Security Considerations in 5G Networks: A Slice-Aware Trust Zone Approach

Dimitrios Schinianakis*, Ruben Trapero†, Diomidis S. Michalopoulos*, and Beatriz Gallego-Nicasio Crespo†
*Nokia Bell Labs, Munich, Germany. Email {dimitrios.schoinianakis, diomidis.michalopoulos}@nokia-bell-labs.com
†Atos Research and Innovation, Madrid, Spain. Email: {ruben.trapero, beatriz.gallego-nicasio}@atos.net

***Abstract*—A security study of 5G networks and the use of security trust zones in network slicing architectures are presented in this paper. In such an approach, the security trust zone concept is analyzed in terms of a profiling methodology that takes into account the characteristics of the supported network slice. Moreover, the performance and isolation capabilities of the trust zone approach is assessed via a simulation framework, in terms of its ability to detect and mitigate simulated threats. Finally, the security study complements the simulated framework with a use-case analysis of a network testbed, carried out in an industrial environment. The conducted analysis shows that security trust zones can offer a security level which can cover the detection capabilities of critical parts of the network.**

I. Introduction

A major requirement of fifth generation (5G) networks is their robust operation, reflected into their ability to provide an agreed level of quality of service for an agreed time of network operation. 5G networks are thus designed on the basis of *resilience* as one of the key performance indicators. In fact, this represents one of the major requirements for services subject to an uninterrupted network operation, such as machine-type and mission-critical communication services.

Together with resilience, *security* in 5G networks is associated with a similar level of importance when it comes to mission-critical communication services. This stems from the fact that failing to achieve the agreed security requirements of a critical service may cause major resilience issues. For instance, in case the network faces a distributed denial of service (DoS) attack, then failing to quickly detect and isolate such attack may cause downtime in the entire network infrastructure, hence disrupting the offered service [1].

A. Security study in 5G networks

Any security study pertaining to 5G networks should incorporate the special features and deployment characteristics of 5G, as compared to predecessor generation networks. In this regard, for defining an end-to-end security approach that applies to 5G, the security considerations for the main as well as peripheral 5G components should be taken into account.

An overview of the main security areas involved in 5G networks is presented in Fig. 1. In Fig. 1, the "devices" may refer to any type of network element used as a transceiver, ranging from typical hand-held devices such as smartphones and tablets, to devices placed in fixed locations such as sensors. The term "5G network" is a rather broad term that denotes all such elements of the 5G network that are susceptible to potential threats. The term "network slices" refers to all components that are associated with a slice-specific network operation, including the concepts of network virtualization and software-defined networking.

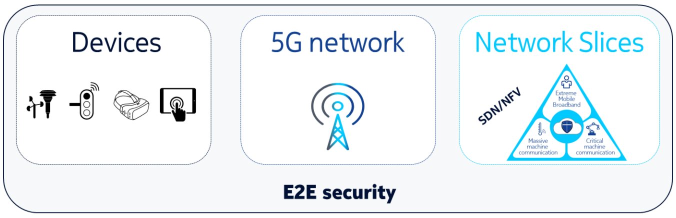

Fig. 1: Main security domains in a 5G network

B. Contribution and paper organization

Capitalizing on the aforementioned 5G security areas, this work proposes a security approach for network slicing-based 5G architectures. In this context, the use of security trust zones is assessed via a simulation setup, followed by an analysis of its implications in an industrial use-case deployment.

More specifically, Section II elaborates on the definition of a security trust zone template. This represents the basis for creating trust zone profiles used for distinguishing different logical and physical areas within the network with distinct security implications to the network. The performance of such security trust zone deployment is then assessed in Section III, via a simulation framework. Together with a simulation analysis, this work provides also a use-case analysis of the security trust zone concept, where a threat analysis of a industrial environment is put forward, on the basis of the main security areas given in Fig. 1. This use-case analysis pertains to a Sea Port 5G network (c.f. [2]), and is provided in Section IV. Conclusions are offered in Section V.

II. Security Trust Zones and Profiling Methodology

The optimization of resources and the flexibility to employ them across multiple application domains is one of the most salient characteristics of 5G networks. Built upon the paradigm of virtualization of resources and network functions, it uses the concept of *network slicing*. In this regard, such optimization refers to the specific resources devoted to a certain domain that operates over a 5G network, which is characterized by specific requirements in terms of performance.

©2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A. Building security upon network slicing

Having different network slices operating over the same 5G infrastructure creates several challenges in what regards to external factors, such as security threats. Such threats are exploited by attackers, thereby undermining the integrity of the rest of the infrastructure, possibly exposing critical data, increasing operational costs, computational resources, reducing performance and availability. Traditional approaches for the protection of critical infrastructures consider a homogeneous infrastructure in terms of security requirements, over dimensioning the security protection capabilities. The concept of network slices managed in 5G networks represents an opportunity to tailor security protection capabilities to the specific requirements of a network slice.

