cloud security

The key security areas are split into Radio Transport Security, Network & Packet Core Security, Cloud Infrastructure Security, Network Slicing Security, Security Operations, Design for Security (DFSEC) and last but not the least are the security professional services which help operators to understand their existing security risks, to design, implement and operate their network the most secure way.

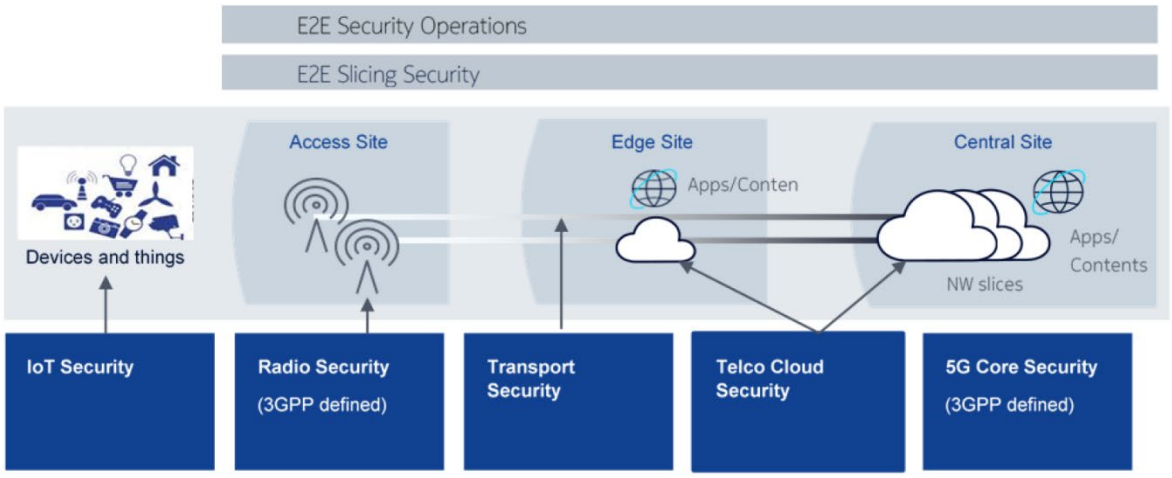

Figure 13 – 5G security overview

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.4 Key defense building blocks

Defense is the deployment of security controls in layers to eliminate or mitigate against threats. Defense includes:

- Layered protections – security layers complement one another, such that what one layer misses, another layer will catch
- Defense in multiple places – security defenses are pervasively located in different places within the network
- Defense through diversification – when possible, using different security controls will limit the effect that a fault or a vulnerability in one part of the network will have on the rest of network

3.4.1 Identity

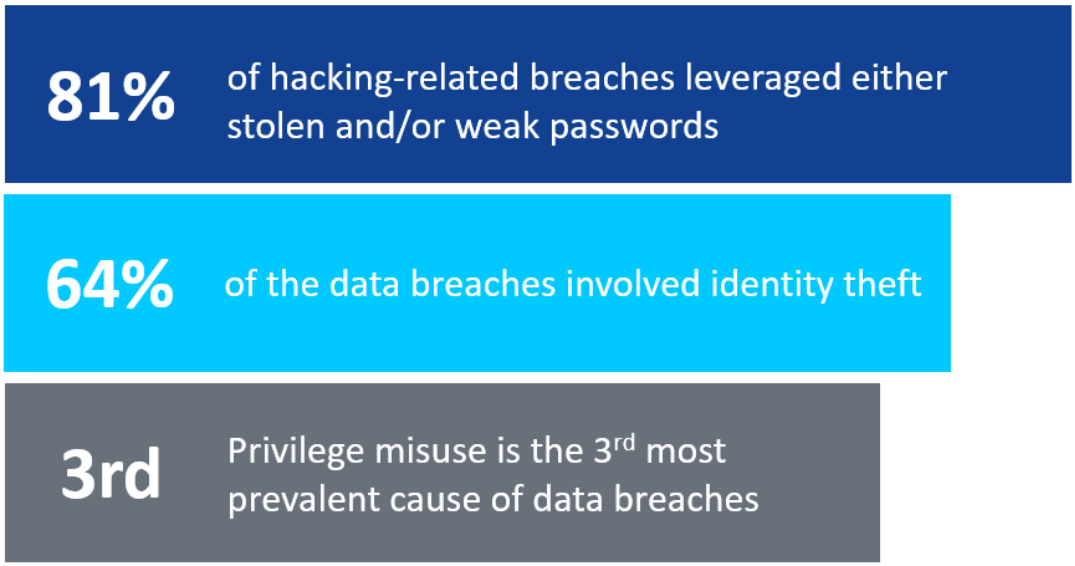

Figure 14 - Identity

Identity is the basis of any sound defensive posture. One must know who a threat is (and who isn't) with certainty, quickly and robustly at scale.

Two primary functions required to maintain identity in the end-to-end network:

- Certificate issuance
- Certificate deployment & Lifecycle Management

These tasks are performed by a Certificate Authority (CA) which must be:

- Centralized

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

- Issues certificates to NFs for NF-NF mutual authentication
- Certificates enable TLS and IPSec for secure NF-NF communications
- Highly scalable – support millions of certificates

3.4.2 Abstraction (or Zoning)

Abstraction is the classification of objects into security classes or groups and assigning security controls, rights, permissions and privileges to these classes or groups. An object in a 5G network could be any network element, application, device or asset which is part of the infrastructure providing the mobile service.

The classification of objects in mobile operator networks should be made based on their criticality to the business and their level of exposure to external threats.

Examples of abstraction in a mobile operator network include division of the network into security zones and the assigning of security controls to mitigate threats specific to each zone. Abstraction also involves the methods used to control how access to different domains of the network is controlled for administrators and network operations personnel, along with controls which are applied to ensure security of the network element configurations.

3.4.3 Zero Trust

As 5G networks are being exposed to a large array of threats, classification of objects based on a "Zero Trust" concept is required.

