Grant Agreement No.: 871808
Research and Innovation action
Call Topic: ICT-20-2019-2020: 5G Long Term Evolution

INSPIRE-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond

D2.1: 5G Security: Current Status and Future Trends

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2020
Submission date	07/05/2020
Lead editor	Orestis Mavropoulos (CLS)
Authors	Grant Millar, Anastasios Kafchitsas, Orestis Mavrooulos (CLS); Anastasios Kourtis, George Xilouris, Maria Christopoulou, Stavros Kolometsos (NCSRD); Edgardo Montes de Oca, Huu Nghia Nguyen (MI); Antonio Pastor, Sonia Fernandez, Diego Lopez (TID); Vincent Lefebvre (TAGES), Chafika Benzaid, Tarik Taleb, Othmane Hireche, Mohammed Boukhalfa, Muhammad Farooq, Dang Yongchao (AALTO); Chrystel Gaber, Jean-Luc Grimault, Morgan Chopin, Jose Manuel Sanchez Vilchez, Kahina Lazri (Orange); Francisco Vázquez-Gallego, Laia Nadal, Ricard Vilalta (CTTC); Gürkan Gür, Bernhard Tellenbach (ZHAW); Jordi Ortiz (UMU)
Reviewers	Diana M. Osorio (OULU), Jean-Philippe Wary (Orange), Pol Alemany (CTTC), Dhuha Ayed (Thales), Pascal Bisson (Thales), Edgardo Montesdeoca (MI), Ricard Vilatla (CTTC)
Work package, Task	WP2, T2.1

Abstract

This Deliverable presents the current security landscape of 5G networks, as well as the evolution of requirements and trends in 5G security. It includes a summary of the 5G threat landscape, the 5G networks classification criteria and their threat taxonomy; a description of security requirements of 5G systems, divided into domain-specific use cases, and the elicitation of security requirements from relevant stakeholders in 5G; the current status of 5G networks, the solutions state for securing 5G systems, the standardization effort in the domain of 5G security, the relevant 5G projects, and open source initiatives; and a description of future trends and technologies in 5G networks, their limitations, and gaps related to the security of 5G networks. This deliverable aims to provide a basis for the identification of use cases and the development of 5G security enablers in INSPIRE-5Gplus.

Disclaimer

Acknowledgment

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement No 871808. The European Commission has no responsibility for the content of this document.

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

EXECUTIVE SUMMARY

This deliverable describes the current security landscape of 5G networks, and the evolution of trends in 5G networks regarding their security and requirements.

The fifth generation of mobile telecommunications (5G) is expected to be one the most important innovations of the current decade. 5G is the motor that will open a new era of accessibility, quality and reliability to everyone. 5G is expected to deliver technological advances with low latency, high speed, and reliable connections to mobile autonomous systems and large-scale deployments of IoT devices for Machine-Type Communications.

The development of the 5G technology is based on the specific requirements of several use cases. The expectations of commercial users are significant. However, mobile communications systems, due to their ease of access, are vulnerable to security exploitation from threat actors. Particularly, in the first generation (1G), mobile phones and their wireless channels were prone to illegal cloning and masquerading attacks. In the second generation (2G), a common attack vector was message spamming. This type of attack was used to inject false information, such as unwanted marketing messages. In the third generation (3G), with the introduction of IP-based protocols and communication, Internet-based vulnerabilities found their way into the wireless domain. The fourth generation (4G) enabled the development of new services and applications to the mobile domain, such as multimedia traffic and an increase in the smart devices. These advanced features led to an increased attack surface for mobile-based systems.

In 5G network, the security threat vector will be expanded even more ~~than 4G systems~~. The exposure of new connected industrial devices and connected critical services (e.g., smart cities, connected road infrastructure) will significantly increase the entry points for threat actors. However, the growing concern of citizens on how their data and information can be protected in such an interconnected world is pushing the innovation for novel, robust security and privacy centric applications.

The content of this deliverable includes:

- A summary of the 5G threat landscape, the 5G networks classification criteria and their threat taxonomy;
- A description of security requirements of 5G networks, divided into domain-specific use cases, and the elicitation of security requirements from relevant stakeholders in 5G;
- The current status of 5G networks, the solutions state for securing 5G systems, the standardization effort in the domain of 5G security, the relevant 5G projects, and open source initiatives;
- A description of future trends and technologies in 5G networks, their limitations and gaps related to the security of 5G networks.

This deliverable will provide a basis for future work in the context of the INSPIRE-5Gplus project. The aim of this deliverable is to facilitate the identification of the use cases and the development of 5G security enablers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBERIVATIONS

5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, Accounting
AAE	Adversarial Autoencoder
ACME	Automatic Certificate Management Environment
AF	Application Function
AI	Artificial Intelligence
AN	Access Network
AP	Access Point
API	Application Programming Interface
APP	Application Publishing Protocol
ARP	Address Resolution Protocol
AS	Application System
BN	Bayesian Network
BS	Base Station
C-V2X	Cellular Vehicle to Everything
CCAM	Cooperated, Connected, and Automated mobility
CFS	Customer Facing Services
CIA	Confidentiality Integrity Availability
CN	Core Network
CNN	Convolutional Neural Network
CU	Control Unit
D2D	Device-to-Device
DAI	Distributed Artificial Intelligence
DAM	Damage
DBN	Deep Belief Networks
DDOS	Distributed Denial of Service
DIS	Disaster
DLT	Distributed Ledger Technologies
DNN	Deep Neural Network
DPI	Deep Packet Inspection
DRM	Digital Rights Management
E2E	End to End
EIH	Eavesdropping/Interception/Hijacking
eMBB	Enhanced mobile broadband (eMBB)
ENISA	European Union Agency for Cybersecurity
ETSI SG MEC Group	European Telecommunications Standards Institute MEC Industry Specification Group
FaaS	Function-as-a-Service
FHM	Fully Homomorphic Encryption
FM	Failures Malfunctions
gNB	Next Generation NodeB
HetNets	Heterogeneous Networks
I2NSF	Interface to Network Security Functions
IAB	Internet Architecture Board
ICT	Information and Communication Technologies
IMA	Integrity Measurement Architecture
IoT	Internet of Things
IIoT	Industrial Internet of Things
LEG	Legal