As an example, let us consider the 5G infrastructure of some telco operator, which has two different network slices: one deployed over a sea port infrastructure and another one deployed over a city to provide touristic services. The security requirements for the first network slice are probably higher than the ones for the latter. The security protection capabilities available in a 5G network can cover both cases, possibly by providing the same security level with the same amount of resources, even when the touristic services network slice has lighter security requirements. This results in overdimensioning on one of the network slices, overspending resources and unnecessarily increasing costs.

To solve the issue of inefficient usage of resources for security purposes, we use the concept of *Security Trust Zone* (STZ) [3]. STZs are conceived to cover the security protection of a subset of elements within a network slice, deploying just the needed mechanisms and components. More specifically, an STZ is defined as a logical area of infrastructure and services where a certain level of security and trust is required. This implies that security is regarded as the capability of being protected against threats, as well as the trust that the security expectations are met in a defined period of time.

B. Security trust zone template

Adapting the security protection features available in an STZ with respect to the security requirements of a certain infrastructure is paramount to guarantee an optimal resource allocation to the required level of protection. To this end, *STZ templates* are used to analyze the domain to protect and adapt the security protection capabilities to deploy in an STZ. The process followed to choose the most appropriate STZ for a given system is illustrated in Fig. 2. As shown in Fig. 2, two parts are required: the different STZs, characterized by their own security capabilities (STZ profiles), and the analysis of the system to protect.

Table I describes the template schema for defining STZ profiles. The characteristics of the STZs are divided into several groups which describe the characteristics of the STZ in different aspects. The general group provides general indicators about security, privacy and integrity levels provided by a certain STZ profile. The security capabilities are represented by the Detection, Prevention and Reaction capabilities.

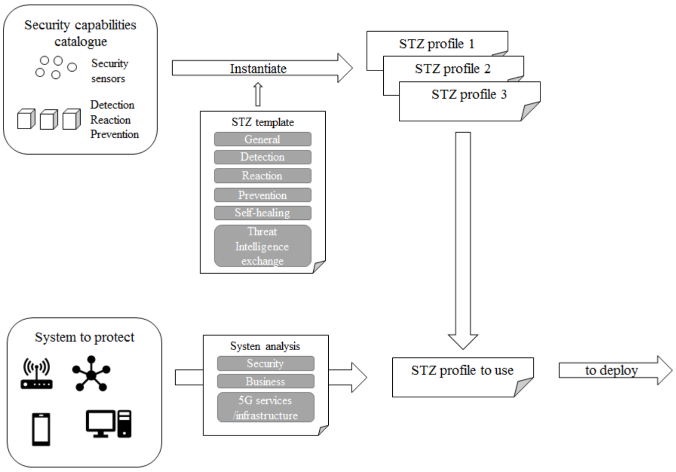

Fig. 2: Process to assign an STZ to a system

Every capability in Table I is described in terms of available sensors, types of events managed, and threats considered. Two additional aspects describe characteristics related to the relationship of the STZ with the rest of the 5G infrastructure. The Self-healing aspect describes the capability of adapting itself to changes at the infrastructure and the degree of autonomy with respect to the rest of the STZs (for example, to operate completely independently from the rest of the network slice, which, depending on the domain where it is applied, might be a mandatory requirement. The threat intelligence exchange group describes the capability of exchanging information received and sent from/to other network slices.

C. Creating security trust zone profiles

The methodology used to create these STZ profiles depends heavily on the type of system to protect. The target system needs to be analyzed in terms of exposure to risks, identification of critical assets and determining the security perimeter of the STZ. Table II describes the criteria to describe the system to protect in order to match the most appropriate STZ template. The security/risks dimension encompasses the traditional risk assessment and security framework guidelines, which will give a first approach agnostic to the particularities of the specific business and 5G context. The business dimension refers to the different requirements that are driven by the tenants, which are actually sharing the same 5G infrastructure. The services/infrastructure dimension takes into account the actual set of assets to protect and the technical resources available.

The business dimension has an impact on the application of some security controls rather than others, which in principle may be judged more appropriate or efficient, only because corporate policy or applicable national regulation impose them. Highly regulated environments such as eHealth or financial services are some examples where the business dimension criteria will weigh more than other dimensions. On the other hand, the agreed terms between tenant and service provider may influence the selection of controls with lower costs or footprint for example, in favour of guaranteeing a