In response to the NIST RFI for Developing a Framework to Improve Critical Infrastructure Cybersecurity (RFI # 130208119-3119-01), Forrester Research introduced the security concept of "Zero Trust"

For years in information security most security concepts were designed based on a model of a "hard shell and soft core". Alternatively called the "castles-and-moat" framework. This model is based on threats always coming from outside the network, requiring a "hard shell", while permitting loose controls on the inside of the network "soft core", where free access to systems is generally employed. This concept has become outdated for many reasons, including:

- The distributed & hybrid nature of the network with edge, core & cloud locations
- The model does not consider or expect internal threats, where "trust" is implicitly granted. However, the reality of the last few years is that internal threats are a significant attack vector into networks, including not only malicious employees, but also human error and identity spoofing. Once in the internal network, the attacker has a free reign to penetrate other systems with almost no risk of detection. And the attacker can stay in the network for extended periods of time, sometime even years
- The model does not account for machine-to-machine/IoT communication, as well as complex automation processes, which cannot be trusted by default just because they are "internal"

The Zero Trust model is straightforward:

- Zero Trust implies that there is no such thing as a pre-granted trust status – nothing and no one is trusted – not even inside your network. This applies to everything in the network including

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

traffic, machines, devices, and people. Zero Trust mandates that since nothing is trusted, controls must be implemented on a per service per request level to protect the business. This is unlike a host or IP-based security mechanism where trust is wholesaled to anyone with a hostname/IP and thus to any application running on that device.

Zero Trust requires that security professionals protect internal data from insider abuse in the same manner they protect external data on the public Internet, following three main principles:

1. All resources must be accessed securely, regardless of their location (logical or physical) in the network
2. Access control and least privileges are key security mechanisms to employ across the entire network
3. The security framework for the network is built based on all available "if-then" scenarios. Logs are gathered, making sure all traffic is inspected, to cover future "what-if" scenarios

Zero Trust also means that security controls are not built on top of each other, but rather controls are built from the inside out, starting with each system and network element, and using that as the basis for building security across the complete network.

3.4.4 Data Hiding

Data hiding is the concept of revealing to any subject only the minimum level of information the subject requires to perform their task. System hardening standards must also be employed to ensure that only the required minimal number of services for a specific implementation are running, thereby reducing the attack vector open to malicious traffic, and minimizing the potential for widespread disruption of service.

3.4.5 Encryption

Information in a mobile operator's network is a combination of data in transit, as well as data at rest. Some of this data is sensitive subscriber data, while other data is critical information needed to configure and manage the network. To protect against attack vectors attempting to exploit this data, encryption is used to control sensitive and critical information while the information is traversing the network (in-transit) or is stored (at rest).

3.5 UEs, Radio & Transport Security

In every mobile network, there is a radio interface. This interface is inherently exposed to attacks and must therefore be secured carefully. Traffic over the radio interface is already encrypted as publicly known, but radio air interface security must go beyond encryption.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

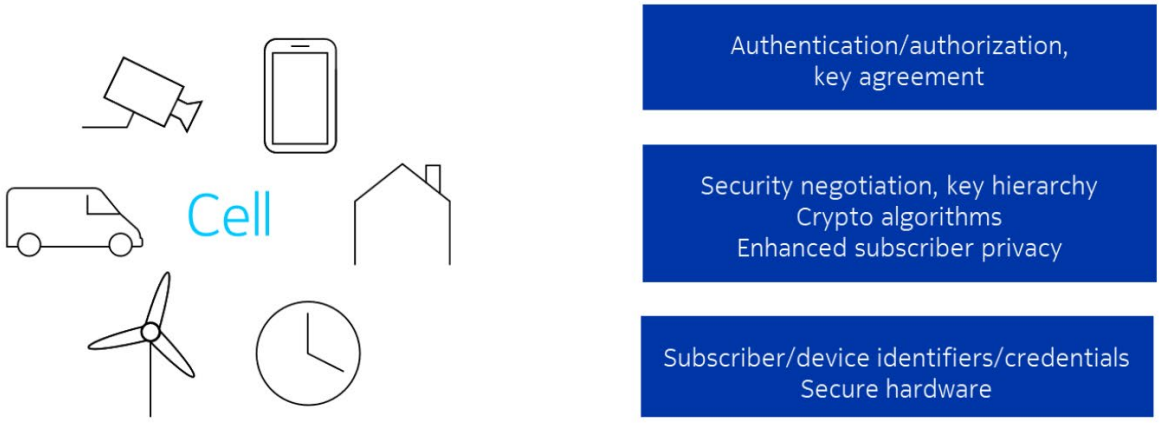

Figure 15 – UE security & privacy protection

First, UEs (mobiles) must be authenticated and authorized to use the network or specific services. The authentication relies on means to identify subscribers or devices, and on credentials that should be stored on the devices securely, making use of specific secure hardware, such as the SIM card. The SIM card is technically called UICC, or Universal Integrated Circuit Card, on which a USIM (Universal Subscriber Identity Module) is implemented. During authentication, a key is agreed upon, from which a hierarchy of session keys is derived to secure the subsequent communication. How security is applied must be negotiated, for example, determining which type of traffic will be secured and by which crypto algorithms this will be achieved.

“Enhanced subscriber privacy” refers to the fact that in earlier network generations, an attacker can trick mobiles into revealing the true identity of the subscription, a practice known as “IMSI catching”, one that is applied not only by attackers but also by law enforcement. In this mechanism, the subscription identifier is never passed in the clear over the air but encrypted. Protection against this kind of attack is considered a requirement for 5G. All falls under the scope of 3GPP.

The attacks on the confidentiality and integrity of the traffic can be mitigated by state-of-the-art cryptography. This has been standardized by 3GPP for many interfaces.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