LI	Lawful Interception
LSTM	Long Short-Term Memory Networks
MAC	Media Access Control
MAD	Manufacturer Usage Description
MANO	Management and Orchestration
MEC	Mobile-Edge Computing
MEO	Mobile Edge Orchestrator
MitM	Man in the Middle
ML	Machine Learning
mMTC	massive Machine-Type Communication
MNO	Mobile Network Operator
MOH	Mobile Edge Host
MTC	Machine Type Communications
MTS	Methods for Testing and Specification
MUD	Manufacturer Usage Description
NAA	Nefarious Activity Abuse
NF	Network Function
NFV	Network Function Virtualisation
NR	New Radio
NS	Network Slice
NSD	Network Service Descriptor
OSS	Operations Support Systems
OT	Operational Technology
OUT	Outages
PA	Physical Attack
PCA	Principal Component Analysis
PCR	Processor Capacity Reservation
RAN	Radio Access Network
RAT	Radio Access Technology
RL	Reinforcement Learning
RRC	Radio Resource Control
RSST	Received Signal Strength Indicator
SAE	Stacked Auto-Encoder
SDN	Software Defined Network
SDO	Software Defined Operations
SFC	Service Function Chaining
SLA	Service Level Agreement
SMART	Stopping Malware and Researching Threats
SotA	State of the Art
SSLA	Security SLA
SUIT	Software Updates for Internet of Things
TC	Technical Committee
TE	Terminal Equipment
TEE	Trusted Execution Environment
TEEP	Trusted Execution Environment Provisioning
TI	Threat Intelligence
TPM	Trusted Processing Module
TRxP	Transmission and Reception Point
UALCMP	User Application LifeCycle Management Proxy
UAV	Unmanned Aerial Vehicle
UD	Unintentional Damage

UE	User Equipment
uMTC	ultra-reliable Machine-Type Communication
URLLC	Ultra-reliable low latency communication
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VM	Virtual Machine
VNF	Virtual Network Function
VNFD	Virtualised Network Function Descriptor
VR	Virtual Reality
WG	Working Group
ZSM	Zero touch Service Management

1 Introduction

1.1 Scope

This is the first public deliverable of the INSPIRE-5Gplus project's Work Package 2 (WP) describing the current status and future trends of 5G security. This deliverable includes a survey of the threat landscape of 5G networks, the security requirements of 5G verticals, the current status of the security of 5G networks and as well as ongoing trends paving its future. The D2.1 addresses the following milestone of INSIPRE-5Gplus: "Understanding the security threats and requirements in 5G and beyond markets".

1.2 Target Audience

The target audience of this deliverable are stakeholders related to security of 5G technologies and infrastructure. The deliverable describes technical terms and technologies that are used to increase the security posture of 5G systems and use cases.

1.3 Structure

The main structure of this deliverable can be summarized as follows:

- Section 2 describes the security landscape, the classification criteria and the taxonomy of threats of 5G networks;
- Section 3 contains the security requirements of 5G in the scope;
- Section 4 contains an analysis of the current status of 5G networks, the latest security practices, 5G security standards, and finally a description of relevant 5G projects and open source solutions;
- Section 5 describes the future trends and technologies of 5G cybersecurity and the identified gaps and limitations;
- Section 6 concludes this deliverable;
- Appendix A. ENISA Threat Landscape Terminology gives more details on the terminology used by ENISA;
- Appendix B. Survey of existing TEEs presents a technical survey of all known TEE technologies;
- Appendix C. Questionnaire presents a survey that has been launched to gather requirements from different stakeholders.

2 Security Landscape of 5G networks

2.1 Classification Criteria

2.1.1 Architectural classification (CN, RAN, end user devices)

The architecture design of 5G networks was planned to allow the support of connectivity and data services. This enables techniques such as Network Function Virtualisation (NFV), Slicing and Software Defined Networking (SDN). The INSPIRE-5Gplus project based its classification on ENISA's threat landscape for 5G networks[2].

The 5G high-level technical architecture as described by European Union Agency for Cybersecurity (ENISA) is depicted in Figure 1 below:

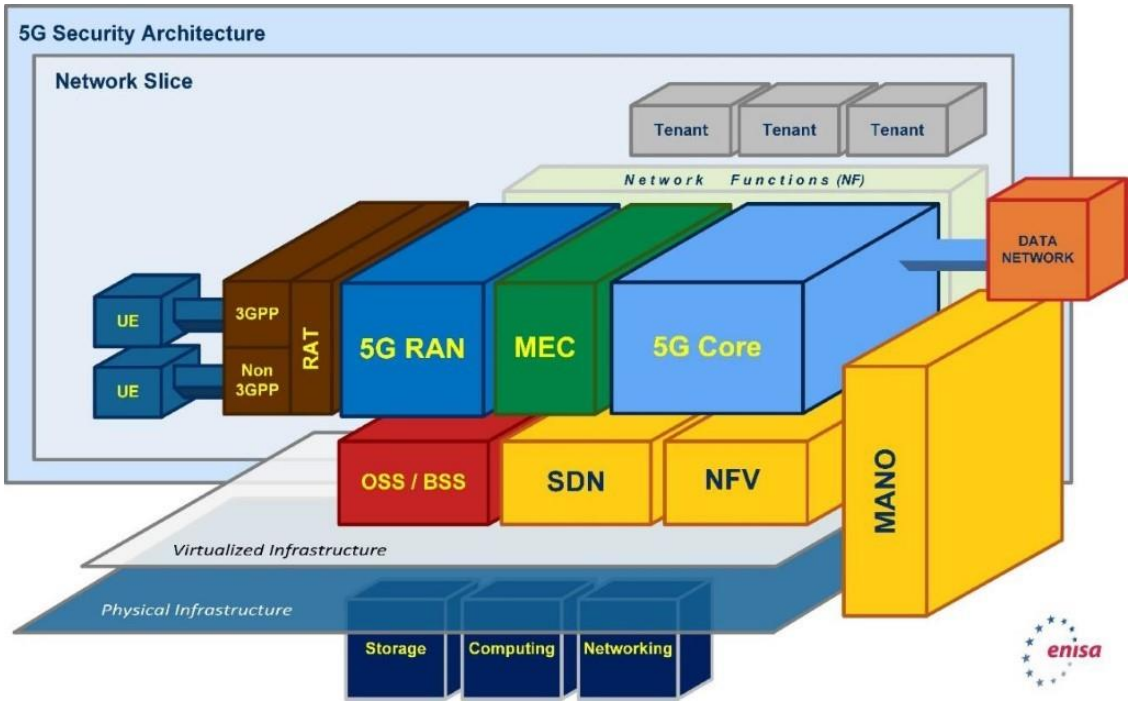

Figure 1: ENISA 5G Security Architecture[2].

The following terminology is derived from the ENISA's threat landscape for 5G networks. INSPIRE-5Gplus will use the same terminology as ENISA in terms of 5G threats.

Assets

An asset is anything that has value to an individual or organisation and requires protection. Due to its value, a digital asset becomes a target for threat agents. Threat agents are human or software agents, which may wish to abuse, compromise and/or damage assets. Threat agents may perform attacks, which create threats that pose risks to assets.