TABLE I: STZ profiling template

Group	Property	Property
General	STZ Level	e.g. L (Low), M (Medium, H (High) or [1..5]
	Privacy level	Determines the privacy-preserving mechanisms put in place, e.g. when sharing threat intelligence between zones
	Integrity level	Determines the resulting integrity level to achieve, which is the objective of the security measures deployed
Detection capabilities	Threats	According to the Threat able to detect Taxonomy, the list of threats
	Rules Deployed	Set of available detection directives (not all might be active all the time)
	Rules Active	The actual set being monitored by default (may change at runtime)
	Sensors Deployed	Set of available sensors deployed (not all might be active all the time)
	Sensors Active	The actual set activated by default (may change at runtime)
	Events	The events understood by the infrastructure (type, XSD schema)
	Alarms triggered	The alarms output (to trigger actions)
Prevention capabilities	Threats	According to the Threat able to detect Taxonomy, the list of threats
	Rules Deployed	Set of available detection directives (not all might be active all the time)
	Rules Active	The actual set being monitored by default (may change at runtime)
	Sensors Deployed	Set of available sensors deployed (not all might be active all the time)
	Sensors Active	The actual set activated by default (may change at runtime)
	Events	The events understood by the infrastructure (type, XSD schema)
	Alarms triggered	The alarms output (to trigger actions)
Reaction capabilities	Countermeasures	According to a Countermeasure Taxonomy, the list of countermeasures able to trigger
	Rules Deployed	Set of available reaction rules (not all might be active all the time)
	Rules Active	The actual reaction rules applicable by default (may change at runtime)
	Actuators Deployed	Set of available reaction mechanisms deployed (not all might be active all the time)
	Actuators Active	The actual set of reaction mechanisms that could be invoked by default (may change at runtime)
	Alarms	The alarms understood by the infrastructure (type, XSD schema)
Self-healing capabilities	Reconfiguration rules	Under certain conditions, the actual configuration of the STZ may be changed to adapt to the context condition
	Autonomy rules	Enables the STZ infrastructure to work in isolation (disconnected) totally or partially (e.g. by logging events/alarms produced and countermeasures triggered, so these can be send back to the central node once the connectivity is restored)
Threat intelligence exchange	Conversion Plugins	Convert from/to different events/alarms formats/schema
	Normalization Plugins	E.g. when data ranges are in different scales (e.g. H, L, M scale vs 0..5 scale), or IP v4 vs IP v6
	Privacy-preserving Plugins	Applies privacy measures on the information contained in exchanged events/alarms (e.g. obfuscation, anonymization, pseudo-anonymization)

compromised service performance and value for money.

The services/infrastructure dimension would determine the most appropriate set of security components to deploy (and their configuration) in order to implement certain security controls. The overall capabilities of the STZ to protect against threats, in terms of detection, prevention and reaction, would be influenced by these criteria. In cases of limited resources, some less critical capabilities will not be activated or not even deployed at all.

As it was mentioned above, different profiles exist for the different STZs that are possible to be deployed according to the defined templates. This is illustrated in Fig. 3, where the security components of the deployed STZs in a network slicing architecture are put forward. In particular, Fig. 3 depicts the security components, which are classified as mandatory or optional depending on the respective STZ profile. Such components are described as follows.

- Security Threats Monitoring (SM). These components might appear in each STZ. Three sub-components can be deployed:
  - Security Threat Detector (SthD) - (Mandatory). This component would integrate a set of security probes (such as Intrusion Detection Systems), receive events from them and normalizing them for their latter correlation.
  - Security Threat Prevention (SthP) - (Optional). This component integrates prevention mechanisms which can receive information about incidents detected in other STZs or network slides, activating measures to prevent the incident in its STZ.

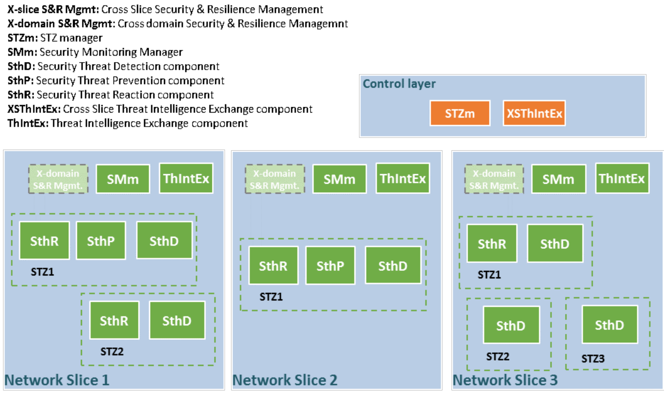
X-slice S&R Mgmt: Cross Slice Security & Resilience Management
X-domain S&R Mgmt: Cross domain Security & Resilience Managemnt
STZm: STZ manager
SMm: Security Monitoring Manager
SthD: Security Threat Detection component
SthP: Security Threat Prevention component
SthR: Security Threat Reaction component
XSThIntEx: Cross Slice Threat Intelligence Exchange component
ThIntEx: Threat Intelligence Exchange component
Control layer
STZm
XSThIntEx
X-domain S&R Mgmt.
SMm
ThIntEx
SthR
SthP
SthD
STZ1
SthR
SthD
STZ2
Network Slice 1
X-domain S&R Mgmt.
SMm
ThIntEx
SthR
SthP
SthD
STZ1
Network Slice 2
X-domain S&R Mgmt.
SMm
ThIntEx
SthR
SthD
STZ1
SthD
STZ2
SthD
STZ3
Network Slice 3