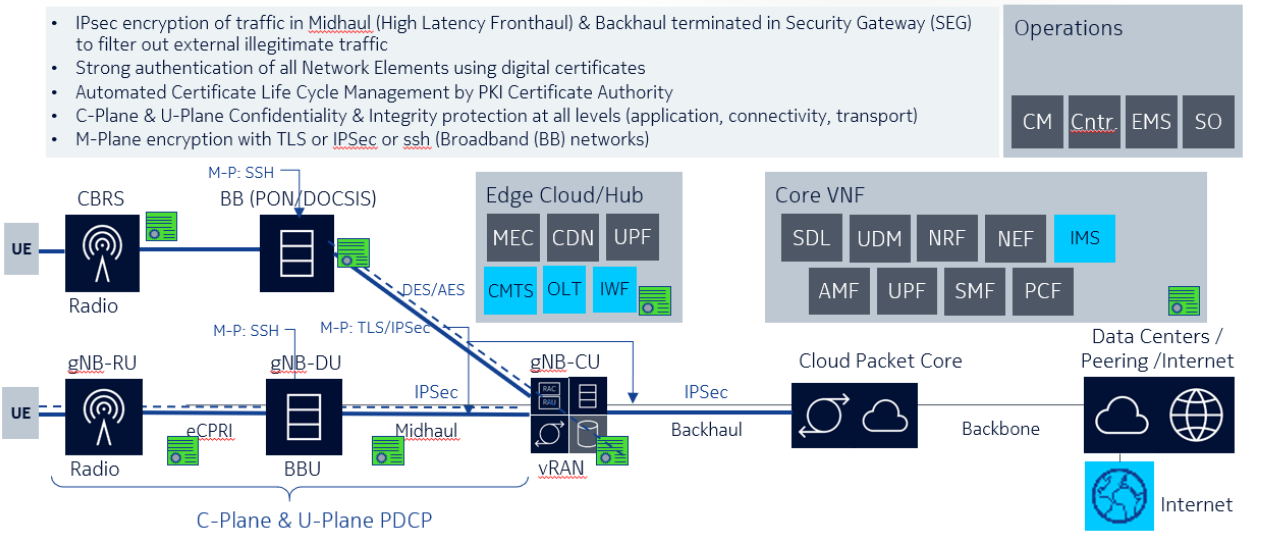

Figure 16 – UE, radio & transport security

Next-generation Node B (gNB), especially CBRS radios, gNB-CU & gNB-DU are located in unsecured locations. Hackers can easily attack the core network from any unsecured DU or CU through the transport network interface. In order to protect the edge cloud and cloud core data centers from illegitimate traffic, the best practice, as recommended by 3GPP, is to encrypt the traffic between gNBs and the core network using IPSec. The concept to encrypt all traffic from DU or CU is not only to ensure confidentiality and privacy of user traffic but more important to ensure all traffic entering the core network is not tainted by hackers in any way. The 3GPP recommendation to filter out unwanted traffic is to encrypt the legitimate traffic with IPSec and authenticate with asymmetrical keys using with Public Key Infrastructure (PKI).

Key solution components for this include:

- Security Gateway (SeGW) devices with GTP firewall and IPsec capabilities
- the centralized security gateway management system and
- PKI, or Public Key Infrastructure. Public Key Infrastructure consists of the Certificate Manager, which is served as the PKI certificate authority. A strong authentication of gNBs is provided with PKI certificates
- Automated Certificate Life Cycle Management is also required to be provided by the Certificate Manager/Authority

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.6 Network & Packet Core Security

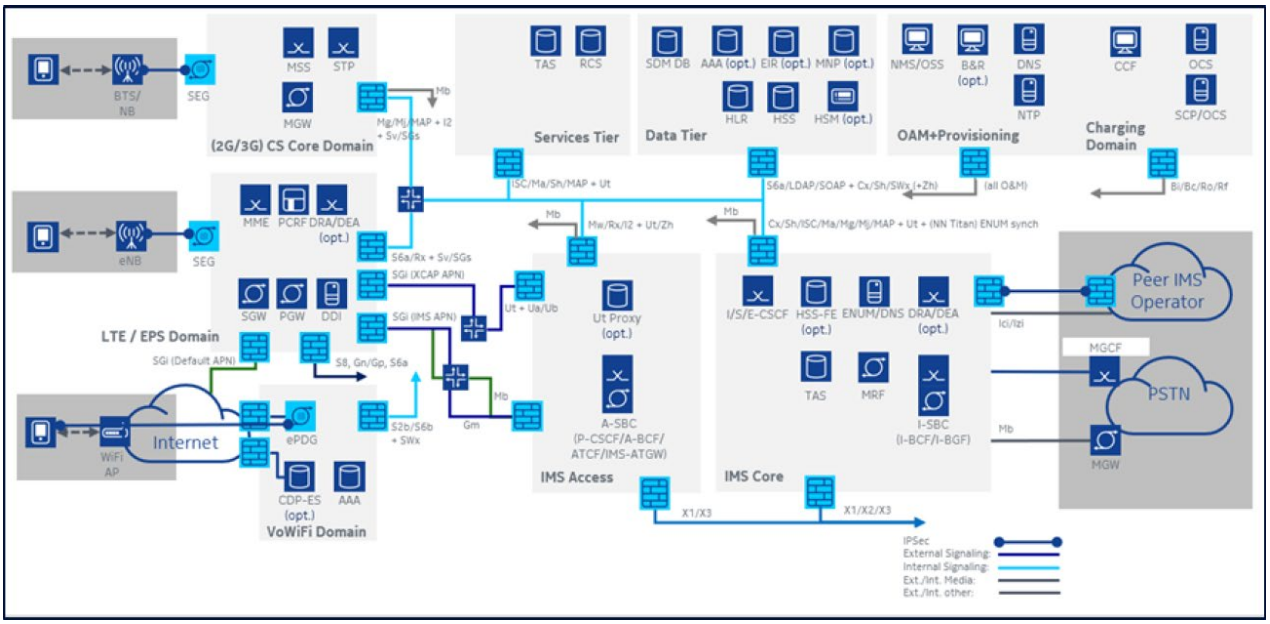

Figure 17 – Network & Packet Core security

A comprehensive security architecture meeting stringent data and roaming security standards includes:

• E2E traffic separation and zoning are mandatory to isolate high exposure equipment from high value assets. In case one security zone is compromised, the exposure can be easily contained before the high value asset is also compromised. Security Zone must be implemented from the beginning or retrofit will be difficult and costly

• Virtualized security appliances provide isolations between security zones or domains

• GTP, SCTP firewall to protect the eNB or gNB interface from radio access network

• Diameter firewall is required to protect the DIAMETER roaming interface

• Physical or virtualized firewall with Intrusion Detection System and Intrusion Protection System (IDS/IPS) is required at DN or SGi interface to internet

• Secure DNS to protect against infiltration of network via DNS

• Protect network from DDoS volumetric attacks

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.7 Cloud Infrastructure, NFV & SDN Security