Assets relationship to the 5G architecture

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Slicing: Represents all 5G operations that create and manage slicing. Slices are independent virtualised logical networks that perform the task of network communication between the user's equipment and the 5G services.

Management and orchestration (MANO): Represent the set of assets that are related to the management and orchestration. The main components of MANO are the Network Function Virtualisation (NFV) orchestrator, the Virtual Network Function (VNF) manager, and the virtualised infrastructure manager. MANO is responsible for managing network functions, their virtualisation, and their software life cycle.

Radio Access Network (RAN): RAN represents the logical components that comprise the operations and functions of the RAN.

Network Functions Virtualisation (NFV): The NFV represents the network functions that are virtualized on top of proprietary hardware. NFV virtualises classes of network node functions and physical network functions (PNF) into blocks.

Software Defined Networks (SDN): Represents assets related to the SDN network controller, virtual network switches, data plane, application plane and control plane.

Data network: The Data network is used to interconnect different 5G network, operators, and providers. It is used to represent connectivity to external data and resources.

Lawful Interception (LI): Lawful Interception is concerned with the 5G functions that perform lawful surveillance and providing legally sanctioned access to 5G private communications.

Virtualisation: Represents assets that are related to virtual machine technologies and the hypervisor.

Cloud: Represents the logical cloud services that relate to the 5G.

Multi-access Edge Computing (MEC): Represents assets related to the decentralisation of cloud functions (storage of data and computing) located closer to the user or edge device.

Threat Agents (Threat Actors): According to ENISA Threat Landscape 2014 [3] a threat agent is "*someone or something with decent capabilities, a clear intention to manifest a threat and a record of past activities in this regard*". The nature of 5G networks will attract the attention of existing and new threat agent groups with a large variety of motives. However, with the implementation of 5G, the attackers' profile is expected to shift to take advantage 5G's novel capabilities. Some examples are:

- The vulnerabilities of interconnected systems will expand the attack surface, and exposure of critical assets;
- Novel tools and methods for vulnerability exploitation will be developed;
- The interconnection of verticals will surface new targets for threat agents;
- Existing groups of threat agents will collaborate to exploit and target critical assets.

Threat agents can be categorised as follows:

Cyber-criminals: Represents individuals who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.

Insiders: Represents malicious attackers perpetrated on a network or computer system by a person with authorized system access.

[3] ENISA Threat Landscape 2013, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Nation States: Are actor that perform state-sponsored attacks. Nation-state attackers target government agencies, critical infrastructure and any and all industries known to contain sensitive data or property.

Cyber warriors: Represents actors that are part of a military organization that maintains their presence in the cyberthreat landscape with a focus on 5G in both roles of defender and offender, depending on global geopolitical developments.

Hacktivists: Represents actors that perform cyber-attacks to achieve political or social gains.

Corporations: Represents actors that are backed by corporations to perform cyber-attacks against competitors.

Cyber-terrorists: Represents actors that their sole aim of violence against clandestine agents and subnational groups through the compromise of 5G infrastructures.

Script kiddies: Represents actors that do not poses deep technical expertise or resources to perform sophisticated attacks. Just as all other threat agent groups, script-kiddies may possess legitimate access to the network and be able to use network functions to manage their own devices, increasing thus the potential of misuse.

	Cyber-criminals	Insiders	Nation States	Cyber-warriors	Hacktivists	Corporations	Cyber-terrorists	Script-kiddies
Nefarious activity/Abuse	●	●	●	●	●	●	●	●
Eavesdropping/ Interception/ Hijacking	●	●	●	●	●	●	●	●
Disasters			●	●			●	
Unintentional Damage	○	●	●	●				○
Outages	●	●	●	●	○		●	
Failures/ malfunctions	●	●	●	●		●	●	●
Legal	○	●	●	○	○	●	○	
Physical attacks	●	●	●	●	●	●	●	

Legend:
Primary group of threat: ●
Secondary group for threat: ○

Figure 2: Threat Actors based on ENISA categorization[4].

The terminology is further detailed based on ENISA's description in Appendix A. ENISA Threat Landscape Terminology.

2.1.2 Key enabling technologies

NFV

To assess the NFV security landscape, firstly we must identify some key factors in its architecture and their possible attack vectors.

A main part of NFV is the Virtualized Network Functions (VNFs). VNFs are network functions that used to be on hardware but now can be deployed as Virtual Machines (VMs), containers or other virtualization techniques (e.g. firewall, vRouter, etc.). Since VNF is a software component, it may

[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

contain potential software vulnerabilities, or it can be a malware itself. Denial of Service (DoS) is a significant threat for them as they can be targeted and affect the entire network and infrastructure. For instance, VNFs can be victims of DoS attacks that causes them to overload and consume all the resources available, not only on the VM but on the host infrastructure as well, depending on the configuration.

To prevent as many as possible of these issues, a few measures are required, depending on the attack vector. To limit a DoS attack, Machine Learning (ML) assisted solutions can be used to detect attack traffic and distinguish it from normal traffic, so that it can be handled appropriately. To prevent a VM from impacting other VMs or even the host, a recommended security practice is to separate VM traffic and management traffic. In this way, attacks are prevented by VMs tearing into the management infrastructure. VNFs can be cryptographically signed and verified during lunchtime in order to enhance their trust level and avoid possible malware insertion [1].

Another important part of NFV and the potential attack vector is the virtualization layer. Attackers can find flaws and exploits in the VM or the hypervisor, permitting them to take advantage and perform unauthorized actions. Using these exploits, the attackers can escape the virtual environment and execute code in the physical host. Another attack can be obtaining privileged stats by using return-oriented-programming. They can also monopolize the resources or steal data from other VMs [2].

The attacks described above are vulnerabilities that can be found and exploited in different hypervisors. A common solution to mitigate vulnerabilities is the use of hypervisor introspection. The hypervisor introspection acts as a host-based IDS that has access to the states of all the VMs so that the rootkit and bootkit inside VMs cannot hide easily [252]. However, itself can also be used as an exploit.

Vulnerabilities and flaws can be found in NFV MANO's and VIMs. They can be exploited to control the host, the infrastructure or other components. If the NFV MANO is not properly secured, attackers may find a way compromise the communication with the MANO. Privilege escalation is a common attack on the VIMs, and, if successful, it can lead to partial control over the host. DoS attacks are also very common in order to overload the components [4].

To prevent these attacks within the NFV MANOs or VIMs, they must be designed with a strong security profile. There are however other steps that can be taken as well. Scaling boundaries can be imposed on the Virtualised Network Function Descriptors (VNFD) or Network Service Descriptors (NSD) so that amplification attacks can be prevented.