Fig. 3: Security components for STZs and Network Slices

  - Security Threat Reaction (SthR) - (Optional). This component will apply countermeasures to mitigate incidents detected in a STZ (i.e., activating specific firewall rules when detected DoS attacks).
- Security Monitoring Manager (SMm) - (Mandatory). This component will be deployed at network slice level. The SthD of every STZ would report normalized events to the SMm,

TABLE II: Criteria to analyze the system to protect

Dimension	**Criterion**	**Impact**
Security	Risk assessment results	Determine the critically of the assets to protect and prioritize some security aspects over others.
	Security Control Framework	Best practices on how to better secure the infrastructure.
Business	Compliance to applicable Regulation	Strict regulations applicable may force to implement privacy measures despite the apparent lack of threats likely to occur.
	Corporate Organisation Security Policy	Some organisations oblige implementing security measures which are not apparently proportionate.
	SLA (e.g. performance, resilience level, multitenancy/isolation)	This will force to relax the security measures in favour of maintaining certain level of performance or availability agreed between client (tenant) and the CSP/Network provider.
5G Services / Infrastructure	Geographical dispersion/distribution (NSs)	The actual Network Slice configuration applicable, with the HW, SW and virtual elements involved will influence the most appropriate STZ configuration (threats, type of sensors, possible countermeasures, etc.).
	Connectivity (Domains)	The more isolated (disconnected) the less prone to threats (in principle). This will also imply a higher degree of self-healing capabilities.
	Resources available	This determines the number and type of sensors that can be deployed, or e.g. the correlation processes that can be running in parallel.

correlating and aggregating these events and triggering alerts in case of detected incidents.

- Threat Intelligence Exchange (ThIntEx) - (Optional). This component will be deployed at network slice level and is in charge of managing the exchange of information between network slices. On the one side it allows to report to other network slices about incidents detected in any STZ of the network slice that it is managing, preventing the propagation of potential incidents. On the other side it receives information about incidents detected in other network slices, notifying the SMs, updating correlation rules for the detection of new incidents or triggering prevention mechanisms at the SthP.
- Security sensors - (Optional). According to the Detection capabilities defined for every STZ profile there can be different security sensors. These security sensors retrieve events from the infrastructure and send them to the SthD. Any component able to report to the SthD events about the behavior of the infrastructure and its assets is considered a security sensor. Some examples are Intrusion Detection Systems deployed in the network, anti-jamming detectors or agents deployed in devices to report about authentication events, performance issues or any type of information that might be relevant for its correlation at the SMm.

III. Simulated Performance of STZs

The STZ based approach for protecting network slices has been validated by creating a simulated 5G infrastructure where the elements of different STZs over two Network Slices have been deployed. The simulation setup consists on two Network Slices (NS1 and NS2) and three STZs: two STZ in NS1 (STZ1-NS1 and STZ2-NS2) and one STZ in NS2 (STZ1-NS2). One STZm is managing the security requirements of every NS, assigning the resources required to every STZ. Similarly, a SMm is managing the detection of incidents detected in the STZs.

Although two SMm could be deployed (one per NS), a single SMm is deployed to manage the detection of incidents of both NS. The SMm and the STZm are based on the Atos XL-SIEM, an incident detector environment that is built on top of an apache storm[1] kernel and a Esper[2] correlation engine. The Atos XL-SIEM supports multi-tenancy, distributed computing and load balancing which, for testing purposes, has been used to act as SMm from different NS with a single instance of the Atos XL-SIEM. For every STZ different security capabilities and security probes can be instantiated. Their number and type depends on the chosen STZ profile.

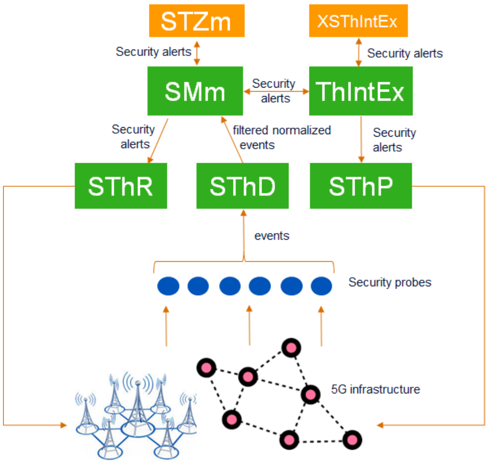

Fig. 4: A typical STZ deployment configuration

A typical STZ is similar to the one detailed in Fig. 4, where security probes receive events from the infrastructure to protect (such as logs or network traffic). The Detection capability would filter and normalize those events, reporting them to the SMm for its correlation (based on Esper directives defined as Event Processing Language (EPL) statements that are used to generate security alerts [3]). These alerts are reported to the ThIntEx to share it with other Network Slices. Additionally, the Reaction and Prevention capabilities use those alerts (received from their local SMm or from other NS through the ThIntEx) to enforce countermeasures or prevention measures