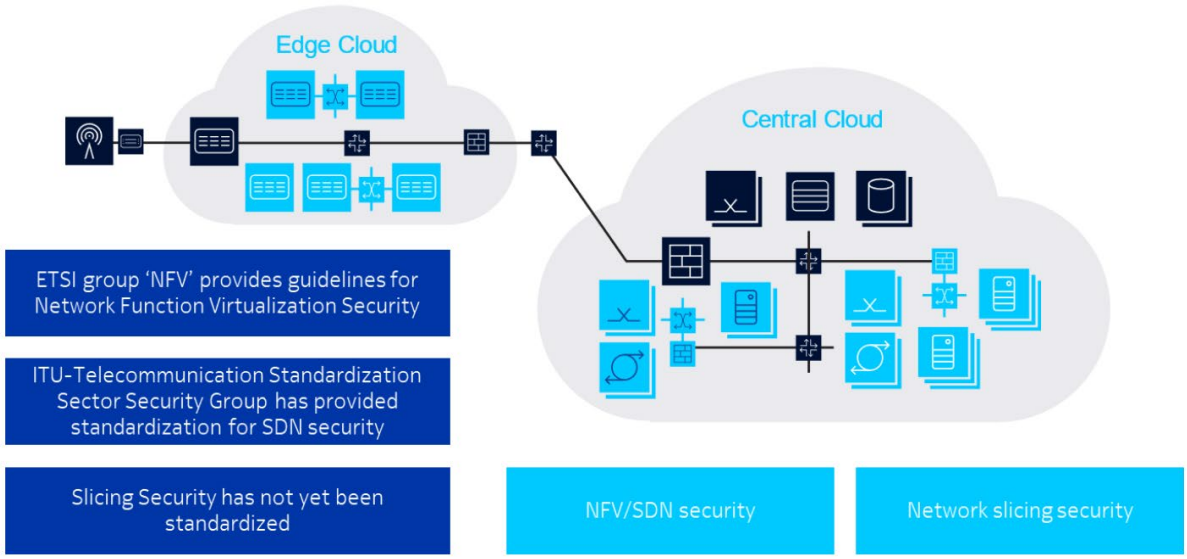

Figure 18 – Cloud, NFV & SDN security

Cloud infrastructure using NFV and SDN technology is crucial in 5G as it enables the flexibility and the elasticity needed for the diverse use cases.

All 5G networks adopt the new networking paradigms Network Function Virtualization and Software Defined Networking, as well as supporting slicing. In this section, we do not cover specific NFV and SDN security measures but only the threat of side channel attacks in NFV environments.

One can conclude that it is important to design and implement the shared cloud platform with a high degree of care, in a way that keeps the residual, exploitable vulnerabilities to a minimum, whilst still being prepared to patch the system quickly, in case one of these residual vulnerabilities are detected. SDN and NFV security are not specified by 3GPP. It is the security group of ETSI that provides guidelines and recommendations for Network Function Virtualization security.

To secure a network implemented in an NFV environment, the following security measures are recommended:

• Secure implementations of the virtualization layer and the overall cloud platform software. The focus here is about implementing a robust hypervisor and good isolation of traffic data. Examples include:

- Root of Trust: software integrity protection, secure boot, & vendor certificate
- Security hardening including zoning, segmentation & traffic filtering
- Security management: Certificate management, malware protection, identity management, & image signing
- Security orchestration: automation of security policies, breach remediation, monitoring & API security
- Robust security implementation of the VNFs & CNFs

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

- Good logical separation of VNFs provided by the virtualization layer. It is possible to have a physical separation of VNFs, but this comes at a cost and less flexibility
- Traffic separation by dedicated virtual switches, VLANs and wide-area VPNs
- Perimeter security and network internal traffic filtering by virtual firewalls
- Logically or even physically separated security zones
- Secure operation and maintenance, secure operation of IP services (e.g. DNS)
- Cryptographic protection of traffic and of data on storage

To ensure the SDN is secure, the SDN controller must be secured. Implement important measures, such as:

- Cryptographic protection
- Authentication and authorization
- Robust implementation of overload control

Microservices architecture introduces different requirements around how applications are developed, deployed, and managed across their lifecycle. It presents new attack vectors – need to be concerned with the fact that containers share a common kernel. Keeping malicious container applications from exploiting kernel and container security holes is a top concern.

All CNF (Container Network Functions) owners must run security audits and security scans on all container images which are produced. The audits must include:

Container provided default security mechanisms e.g. process restrictions, file & device restrictions, sandboxing using Linux namespaces, & Linux kernel hardening

Image provenance: Check if images and packages inside images are up-to-date and are free of security vulnerabilities

Namespace quotas

Application separation by namespaces or clustering or zoning (Kubernetes provided)

- Audit automatization, we must be able to automatize all checks. That will save precious time and one can run it as often as one requires. Manual audit is not an option unless one is just testing or learning
- Container links and volumes. If you use read-only filesystem in your running container “docker diff” can help you to find issues
- The bigger an image is, the harder the audit will be. Reduce the size of your images as much as you can
- The host kernel is the shared point between all containers in the same server, keep that kernel up-to-date

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.8 Self-adaptive security management and orchestration