SDN

As it is known Software Defined Networking (SDN) consists of three layers, infrastructure, control, and application layer. In the infrastructure layer or data plane there are network elements and devices, such as switches, that provide forwarding capabilities. In the control plane, there is the controller that work as the brain of the network, supervising network forwarding behaviour, routing, etc. Finally, in the application layer, there are the SDN applications providing various kinds of functionalities. These can include network monitoring, analytics, load balance and more [4].

Consequently, there are several attack vectors that must be considered when dealing with SDN security. Controllers, being the centre and intelligence of the deployment, are a valuable target to attack. They can be targeted in various ways, from DoS, unauthorized access attack or topology poisoning attacks. Attackers can compromise the network by injecting malicious hosts into the topology and taking advantage of routing algorithms to perform a Man-in-the-Middle (MitM) attack.

Other vulnerable components are the switches. As the network traffic flows through the switches, they can be hit with a DoS attack, flooding the switch with large payloads with different flows. This can lead the flow table and buffer to fill up, and, as a result, new legitimate incoming packets would be dropped. The communications between control and data plane can also be compromised. MitM attacks can be performed by Address Resolution Protocol (ARP) poisoning, resulting in traffic

interruption. This can extend to traffic modification by replying to ARP requests with the attacker's own MAC address [5].

Another security issue is how to handle applications and new network applications in the application layer. Controllers do not have the ability to distinguish applications' legality or trustworthiness. Moreover, applications can have software vulnerabilities due to poor design or bugs, thus making them a potential target for exploitation. Attackers can also plant malicious applications performing attacks directly to the controller causing to crash or, otherwise, confuse it.

As seen previously, one of the main security threats in SDN is (D)DoS. This type of attack can be directed to all layers creating all sorts of issues in the deployment. DDoS detection is an effective way to mitigate the attacks. One innovative enabler of this is using entropy. The higher the entropy is, the higher the randomness. On a coordinated attack, the entropy lowers so that it could be used to identify it as an attack and take necessary measures [6]. Those can include the use of load balancer, dropping packets from recognized malicious IPs and MACs, coupled with anti-spoofing techniques such as Virtual Source Address Validation Edge. Currently, there are many solutions trying to detect such an attack but if that cannot be achieved, isolation of the network should be a goal as well. This can be done by network slices so that an attacker cannot affect the entirety of the infrastructure.

Another main attack type is network intrusion using various techniques. This can be countered by using ML enhanced network intrusion detection tools that recognize the infiltration and deploy extra security measures. Another way to deal with this is by amplifying the access security mechanisms and schemes. By boosting authentication, this type of attack can be prevented in the first place.

Finally, Application trust management is a great security concern for SDN. As explained before, attackers can take advantage of deployed applications or insert their own malware apps and perform all kinds of ill-intentioned actions. Periodic Topology checks are a way to secure the network by verifying the legitimacy of host migration, application insertion, etc. Enhanced authentication should also be implemented so that network visibility poisoning attacks can be prevented. Isolation of the applications can also be a useful tool, which can be achieved by using a sandbox approach of app deployment or other techniques [7].

MEC

MEC moves the computing of traffic and services from a centralized cloud to the edge of the network and closer to the customer. This way, by having the edge cloud collect and process the data closer to the end user, it reduces latency and brings real-time performance of high-bandwidth applications [8].

Any device with direct contact with the MEC system can be considered User Equipment (UE). This includes devices such as smartphones, Virtual Reality (VR), drones, tabs, so each of them can have different threat vectors compromising the security. These devices are usually attacked by physical tampering, malicious code injection or hardware trojans [9]. A compromised UE or UE app can threaten the MEC system in various ways. For example, attackers can deplete the resources of the UE disrupting the Mobile Edge Service (MES) or even manipulating the Mobile Edge Host (MOH) to allocate it more resources. In addition, the attackers can possibly convey malicious content to the MOH. An intrusion detection system can be implemented as a possible solution to this threat vector. Such system would be able to detect any intrusions and isolate the compromised UE preventing further damage [10].

One of the main attack vectors in MEC is the access network that is formed between the UEs and the Base Station (BS). Due to the nature of this network, it is susceptible to several attacks, such as MitM, eavesdropping, spoofing and more. This can lead to several threats for the MEC system, including the transfer of malicious code, interoperability issues, etc. To counter the threats, physical layer security methods are employed, thus avoiding excess overhead on the network, while advanced authentication methods are required, leading to enhanced security.

In MEC systems many threat vectors overlap with the vectors found in SDN and NFV, as MEC relies on these technologies. For example, the Edge network and entities such as VIMs and VNFs are a target for an attack. As discussed earlier, this can lead to VM escape or manipulation, DDoS attacks, as well as a disruption to MESs among other threats. Countering those vulnerabilities relies on using similar counters as discussed earlier in SDN and NFV, such as virtual machine introspection, security frameworks, and others.

Finally, a significant threat vector can be found in vulnerabilities in MEC control elements, such as the Mobile Edge Orchestrator (MEO), Operations Support Systems (OSS), User Application LifeCycle Management Proxy (UALCMP) and Customer Facing Service (CFS) portal. All these components are part of the Mobile Edge System Level. These modules are susceptible to various attacks, differing based on the role they are performing for the system. These attacks include DoS/DDoS and relay forwarded via the edge level, masquerading and spoofing intended to acquire accessibility, disrupting operation or services on the MEO, etc. Solutions to these vectors include hypervisor introspection methods and TPMs in order to certify the trust of entities [16].

“Security by the MEC”

The concept of “Security by the MEC” meets the needs to secure communications for Internet of Things (IoT) or Industrial IoT (IIoT) objects which are not capable by themselves to implement an enough security level for the considered use case. The principle consists in locating security functions as close as possible to the objects. The potential domains in which the security by the MEC could apply are numerous; we can quote for example: the industry, the smart city, the airports, the connected and autonomous vehicles, etc.

The requirements and mechanisms of the MEC such as specified by the European Telecommunications Standards Institute MEC Industry Specification Group (ETSI SG MEC group) (e.g. the specifications [11], [12], [13], [14]) define functionalities which can be harnessed for bringing security. These functionalities are of various types:

- **capacities of filtering in the data plane**, at the request of the MEC platform or of authorized MEC applications, possible filtering based on the customer identity;
- capacities to put **a MEC application in the data flow** (for example, in the scope of security, to implement some enciphering or to check messages content);
- **location service** provided by the MEC platform which can be provided to authorized MEC applications and which can help in a **monitoring service**;
- ability to chain two MEC applications;
- capacity to make **two MEC applications communicating**, even if hosted in two different MEC hosts.