[1] http://storm.apache.org

[2] http://www.espertech.com/esper/

[3] https://docs.oracle.com/cd/E13213_01/wlevs/docs20/epl_guide/overview.html

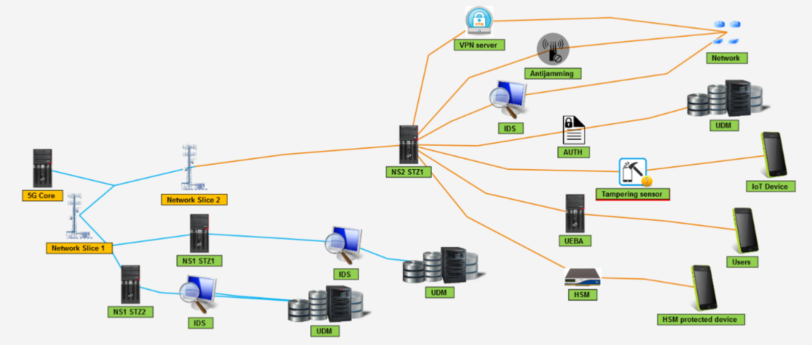

Fig. 5: The deployed simulation setup

in the infrastructure in order to fix or prevent, respectively, a potential incident.

The deployed simulation setup includes six security probes, as described in Table III. Four of such probes have been simulated (namely, Hardware Secure Modules (HSM), Anti-jamming, VPN server logging and Tampering sensor) and two have been actually deployed (namely User & Entity Behavior Analytics (UEBA) and Intrusion Detection System - IDS probes). These probes have been chosen based on the most relevant threats over a 5G infrastructure where a diverse set of devices (IoT devices, smartphones, etc.) are operating over a critical infrastructure (such as a sea port). For instance, in a network slice in charge of managing mission critical services it would be convenient to have tampering sensors in order to alert about physical manipulation of devices, though having HSM might be less relevant in this context.

In addition, the simulation setup includes Detection capabilities, with a SthD deployed for every STZ. In the deployment of the simulations, the NS1-STZ1 and NS1-STZ includes an IDS in every STZ, which is monitoring the network and an asset that represents the Unified Data Management (UDM) of a 5G infrastructure. The NS2-STZ1 includes the six security probes specified in Table III, and additional assets to protect, that is network, the 5G-related Unified Data Management (UDM) function (in part offering functionalities of the Home Subscriber Server (HSS) database in 4G networks like user authentication), IoT devices, User-Agents and devices protected with HSMs. A complete deployment of the setup is depicted in Fig. 5.

A set of simulated attacks have been carried out to show the capabilities of the security infrastructure based on STZs. The Atos XL-SIEM has been adapted to support the management of STZs, acting as SMm and STZm. Three SthD has been deployed, one per STZ. Every SthD is aware of the security probes running in their respective STZ, and therefore is capable of processing and normalizing their events. The attacks has been triggered from a Kali Linux distribution, which has been used to trigger DoS attacks (using the *hping3* tool), brute-force attacks (using the *ncrack* tool) and network scanning attacks (using the *nmap* tool).

The rate of events sent for every attacks depends on the type of incident simulated. The DoS attack generated a total of 3.091.103 packets transmitted in 20 seconds against the SSH port of the victim (enough to exhaust the targeted machine). The SMm detected the DoS 200ms after triggering the attack. The bruteforce attack required 10 login attempts in less than 30 seconds to alert about a potential incident. The network scanning attack took 13,14 seconds to completely scan the simulated network, while the detection of the scan was detected 500ms after triggering the attack. That is, the attack was detected before it finished. The rest of the probes were tested by generating events representing incidents, at different rates (100 events every 50ms and 100ms). After this stress test the result was a rate of detection of 100%, with an average delay of around 200ms between the generation of the alert and the detection of the incident. In general terms, the difference between sending a big rate of events every 50ms or 100ms is minimum. In fact, in real world, with the exception of DoS attacks, the rate of packages received in case of incident is way lower than the tests carried out in this work, which demonstrate the stability of the solution and the good performance.

The events are received by the SthD of every STZ, normalizing them and sending to the SMm. The SMm is capable of representing, filtering, and storing them for their correlation (based on Esper correlation rules) [4], generating security alerts in case of a positive match. It is worth noticing that the SMm is capable of managing independent correlations per STZ, using multi-tenancy capabilities to correlate, in an incident way, the events received by every STZ. As a result, mixing the correlation and reporting incorrect security alerts are avoided.

In general terms, the advantages of managing security at STZ are significant. The usage of STZs allows to address the problem in small niches, rather than addressing the protection of the 5G infrastructure as a whole. This allows to tailor the security protection capabilities to the security requirements of the STZ, optimizing resources and isolating the incident within the STZ. The promise of reducing complexity by reducing a problem to smaller problems applies in the case of STZs, which results in noticeable advantages in terms of reliability, performance and costs reduction.