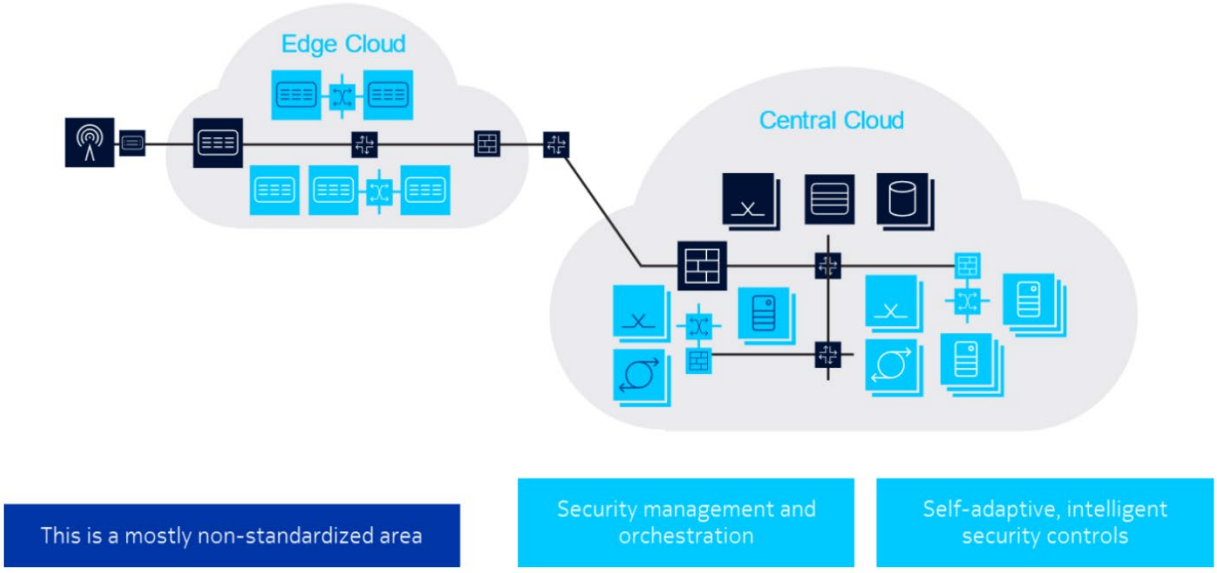

Figure 19 – Security management & Orchestration

There are two key parts of the 5G security architecture Security Management and Orchestration, and what is known as “self-adaptive, intelligent security controls”, which describes tools that monitor the network pervasively, analyze the information gained to detect anomalies and attacks, and trigger suitable countermeasures, with as little need for human interaction as possible. Again, this is an area that is mostly non-standard.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.9 Network Slicing Security

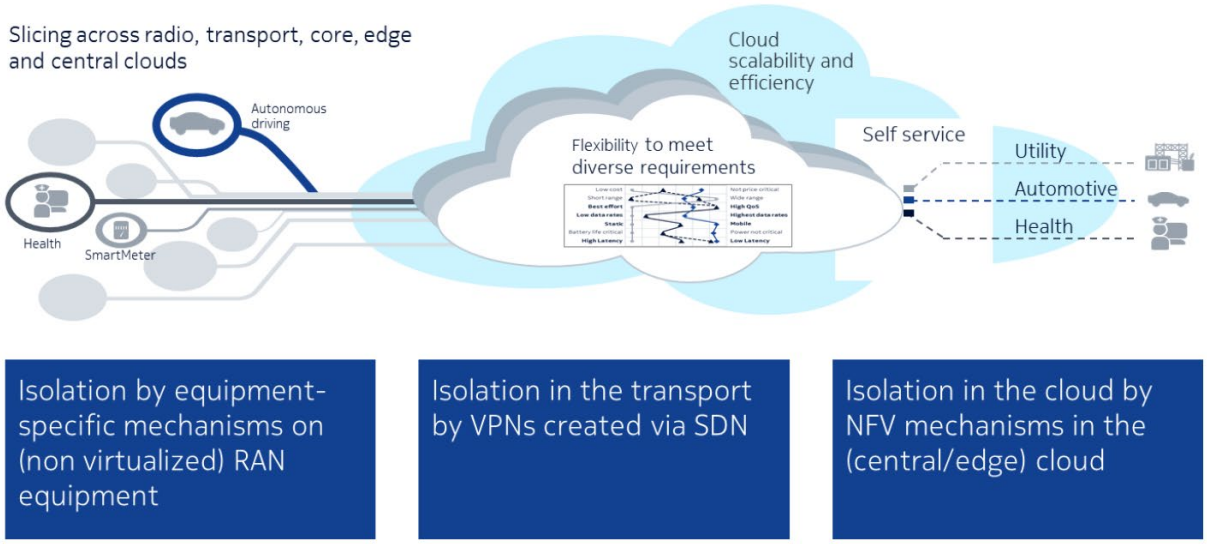

Figure 20 – Network slicing security

The crucial aspect in slicing security is slice isolation. Isolation has two angles:

- Availability: resources dedicated to one slice cannot be consumed by another slice
- Confidentiality: data/traffic cannot be intercepted/faked by entities of another slice

Network Slice Isolation = Resource Isolation + Security Isolation

Isolation will confine any effects of a potential cyber-attack to a single network slice. It is obvious that perfect isolation is required in a multi-tenant setup, where tenants may be competing organizations, such as different manufacturers running each running its own industrial automation slice.

As mentioned earlier, 5G security must be flexible. Instead of a one-size-fits-all approach, the security setup must optimally support each application. In a sliced network, this can be achieved by customizing the security setup per 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).

Below are recommendations for network slicing security:

1. Better isolation if less components are shared

No side channel attacks if computer hardware and hypervisor are not shared

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

Tradeoff between resource usage efficiency and degree of isolation

Sharing increases the resource usage efficiency but potentially lowers the isolation

In a big central data center, there may be abundant physical resources, so some physical resources may be dedicated exclusively to one application, e.g. the UDM or a network management system. In small (far) edge cloud deployments, it may not be possible to set aside part of the physical resources for a single application only

2. Cloud Infrastructure security is mandatory. Cloud infrastructure must be carefully designed, implemented, and hardened to minimize vulnerability and side channel attack

3. Secure, trusted parties operating the shared parts are required

In most cases, a mobile network operator MNO may be considered a trusted party by its customers. There can also be use cases where the tenant cannot afford to rely on the security provided by an MNO, but needs to establish its own security mechanisms, including the use of tenant-owned infrastructure (for sensitive data, e.g. subscription data), where the MNO has no access at all

If untrusted parties need to deploy their application in a shared infrastructure, for example, online game vendor may want to install their gaming software in the Mobile Edge Compute (MEC) platform in order to reduce network latency, it is suggested operators must have a well-defined onboarding process to ensure the 3rd party software is fully tested and validated in a sandbox environment before deployment

4. Security automation & orchestration is needed to cope with dynamic nature of slicing. Security management and orchestration must be aware of slicing, same for the reactive security controls. Some security tools may only run within one slice, not aware of other slices, but there must be others that have the complete network view