The security functions potentially implementable in the MEC can be:

- The security functions **useful to the operator** to protect its network, to conform to national regulations or to make sure that the contract between the customer and the operator is duly respected; one can think at:
  - **network services limitations** (controls of the recipients’ address),
  - **monitoring**, for example in industrial use case where objects are not too much mobile,
- The security functions meeting the **customer needs;** in this category we can quote for example:
  - an enciphering/deciphering functions to assure the **data confidentiality**,
  - an access control function of an object to another object or to a corporate server.

It is necessary to note that security functions can be implemented as a MEC application **pertaining to the customer** (or to a third party) or as a MEC application **pertaining to the operator**. On the scope of a security framework harnessing the MEC capabilities, some questions must be studied, in particular:

- questions about performances of security functions implemented as MEC applications (e.g. enciphering function);
- variety of possible business models, for example in the context of configurations combining operator MEC equipment and customer MEC equipment to provide security functions;
- relationship between the MEC and the 5G.

Relationship between the MEC and the 5G for security purposes

Regarding the relationship between the MEC and the 5G, the 3GPP 5G system specifications define enablers for edge computing, allowing a MEC system and a 5G system to collaboratively interact in traffic routing and policy control related operations. In particular, the MEC has the ability, as a 5G AF ("Application Function"), to interact with the 5G system to influence the routing of the edge applications' traffic and the ability to receive notifications of relevant events, such as mobility events, in the 5G system [15].

2.1.3 5G Vertical Use cases requirements

5G verticals can be categorized based on their network design and architecture. The 5G verticals were defined by the 3GPP during the New Services and Markets Technology Enablers (SMARTER) project[5]. The SMARTER project's main objective was to develop high-level use cases and then identify which features and functionalities are required to enable them. The project started in 2015 and identified over 70 use cases. The use cases were initially grouped into five categories, and then they have been reduced into three. The set of the 5G verticals are the following:

- **Enhanced mobile broadband (eMBB)[6].** The eMBB is an extension to the existing 4G broadband services. The eMBB will be the first commercial 5G service enabling faster and reliable downloads. The ITU requirements for eMBB sets the thresholds at a minimum of 20Gbps for downlink and 10Gbps for uplink. The minimum requirement for eMBB mobility interaction time is 0ms.
- **Ultra-reliable low latency communication (URLLC).** URLLC is designed to support businesses on mission critical communication scenarios, such as emergency situations, autonomous systems operations, etc[7]. Examples of such scenarios include, public safety services, operations of mining, autonomous vehicles, oil and gas pipelines, robotics and health applications. Realising URLLC is one of the major challenges that is faced by 5G networks.
- **Machine Type Communications (MTC)** [33]**.** The MTC is expected to play an essential role in the future of 5G systems. The METIS[8] project has further classified MTC as "massive machine-type communication" (mMTC) and "ultra-reliable machine-type communication" (uMTC). The mMTC is focused on the wireless connectivity to billions of machine-type terminals. The uMTC is focused on availability, low latency, and high reliability. The significant challenge for the mMTC is the delivery of scalable and efficient connectivity for systems composed by a massive number of devices sending very short network packets. This challenge is something that is not adequately addressed in current cellular systems designed for human-centric communications. Additionally, mMTC solutions will need to enable wide are coverage and signal penetration indoors. In the same time, it must be low cost and energy efficient. The ITU minimum requirement for connection density is 1,000,000 devices per km^2.

[5] https://5g-ppp.eu/wp-content/uploads/2016/11/01_10-Nov_Session-3_Dino-Flore.pdf
[6] https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/
[7] https://arxiv.org/pdf/1801.01270.pdf
[8] https://metis2020.com/

Future implementations of 5G can be anticipated in multiple deployment scenarios for eMBB, mMTC, and URLLC. ETSI has provided the results of a study[9] for these future scenarios, which are presented in Table 1.

Deployment Scenarios
Indoor hotspot
The indoor hotspot deployment scenario focuses on small coverage per site/TRxP (transmission and reception point) and high user throughput or user density in buildings. The key characteristics of this deployment scenario are high capacity, high user density and consistent user experience indoor.
Dense Urban
The dense urban microcellular deployment scenario focuses on macro TRxPs with or without micro TRxPs and high user densities and traffic loads in city centres and dense urban areas. The key characteristics of this deployment scenario are high traffic loads, outdoor and outdoor-to-indoor coverage. This scenario will be interference-limited, using macro TRxPs with or without micro TRxPs. A continuous cellular layout and the associated interference shall be assumed.
Rural
The rural deployment scenario focuses on larger and continuous coverage. The key characteristics of this scenario are continuous wide area coverage supporting high-speed vehicles. This scenario will be noise-limited and/or interference limited, using macro TRxPs.
Urban macro
The urban macro deployment scenario focuses on large cells and continuous coverage. The key characteristics of this scenario are continuous and ubiquitous coverage in urban areas. This scenario will be interference-limited, using macro TRxPs (i.e. radio access points above rooftop level).
High speed
The high-speed deployment scenario focuses on continuous coverage along track in high speed trains. The key characteristics of this scenario are consistent passenger user experience and critical train communication reliability with very high mobility. In this deployment scenario, dedicated linear deployment along railway line and the deployments including SFN scenarios captured in Section 6.2 of 3GPP TR 36.878 are considered, and passenger UEs are in train carriages[10]. UEs, if the antenna of relay node for eNB-to-Relay is located at top of one carriage of the train, the antenna of relay node for Relay-to-UE could be distributed to all carriages.
Extreme long-distance coverage in low density areas
The extreme Long-Range deployment scenario is defined to allow for the provision of services for very large areas with low density of users whether they are humans and machines (e.g. Low ARPU regions, wilderness, areas where only highways are located, etc). The key characteristics of this scenario are Macro cells with very large area coverage supporting basic data speeds and voice services, with low to moderate user throughput and low user density.
Urban coverage for massive connection
The urban coverage for massive connection scenario focuses on large cells and continuous coverage to provide mMTC. The key characteristics of this scenario are continuous and ubiquitous coverage in urban areas, with very high connection density of mMTC devices.

Table 1: 5G deployment scenarios

[9] https://www.etsi.org/deliver/etsi_tr/138900_138999/138913/14.02.00_60/tr_138913v140200p.pdf
[10] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2885

2.2 5G Security Threat Ontology / Taxonomy

The innovation of 5G to mobile networks relies on the integration of multiple and different type of technologies. While the integration of technologies significantly improves mobile networks, it drastically increases their attack surface. The risks and threats are not fully documented and mitigated. The threat taxonomy of 5G combines traditional network-based threats with the novel 5G network infrastructure, backward compatibility with insecure legacy 2/3/4G generations and threats introduced with the virtualization of resources.

2.2.1 Taxonomy of Threats

The following list presents a general categorization of threats that target 5G systems. The list is based on the ENISA's threat taxonomy for 5G networks[11].