TABLE III: Security probes available at the simulation setup

Security Probe	Asset monitored	Possible attack and detection
HSM	UA with HSM	Bruteforce attack against HSM protected device ; Main in the middle attack: modification of message integrity ; Detection of unsecure connections through HSM
Anti-jamming	Wireless network	Pulsed Based jamming attack; Wide Band jamming attack; Wave Form jamming attack; LFM Chirp jamming attack
VPN Server Logging	VPN server and connections	Detection of weak encryption in VPN connections; DoS attack against VPN server: connection requests flooding; Bruteforce attack against VPN server; Settings manipulation attack: authorized change of configuration for VPN connections
Tampering Sensor	Physical devices	Detection of unauthorized physical manipulation of devices
User and Entity Behavior Analytics (UEBA)	User Agents	Detection of anomalies in the behaviour of UA when using several services: SMS, Voice Calls, VR, etc.
IDS	Network, UDM	Denial of Service attack against assets (i.e., UDM); Bruteforce attack against assets (i.e., UDM, SthD, etc.); Malicious scanning of services (i.e., Port scanning)

IV. Use-Case Analysis: The Smart Sea Port

Besides the simulated analysis described in Section III, the use of STZs in network slicing architectures is assessed in a 5G testbed which is carried out in the industrial environment of the Sea Port in Hamburg. The Smart Sea Port use-case encompasses all the characteristics of a typical industrial IoT (IIoT) application, one of the main use-cases considered in 5G. This is dictated not only by the significant number of sensors, but also from the different requirements posed by each sensor-family, either it being ultra-reliable and low-latency communications (URLLC) (smart traffic light system for ship management), or massive Machine Type Communications (mMTC) (on-ship sensors for pollution measurements) or enhanced Mobile Broadband communications (eMBB) (assisted operation for port engineers).

This testbed showcases the use of network slicing, focusing on highlighting the co-existence of mission critical services with high data-rate applications. In this respect, the considered use cases involve i) intelligent transport applications with automated traffic lights; ii) enhanced sea port operations with the use of virtual and augmented reality; iii) improved pollution control with the use of sensors placed on ships. Details about the Smart Sea Port testbed are available online in [2]; the high-level architecture view of the testbed is given in Fig. 6.

This section contains a security analysis of the Smart Sea port testbed. In the following paragraphs three areas of interest are analyzed, namely i) the security of the involved *devices*; ii) the security of the respective *5G network components*; iii) the security aspects of the deployed *network slicing* architecture.

A. Device security

When it comes to device security, the first consideration relates to the support of USIM/UICC cards. Since the end-devices need to authenticate themselves as typical mobile devices in the 5G network, it is expected that they support at least a secure computing environment for storing critical keying material and performing sensitive cryptographic operations. Since many of the sensors are physically exposed, this turns to a major security concern. Integrated modules like Hardware Secure Modules (HSM) may mitigate the risk, since there exist already lightweight HSM-smart card solutions even for IoT devices [5].

Another issue relates to the support of cryptographic operations, in order to address the stringent requirements of some use-cases, like for example the URLLC application of smart traffic light systems. In this case, a crypto-algorithm that would not hinder the end-to-end latency is preferred. There exist several tailored crypto-solutions for such use-cases, although their standardization is still a work in progress [6]. Nevertheless, the well-established AES algorithm has exhibited remarkable resistance over the years and its lightweight versions might be able to address the performance requirements of most use-cases in the port [7]. Careful examination of performance figures can reveal whether standardized AES-based libraries are sufficient for each case.

A key-challenge closely related to the physical access of the devices is physical attacks. Physical attacks may include intrusive and non-intrusive cases, with the latter being of great importance, assuming that dedicated security personnel could hinder the intrusive attacks. Non-intrusive attacks may refer for example to electromagnetic or power analysis attacks, during which the attacker may be able to expose keying material or other sensitive information only by analyzing the electromagnetic emissions of the sensor or by examining its power traces during its operation. In these cases, the devices should adhere to at least all mandatory packaging regulations or incorporate countermeasures (could be in hardware) to mitigate the issue (for example trivial modifications in the computations data-path may produce normalized power dissipation traces or electromagnetic emissions without significant hardware footprint).

B. 5G security

When it comes to 5G security, 3GPP standardization work may serve as the main anchor point for our baseline security [8]. Indeed, the latest version addresses most of the security procedures required in a 5G network environment namely from gNB configuration to core network and UE-5G network connectivity security. In the Smart Sea Port these requirements are a prerequisite and in the next paragraphs we build further security considerations on top of 3GPP security work.