3.10 Design for Security (DFSEC)

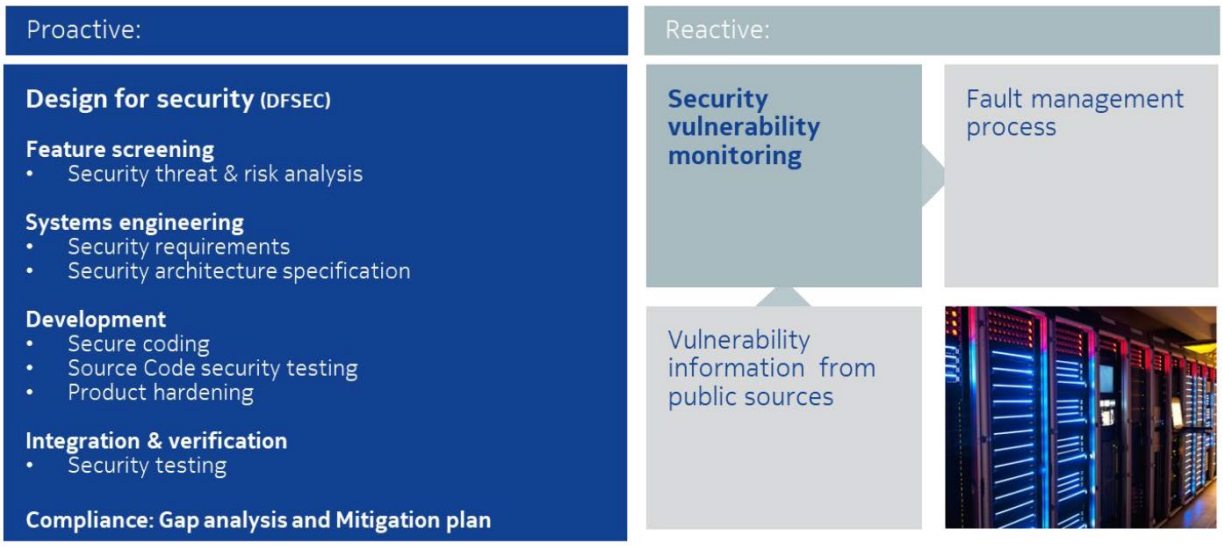

Figure 21 – Design for Security (DFSEC)

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

The vendor community recognizes that product security is not limited to security functions and protocols implemented in the product itself. Product security is strengthened and augmented by information security, incident response/vulnerability management and independent checks and audits.

Vendors must be capable to comply with legal and regulatory requirements around the world. And implement a security management processes and contractual security requirements for their internal teams and suppliers. Privacy by design is a part of Design for Security (DFSEC). Data privacy modelling and security features must be inbuilt to protect sensitive and private customer information in their products and ensure that product design complies with applicable regulatory requirements such as GDPR.

DFSEC is based on standards, industry best practices and customer requirements. Vendors' processes must be aligned with global security assurance frameworks from 3GPP (GSMA NESAS), TL9000 etc. Products must undergo customer acceptance tests, and security is a part of this testing. Below is a list of industry standards that must be employed in different phases of the Design & Development process.

Table 2 – DFSEC requirements

DFSEC Phase	Standard Compliancy
DFSEC	• SSE-CMM (SSE-CMM)
Threat / Risk Analysis	• ISO/IEC 27001 • 3GPP TS 21.133 Security Threats and Requirements • ITU-T X.805 (threat categories) • Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2
Security Requirements	• ISO/IEC 27001 • ISO/IEC 17799
Security Architecture	• ITU-T X.805
Secure Coding	• MISRA C
Security Testing	• NIST-1 (2003). NIST Guideline for Network Security Testing.
Security Auditing	• Common Criteria, Common evaluation methodology
	• ISO/IEC 19011 Guidelines for quality and/or environmental management system auditing.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

Vendors must have a Design for Security (DFSEC) process embedded in the product development lifecycle and applies security requirements and security architecture at the beginning of the lifecycle, shifting the product security process from being reactive to proactive. DFSEC covers all the product development phases from feature screening, systems design, software development, integration, to verification processes.

Security is never a one-time effort. Every modification makes it possible for software bugs and security vulnerabilities to emerge. Therefore, security development must be process-oriented. Every release will undergo same threat & risk assessment, security checks, tests etc.

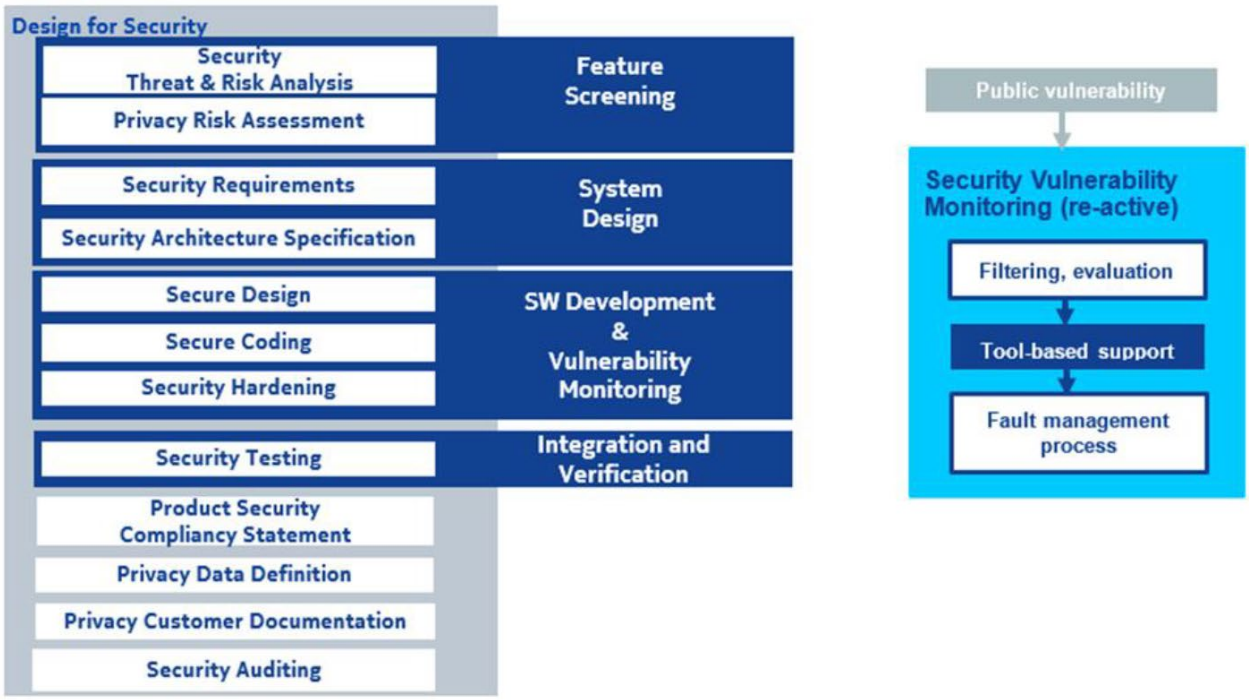

Figure 22 – DFSEC in action

Independent audits give customers further confidence in security promises and helps vendors identify areas where they can improve to meet the latest threats. Vendor must conduct third-party vulnerability scanning and penetration testing for their product samples. And ensure that operations support centers are certified to ISO 27001 standards.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