- Eavesdropping/Interception/Hijacking (EIH): This threat category is defined as "actions aiming to listen, interrupt, or seize control of a third-party communication without consent";
- Damage (DAM): This threat category is defined as intentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness";
- Disaster (DIS): This threat category is defined as "a sudden accident or a natural catastrophe that causes great damage or loss of life";
- Physical Attacks (PA): This threat category is defined as "actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection";
- Outages (OUT): This threat category is defined as "unexpected disruptions of service or decrease in quality falling below a required level.";
- Failures or Malfunctions (FM): This threat category is defined as "Partial or full insufficient functioning of an asset (hardware or software)";
- Nefarious Activity/Abuse (NAA): This threat category is defined as "intended actions that target Information and Communication Technology (ICT) systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target".
- Unintentional Damage (UD): This threat category is defined as unintentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness";
- Legal (LEG): This threat category is defined as "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law".

The threat taxonomy can be further grouped by the location of the exploitation's target in the 5G systems. Based on that criteria the threat taxonomy can be categorized as follows:

- Core Network threats: These threats relate to elements of the Core Network that includes SDN, NVF, Slicing and MANO. The majority fall under the categories of "Nefarious activity/abuse" (NAA) and "Eavesdropping/ Interception/ Hijacking" (EIH);
- Generic threats: These are threats that typically affect any ICT system or network. The generic threats are important to mention since these helps defining and framing the ones specific to 5G. As an example: many 5G specific threats may result in a network service shutdown that in general terms is defined as a Denial of Service (DoS) threat;

[11] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

- Physical Infrastructure threats: These are threats related to the underlying IT infrastructure that supports the network. The majority fall under the categories of "Physical attacks" (PA), "Damage or loss of equipment" (DAM), "Equipment failures or malfunctions" (FM), "Outages" (OUT), "Disaster"(DIS);
- Access network threats: These threats relate to the 5G Radio Access Technology (RAT), radio access network (RAN) and non-3GPP access technologies. These include threats related to the wireless medium and radio transmission technology. Most of the threats fall under the categories of HIJ;
- Multi-edge computing threats: These threats relate to components located at the edge of the network. The majority fall under the categories of NAA and HIJ;
- Virtualisation threats: These are threats related to the virtualisation of the underlying IT infrastructure, network and functions;
- SDN threats: These are threats related to the SDN functions that are omnipresent in the entire 5G infrastructure, including optical and IP transport networks.

This threat taxonomy is further elaborated in the ENISA's report "5G Threat landscape for 5G Networks" [243].

3 Security Requirements of 5G

To realize vertical uses in 5G network environments, exists the need to manage services and application in a dynamic manner. Services and applications will need to be continuously delivered within the expected QoS while in the same time ensure security. To tackle this, it is critical to ensure the accurate elicitation of the security requirements of the 5G vertical domains.

3.1 Requirements in the System's Lifecycle

In the domain of cybersecurity, security requirements are the practice of researching and discovering the security related requirements of a system as elicited by users, customers, and other stakeholders. The elicitation of security requirements is part of the engineering design process. The transformation of the stakeholder desires into security requirements is not an automated process hence, it needs appropriate design to prove valuable for the architectural design of the system (Figure 3). The result of this process needs to be validated against real-world needs.

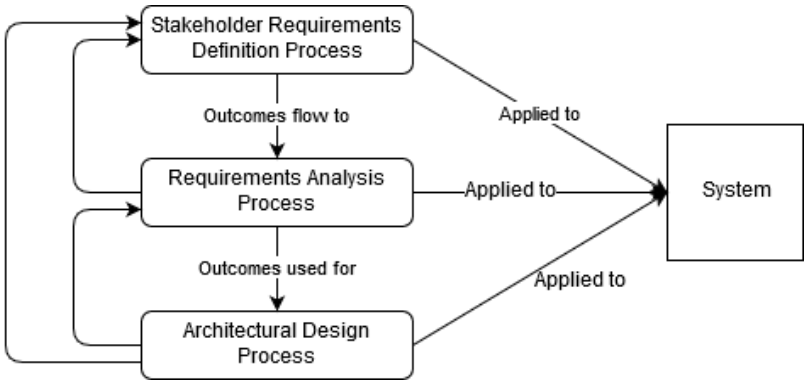

Figure 3: Iterative application of the requirements process.

Requirements play an important role for the entire system's lifecycle, not only at the beginning of the project. During the project, requirements undergo a process of continuously updating, validation and refining. The phases of this process can be summarised as follows:

- **requirements engineering** is concerned with discovering, eliciting, developing, analysing, determining verification methods, validating, communicating, documenting, and managing requirements;
- r**equirements management** elucidates the activities that ensure requirements are identified, documented, maintained, communicated and traced throughout the life cycle of a system, product, or service;
- **requirements traceability** is a document/project management tool that maps the requirements to their origin and traces them throughout the project life cycle;
- **requirements validation** confirmation by examination that requirements (individually and as a set) define the right system as intended by the stakeholders;
- **requirements verification** confirmation by examination that requirements (individually and as a set) are well formed.

3.1.1 Requirement's Syntax

A requirement is a statement which translates or expresses a need and its associated constraints and conditions with the purpose to transform through their analysis the stakeholder, instead of requirement-driven view of desired services into a technical view of a required product that could deliver those services.

There are plenty alternatives of how to express a requirement, however the following syntax was chosen for the current deliverable to focus on a user-centric approach:

[Subject] [Action] [Value]

EXAMPLE: The Invoice System [Subject], shall display pending customer invoices [Action] in ascending order [Value] in which invoices are to be paid.

3.1.2 Types of Requirements

Commonly requirements are grouped in two main types: i) the functional and ii) the non-functional.

- Functional requirements are the fundamental or essential subject matter of the product. They describe what the product must do or what processing actions it is to take, meaning the expected inputs and outputs. Furthermore, functional requirements describe calculations, technical details, data manipulation and processes.
- Non-functional requirements are the properties that the functions must have, such as performance, usability, data security needs. They specify the criteria that can be used to judge the operation of a system, rather than specific behaviours. They are contrasted with functional requirements that define specific behaviour or functions and they are also related to the quality characteristics of the system. According to ISO/IEC 25010[12], the quality characteristics are summarized in Figure 4.