In Fig. 6 the general architecture of the Smart Sea Port use-case is illustrated. The numbered bubbles depict parts of the network where extra attention is required to safeguard a secure environment. In part 1 of Fig. 6, the connection between the

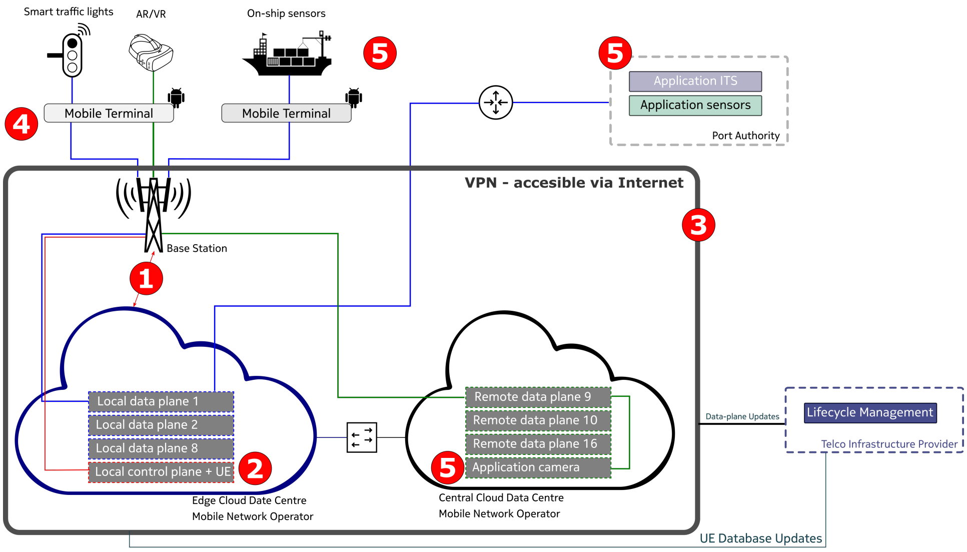

Fig. 6: High-level architecture of the Smart Sea Port use-case

gNB tower in the port and the local Edge Cloud infrastructure in Hamburg is considered. The main requirement here is a secure IPSEC connectivity between these two entities.

In part 2 of Fig. 6, the security of the Unified Data Management (UDM) and Authentication Server Function (AUSF) are examined (they provide partly the functionality of the Home Subscriber Server (HSS) in the EPC world). The main role of AUSF is to handle authentication requests both for 3GPP and non-3GPP access and inform the UDM upon successful or unsuccessful authentication of a subscriber. In the port scenario, these functions are part of the software stack of the local edge cloud, hence it is of paramount importance to assure a robust software implementation, especially against attacks which target subscribers data, DoS, etc.

Point 3 refers to the perimeter security provided by the VPN infrastructure. Although this might seem as a trivial remark, there are several examples of badly configured VPN connections with detrimental results. For example, in [9] a typical username/password enumeration vulnerability is described, where the attacker may infer whether a username exists or not and create usernames with the same pattern. Recently, another attack based on a 20-year old protocol (Internet Key Exchange - IKEv1) was unveiled. The researchers in [10] proved that by using a Bleichenbacher oracle in IKEv1 they could break RSA encryption and RSA signature-based authentication, both in IKEv1 and IKEv2. Other risks involve insecure password storage on the server side, re-use of cryptographic parameters, etc. As such, a VPN infrastructure needs to be meticulously planned to avoid implementation flaws. At the same time, high awareness of the latest advances in cryptanalysis and insecure software/hardware implementations is required, in order to apply the respective patches as quickly as possible.

Finally, point 4 refers to the mobile terminals that serve as the connecting point between the UEs and the gNB tower. The mobile terminals are basically Android devices and as such, they exhibit all risks and flaws in Android OS and are prone to all attacks tailored for this specific OS. For example, researchers in Nightwatch Cybersecurity published recently a vulnerability that purportedly exposes information about a users device to all application running on the device [11]. As such, an up-to-date OS and proper awareness/education of the device administrators are required to ensure error-free operation.

As a last word of notice, mobile terminals and UEs allow for close proximity in their surrounding environment, mainly due to their physical footprint and location. As a result, jamming attacks in their radio interfaces cannot be excluded. In this case, the concept of STZs might prove useful to detect a jamming attack and apply mitigation actions, as discussed in Section III.

C. *Network slicing security*

Network slicing security is a rather generic term, as it relates to software or hardware strategies and best practices that achieve the desired levels of security and slice isolation. To illustrate the variety of the topics related to network slicing security we offer a comprehensive enlistment in Table IV. Their status in the Smart Sea Port use-case is as follows.

The 1st risk refers to the common interfaces between the port authority and the network operator. A crucial point is the connection between the mobile terminals and the UEs. Fortunately, this connection is encrypted and as such resource mixing is prohibited.

The 2nd risk relates to DoS attacks targeting specific slices. In this case, the concept of STZs along with the possibility of deploying tailored HIDS systems and overload mechanisms is important and mitigates the risks.