3.11 Security Operations

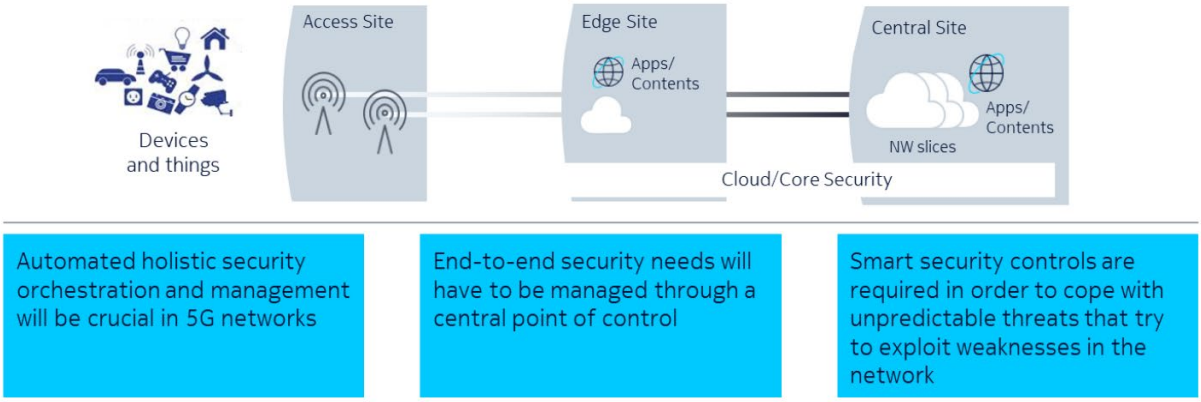

Figure 23 – Security Operations

Today, security professionals monitoring service provider and critical infrastructure networks often get thousands of cyber security alerts each day. Many are false alerts and duplicates. Yet, the sheer number of alerts can overwhelm a company's security team, resulting in incidents that are not investigated. For example, the "2018 Ponemon Security study" found that on average, 44 percent of alerts are not investigated, and of those investigated and deemed legitimate, nearly half (49 percent) go un-remediated. Teams need better ways to automatically prioritize alerts that allows them to focus on the most severe ones first. It is not an option to stay with the manually-intensive approach in the 5G era and must be migrated to an automated approach supported by artificial intelligence, data analytics and machine learning.

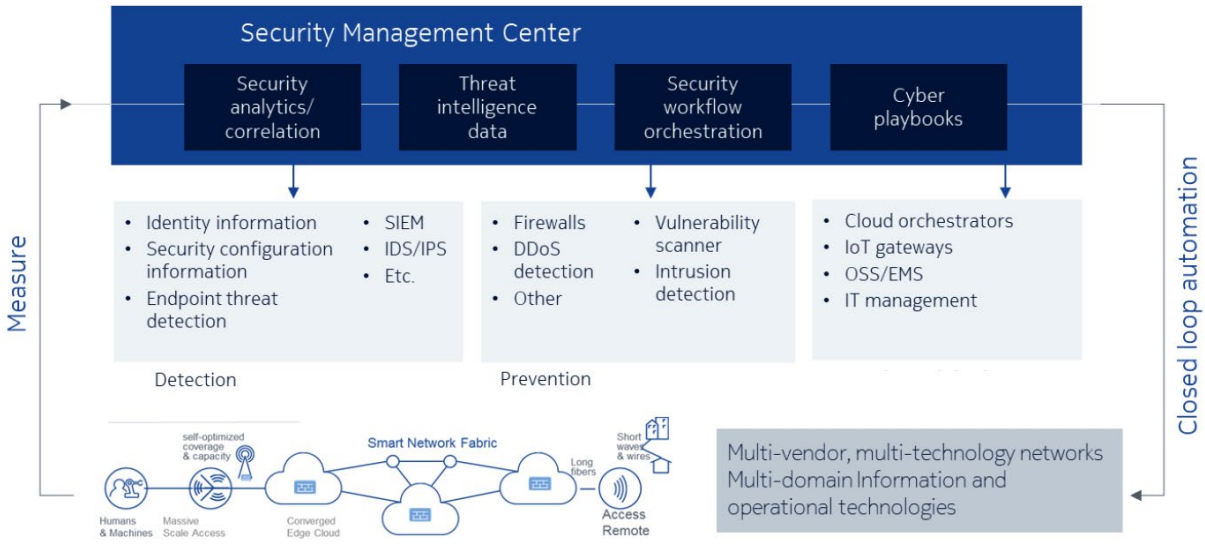

Figure 24 – Security Management & XDR

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

SOAR solution has been developed to replace today's manually-intensive approaches with security systems built on three pillars – intelligence gathering and analysis with machine learning and automation.

Intelligence gathering and analysis correlates data from across the network, devices, and cloud layers to spot suspicious anomalies, and provide insight into the nature of the threat, the associated business risk, and the recommended response.

Security Orchestration, Analytics & Response (SOAR) must be supported by an umbrella of security applications covering all aspects covered earlier in the paper:

1. Identity Access Manager

implements access controls to ensure least privileged access to key operational systems. It provides jump-host for CLI and GUI access to all (physical or virtual) network elements. i.e. no direct access from operator's consoles to management interfaces of the network elements. Human credentials are segregated from network elements' credentials. It also assures traceability of operator actions

2. Audit Compliance Manager

automatically and continuously audits the configurations of network entities for compliance with golden configuration

3. Certificate Lifecycle Manger

automates certificate enrollment and deployment, discovery, and audit

4. Endpoint Security

- analyzes network traffic in order to detect malware and anomalies of all end-user devices

5. Security Management Center

- aggregates logs and data for real-time monitoring & management. It provides a consolidated view for efficient reporting and simplifies incident management and forensics

3.12 Extended Detection & Response (XDR)

A fragmented security posture must move towards integration across Security Operations, Security Tools and Threat Intelligence. Extended Detection and Response (XDR) enables all three areas of integration. XDR takes security orchestration, automation, and response (SOAR) to even greater effectiveness through a cloud-native architecture built to accommodate the ever-growing and increasingly complex volumes of data coursing through 5G networks. XDR-based security operations are anchored by a robust data pipeline. That makes it possible to collect more data from more sources, all processed and analyzed through one cohesive security management system — so threats can be acted on faster and more effectively than ever before.