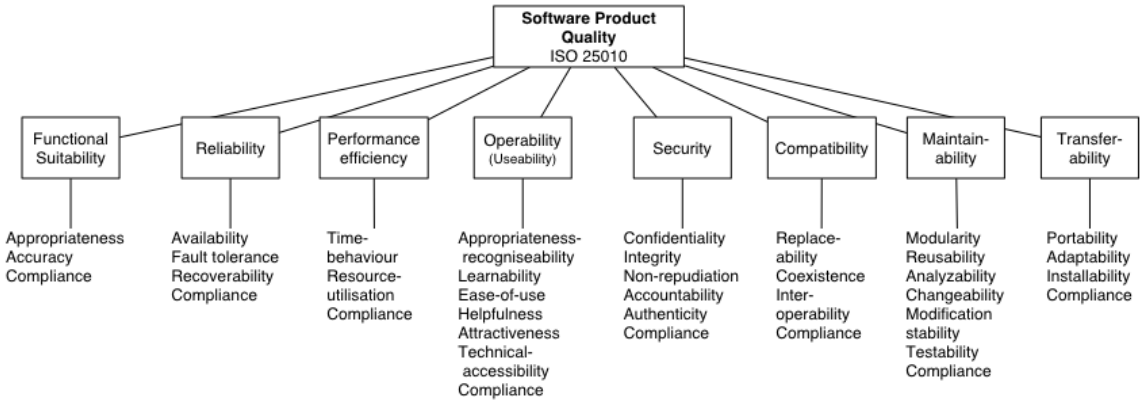

Figure 4: Non-functional requirements (ISO/IEC 25010) & Infrastructure security requirements of 5G[12]12

3.1.3 Security Objectives and Requirements Engineering

Security objectives are goals and constraints that affect the confidentiality, availability and integrity of data and applications. A constraint in this manner is a restriction related to security issues, which can influence the analysis and design of a system under development by restricting some alternative design solution, by conflicting with some of the requirements of the system, or by refining some the system's objectives [17]. Security objectives offer a high-level framework where security analysts can structure their analysis process. During the security analysis process, security analysts elicit the security requirements of the stakeholders. The resulting security requirements are then translated into the security objectives of the system.

[12] https://www.iso.org/standard/35733.html

The degree of success of a software system is the extent to which it meets its intended purpose. The process of discovering that purpose by identifying stakeholders and their needs is the field of requirements engineering [19]. Requirements engineering advocates the identification of Security Requirements in the early stages of product development [18]. The need to use a systematic approach to producing better requirements is highlighted in "Requirements Engineering: A Good Practice Guide" [20]. Some approaches have been developed so far that provide a set of instructions to help identify the security requirements of a developing product. Security engineers use security frameworks to produce *security requirements*. Requirements frameworks can be classified according to their approach to how they are used to model a system from a core concept. Popular approaches are *(1) Goal modelling*: which uses the concept of a *goal* as a core concept [21] and *(2) Threat modelling*: which models how threats are affecting a system [22].

Common Criteria is a security framework that proposes certain steps that once followed will result in a list of the security requirements for the system. Common Criteria is one of the oldest security frameworks, and several other frameworks are built upon it [23]. System Quality Requirements Engineering (SQUARE) develops security requirements by having requirements engineers interact with the stakeholders of the IT project and translating their security goals into security controls [24]. CLASP [25] is another methodology that specifies a set of processes that can be integrated into the software development circle [26]. Secure Tropos is an extension of the Tropos methodology, that aims to incorporate security concerns throughout the development stages [27]. Tropos is an agent-oriented software engineering (AOSE) methodology that covers the whole software development process. Secure Tropos extends Tropos to model and analyse security requirements alongside functional requirements. ModelSec is modelling approach to security, targeting the software engineering field [28].

The National Institute of Standards and Technology (NIST) organization developed a framework for cybersecurity. The main difference with the frameworks mentioned above is that it is based on security standards namely Cobit and SOX [29], instead of system requirements [30]. The framework can be used to design models of a system that complies with security standards. Security Requirements Engineering Process (SREP) used Common Criteria as a basis, trying to improve it by modernizing its components with policies for distributed networks and multiuser ownership. SREP is UML complaint, and the resulting security models evolve along the with the development cycle of the product by performing some activities in each iteration step. Haley proposes a security framework that identifies security goals based on the assets of the system. From the security goal, the security requirements are derived, while they are validated using a process named *satisfaction argument* [31]. Bostrom *et al.* proposes a framework that views security requirements from the agile development perspective while focusing on extreme programming. Microsoft Trustworthy Computing Security Development Lifecycle (TCSDL), identifies security activities that take place in different stages in the development cycle. Compliance with standards is of high importance as are security requirements based on customer satisfaction, especially in industrial settings. A framework proposed in [32] suggests four steps in security analysis that should be performed by the developers instead of requirements engineers. Those are: (1) Identify the security environment and objectives; (2) Determine the threat model; (3) Choose a security policy that includes prioritizing according to the information's sensitivity; (4) Evaluate risk.

In the context of INSPIRE-5Gplus, the methodology that is being used is the NIST cybersecurity framework [253].

3.2 5G vertical domains

The security requirements of mobile networks have evolved with each network iteration, from 3G networks to 4G networks and most recently to 5G networks. 3G mobile networks were the first mobile network that supported security mechanisms such as firewalls and Virtual Private Networks (VPN). 2G networks used a unique ID on the SIM card while in 3G and 4G LTE, used a temporary session ID to limit the chances attackers obtaining them. On the other hand, 5G networks support

virtualized architecture along with SDN, which can greatly improve security by introducing additional layers of security.

In this deliverable we define the vertical domains that the use cases of the project will target. We present a high-level requirements analysis that the use cases targeting each vertical will need to comply with. We define the following vertical domains: 1) energy utilities; 2) vehicular communications; 3) enhanced content delivery; and 4) media production and delivery.

Energy utilities domain

Energy utilities is a novel vertical domain regarding mobile networks. The introduction of 5G technology will unleash a new wave of smart grid features and improve efficiency tenfold by allowing many devices that are currently unconnected, to be monitored for their energy usage. This will allow users to better understand their energy consumption, forecast their needs and avoid unnecessary energy usage and additional bills. On the supplier's management side, they will be able to predict energy peaks, help to support load balancing and avoid waste, allowing them to improve energy distribution which will ultimately result in reduced cost for consumers. The ability to capture all this data using 5G connections will enable larger cities to plan their infrastructure spending, accordingly, resulting in less downtime and higher efficiency. And important point in term of reliability if the investigation of cross dependencies between Energy Grid and 5G Network (Energy suppliers needs 5G network to monitor their infrastructures and 5G Network need energy to run their infrastructure). There are several challenges to be resolved at the interface between these two entities, from sharing information in conformance with RGPD and ePrivacy to level of control/command shared between them.

Vehicular communications domain

Vehicular communications are significant part of 5G applications. They involve multiple use cases, traffic types and communication protocols. Automakers may offer different classes of services to their clients, such as remote maintenance and tele-operated driving. Both require connectivity between the vehicle and the automaker's cloud, although each with completely different service level requirements. In the vehicle, the weak spot is the complexity and vulnerability of current embedded architectures. Virtualization reaching into the vehicle is a major disruption as it becomes a "data-centre on wheels" with system isolation, monitoring, and device management challenges. Data protection is also needed in terms of privacy-by-design for regulatory compliance. A last point is that Stakeholder responsibilities should also be clearly identified and today an overall liability model lacking.