The 3rd point refers to attacks in inter-slice interfaces or in other words how is network slice isolation achieved. Again, the project offers several mechanisms to protect against such threats. Firstly, different slices forward packets to different

TABLE IV: Network slicing security risks in smart sea port use-case

Security Risks	Countermeasures
1. Attacks on common i/f (HPA - MNO)	Mobile Terminal - UE connection is encrypted. Resource mixing is prohibited
2. DoS	IDS systems deployment, STZ, overload mechanisms
3. Attacks on inter-slice i/f	1) Different slices forward packets to different PGWs, thus separation is achieved. Encryption can be applied on top 2) Static p2p connection between PGW SGi i/f - tenants data center. Injection is prohibited.
4. Procedural attacks: slice authentication, authorization, slice management. Insider attacks: make use of another slice for cheaper performance	STZ, Access attempt and brute-force attacks monitoring, policies for level-access per user
5. Malicious message routing among slices	IDS, traffic analysis, behavioral analysis, anomaly detection, STZ
6. SDN/NFV security	Robust SW implementations, secure coding, overload control, cryptographic protection, integrity assurance of VNFs, logical separation of VNFs

Packet Gateways (PGWs), thus separation is achieved by design. On top, we have the option to apply encryption, thus strengthening isolation. Secondly, the connection between the PGW SGi interface and the tenants data centre is a p2p static connection thus inter-slice traffic injection can be prohibited.

The 4th risk refers to procedural attacks, namely slice authentication, authorization and management. The concept of STZs offer access attempt monitoring and resistance against brute force attacks. In the extreme case of a malicious insider attack that may by-pass or misuse a slice to achieve for example better rates for free, there is the possibility to implement level-access per user. In any case, those considerations are with the operator to implement and assess.

A 5th risk asserts the scenario of malicious message routing among slices (e.g., malware infected packets that may spread in the network). This topic is closely related to the slice isolation problem, but especially for malware we could leverage on behavioural analysis, traffic analysis, and anomaly detection mechanisms all well compatible with the concept of STZs.

Finally, the concept of NFV/SDN security is included in Table IV, since it is closely related to the slicing framework. There is minimal standardization work in this area, so our security assurance is associated with robust software implementations, secure coding, overload control, cryptographic protection, and the integrity assurance of VNFs. All these techniques, although generic, apply quite logically to the software stack of VNF/SDN. The point is that, as SW systems, VNF/SDN should adhere to the best possible secure coding techniques, undergo thorough testing, and support a safe procedure for SW updates in case of security failures.

V. Conclusion

The use of security trust zones offers a baseline that could offer adequate levels of security that is inline with the special characteristics of 5G networks. In particular, security trust zones can cover most of the detection capabilities for crucial parts of the network as we have shown for network slicing and inter/intra-interface connections between the various 5G stakeholders. Nevertheless, a semi-open point remains the assurance of robust SDN/NFV implementations. This can be provided by means of secure coding techniques or logical separation. In any case, the stakeholder that implements the respective software stacks may need to provide at least a certification of secure coding methodology throughout the implementation phase.

Acknowledgment

This work has been performed in the framework of the H2020-ICT-2016-2 project 5G-MoNArch. The authors would like to acknowledge the contributions of their colleagues. This information reflects the view of the consortium, but the consortium is not liable for any use that may be made of any of the information contained therein.

References

[1] H2020 ICT 2016 project 5G-MoNArch, "Deliverable D3.1: Initial resilience and security analysis," Jun 2018.

[2] ——. (2018, Aug) Deliverable D5.1: Testbed setup and 5g-monarch technologies demonstrated. [Online]. Available: https://5g-monarch.eu/smart-sea-port-use-case/

[3] B. Han, S. Wong, C. Mannweiler, M. Dohler, and H. D. Schotten, "Security trust zone in 5g networks," in *24th International Conference on Telecommunications (ICT)*, May 2017.

[4] EsperTech. (2018, Oct) ESPER documentation. [Online]. Available: http://www.espertech.com/esper/esper-documentation/

[5] Gemalto. (2018, Oct) IoT secure manufacturing. [Online]. Available: https://safenet.gemalto.com/data-protection/iot-secure-manufacturing/

[6] NIST. (2018, apr) NIST issues first call for lightweight cryptography to protect small electronics. [Online]. Available: https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics

[7] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," *IEE Proceedings - Information Security*, vol. 152, no. 1, pp. 13–20, Oct 2005.

[8] 3GPP. (2018, sep) TS 33.501 v15.2.0, Security architecture and procedures for 5G system (2018-09).

[9] S. Rahimi and M. Zargham, "Analysis of the security of VPN configurations in industrial control environments," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 1, pp. 3 – 13, 2012.

[10] D. Felsch, M. Grothe, J. Schwenk, A. Czubak, and M. Szymanek, "The dangers of key reuse: Practical attacks on ipsec IKE," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 2018, pp. 567–583. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/felsch

[11] N. C. Security. (2018, Aug) Sensitive data exposure via wifi broadcasts in android os [cve-2018-9489]. [Online]. Available: https://www.nightwatchcybersecurity.com/2018/08/29/sensitive-data-exposure-via-wifi-broadcasts-in-android-os-cve-2018-9489/