With machine learning (ML), the effectiveness of intelligence gathering, and analysis will improve continuously. Having access to a massive amount of high-quality data is the basis for training an AI/ML system. When using a security product that includes ML, you will want to augment the things you have

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

done in the past, like signature collection and automated malware analysis, and combine them with the machine's capability to determine new, malicious content.

A data pipeline also allows XDR to provide overarching security lifecycle management, orchestrating and automating all aspects of risk and threat prediction, detection, and response. Security teams can more easily integrate disparate threat intelligence data that is tailored to their unique requirement, model specific threats and attacks to their networks, and automatically apply the most appropriate preventative controls.

XDR solutions should provide the following features:

- Integrated security operations: End-to-end visibility across networks, clouds, and endpoints through a "single pane of glass" management interface — allowing security teams to quickly pinpoint the exact source of any potential breach
- Integrated security tools: Manage and administer disparate point products in a coherent and consistent way, providing a library of interfaces and connectors that bring a range of end-to-end infrastructure components and multi-vendor security tools under a single security management platform
- Integrated threat intelligence: Cognitive threat detection analyzes network sessions for malware or anomalous device behavior, and interprets the global threat landscape in a consistent, actionable way. Automated alert prioritization and classification eliminate the need for security teams to investigate redundant or lower-priority notifications so they can focus on blocking legitimate attacks

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

1. Summary

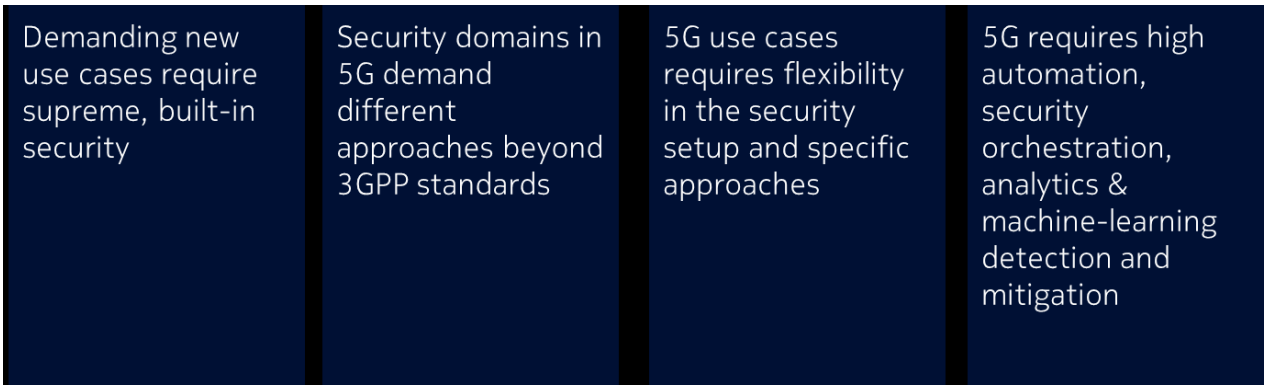

Figure 25 – End-to-end 5G security

End-to-end holistic security is mandatory in 5G network deployment and it is clear that:

1. 5G has a lot of mission critical use cases requiring supreme, built-in security. All network functions in the system must be hardened to avoid known vulnerabilities. Retrofit is always challenging and costly and, in some cases, service impacting
2. Number of network functions in a typical 5G network will be an order of magnitude more than 4G or fixed (cable or fiber) BB networks. Number of incidents and security logs will increase in the same order of magnitude. Adding the dynamic nature of the network configuration, 5G requires automation, security orchestration and machine-learning to identify and mitigate security threats
3. Different use cases may have different security requirements in different domains. Additional or overlapped security measures need to be implemented on top of recommendations from 3GPP standard
4. Because of dynamic nature of 5G network slicing, 5G use cases require flexibility in the security configuration

By introducing the security solution early on, operators can leverage security from the very beginning of their 5G rollout, rather than shelling out for an expensive retrofit further down the line. Operators can start to enrich security workflows, analytics, and training prior to the mass-deployment.

Security is a process (not a destination). Operators require a partner who is experienced in both 5G and security realms who has the skills, deployment experience in numerous 5G networks to be on top of any evolving threats and strong engineering and financial capabilities to continue investing in the 5G.

And most of all, a partner who is aligned in the overall goal to make 5G a secure, safe environment for everyone.

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

4 Acronyms

3GPP	3rd-Generation Partnership Project
AI	Artificial Intelligence
AKA	Authentication & Key Agreement
AMF	Access & Mobility Management Function
AR	Augmented Reality
AUSF	Authentication Server Function
BB	Broadband
CA	Certificate Authority
CMTS	Cable Modem Termination System
CNF	Container Network Function
C-Plane	Control Plane
CU	(gNode B) Central Unit
DFSEC	Design for Security
DN	Data Network
DNS	Domain Name Server
DOS	Denial of Service
DDOS	Distributed Denial of Service
EAP	Extensible Authentication Protocol
gNB	5G gNodeB base station
GTP	GPRS Tunneling Protocol
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPS	Intrusion Protection System

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

IPX	IP Exchange
MEC	Multi-access Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
N3IWF	Non-3GPP Interworking Function
NEF	Network Exposure Function
NFV	Network Function Virtualization
NGFW	Next Generation Firewall
NRD	Network Resource Directory
NRF	Network Repository Function
NSSF	Network Slice Selection Function
OSS	Operation Support System
OLT	Optical Line Terminal
PCF	Policy Control Function
PKI	Public Key Infrastructure
RAN	Radio Access Network
RU	(gNode B) Remote Unit
SBA	Service Based Architecture
SDN	Software Defined Networking
SeGW	Security Gateway
SEPP	Security Edge Protection Proxy
SIM	Subscriber Identification Module
SMF	Session Management Function
SOAR	Security Orchestration Analytics Response
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.

TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
U-Plane	User Plane
V2X	Vehicle to Anything
VNF	Virtual Network Function
VR	Virtual Reality
VSR	Virtual Service Router
XDR	eXtended Detection & Response

© 2021, SCTE® CableLabs® and NCTA. All rights reserved.