Enhanced content delivery domain

Within the broad variety of services that 5G networks target, there are use cases that requires content delivery to a group of end devices using broadband connectivity over mobile and converged networks. Example of such use cases are live video streaming, mission critical communication, information dissemination in IoT and vehicle to everything (V2X) domains.

Media production and delivery domain

Media production is a major driver for the adoption of 5G networks, with a heavy focus on the Function-as-a-Service (FaaS) technology. FaaS addresses use cases that happen spontaneously and require immediate setup of an elastic communication service. Such an approach aims at overcoming today's limitations posed on traditional broadcast productions by implementing orchestrated mobile content contribution, remote and smart media production, and low-latency and high-bandwidth media distribution (e.g., streaming) over 5G networks.

3.2.1 Description of Security requirements of 5G domains

The following security requirements are derived from our initial security analysis of 5G vertical domains.

Subscriber Authentication: Similarly to 4G, a strong 5G authentication will represent a robust platform upon which operators can develop identity management services: the 5G network operator, acting as an Identity Provider, could thus be responsible for users' identity authenticity towards external partners, providing transparent identification and seamless authentication to Application Services on behalf of the user. The subscriber's identity together with secret data allowing access to a given network shall be stored in a secured physical entity. The data necessary to access an operator network remain the sole ownership of the operator running this network.

The system shall offer the capability to protect 5G customers from common security threats (e.g., impersonation, traffic eavesdropping, etc.,) thus increasing the level of trust that is associated with their network subscribers' identity. Also, the design of security solutions (e.g. key exchange/derivation protocols upon handover or when interworking with other RATs) should provide better secrecy than 4G without sacrificing efficiency.

User Privacy: The 5G system must provide security mechanisms for privacy assurance of a variety of trusted information regarding human as well as machine-users (e.g., identity, subscribed services, location/presence information, mobility patterns, network usage behaviour, commonly invoked applications, etc.).

Beyond Hop-by-Hop Security: 5G architecture can create additional business value by facilitating bearer-independent (e.g., higher-layer) security, and extending to servers on the internet, or extending to device-to-device communications. Any mechanism conceived to realize such bearer-independent security should also be compliant to lawful interception obligations when these are required. Similarly, security mechanisms are needed to fight growing inter-operator fraud and misuse of international signalling networks. 5G roaming signalling protocols must enable the home network to verify that a user is attached to a serving network that claims it is.

Liability: With 5G worldwide deployment, multiple stakeholders with different requirements and security levels will interact and cohabitate in this infrastructure. This new technology relies on complex interconnections of hardware, software, plane levels (e.g. data or control planes) which will defy the appreciation of the stakeholder's liabilities.

As demonstrated by the Y2K bug and United States' "Y2KAct" in 1999 [257], legal liability, torts and insurant play a crucial role in the political management and mitigation of technological breakdowns. With computer systems more and more interweaving with our lives, impacts of such breakdowns will grow and will result in liability and insurance claims. Following the lead of the "Y2k Act", one can expect that in the context of 5G, legal and financial responsibility would have to be distributed proportionately among any liable companies and that the claimants would need solutions to gather proofs of any malfunction or wrongdoing. However, 5G networks are so complex and involve so many actors that it seems extremely difficult to determine the liability perimeter of each actor and to gather evidence.

Today, there is no solution addressing this issue as a whole. Several technologies such as Root Cause Analysis, Remote Attestation, Path Proofs, component labelling or attack graphs propose solutions for different aspects of this issue. They need to be enhanced and brought together in order to build the first bricks of a trust and liability system.

Network Security: Network security of 5G systems require additional resources for robust security due to their interoperability with devices from different domains. With the massive penetration of IP protocols for control and user plane in all network functions, with the diffusion of low-cost MTC devices or smartphones where mobile malware could be easily propagated, the operator's 5G core and radio networks could become more vulnerable. The following requirements highlight areas for improvements, with respect to LTE/LTE-Advanced (4G) security:

- Improve resilience and availability of the network against signalling-based threats, including overload caused in a maliciously or unexpectedly manner;

- Specific security design for use cases which require extremely low latency (including the latency of initiating communications);
- Comply with security requirements that are defined in 4G 3GPP standards. This will apply especially to a virtualised implementation of the network (virtual appliance, hypervisor);
- In the context of Public Safety and Mission Critical Communications, it is expected that 5G technology will allow reduction of cost and improvement of functionality of these networks. Besides supporting emergency communications, the 5G commercial system should be able to provide basic security functions in emergency situations, when part of the network infrastructure, including the security infrastructure, may be destroyed or inaccessible. The security services should be able to provide protection against malicious attacks that may intend to disrupt the network operation and allow the secure implementation and deployment of essential infrastructure;
- Improve system robustness against smart jamming attacks of the radio signals and channels;
- Improve security of 5G small cell nodes, taking into consideration their geographical distribution and their easy accessibility.

An initial set of INSPIRE-5Gplus high-level security requirements is shown in Table 2. The security requirements are elicited from the Inspire-5Gplus architecture:

Security Requirement No.	Requirement
SEC-REQ-01	The 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system.
SEC-REQ-02	The 5G network shall only allow authenticated users to consume the services provided by the 5G system.
SEC-REQ-03	The 5G network shall warrant measurable level of availability of its services to the relevant stakeholders.
SEC-REQ-04	The 5G network shall ensure the necessary network capacity and network resources necessary for the critical operations of the 5G services.
SEC-REQ-05	The 5G network shall enable a secure platform for vertical services to be deployed.
SEC-REQ-06	The 5G network shall enable the state management of its platform components.
SEC-REQ-07	The 5G network shall be able to revert to previous states with minimal service disruption of deployed application in case of malicious compromise.
SEC-REQ-8	The 5G network's security mechanisms should not impact the functional requirements of critical operations for vertical applications.
SEC-REQ-9	The security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality.
SEC-REQ-10	The security mechanisms of the 5G network shall be able to measure/evaluate trust level of its components and platforms and share this information with verticals in a safe and trustable way.
SEC-REQ-11	The security mechanisms used in a complex 5G eco-system shall be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.
SEC-REQ-12	The 5G eco-system shall be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.
SEC-REQ-13	Technologies used to distribute over 5G eco-system (end to end) and evaluate post security incident root cause of failure are trustable.

SEC-REQ-14	The 5G system must provide security mechanisms to ensure that user (and endpoints) data are securely processed and stored wherever it is processed or stored. Both confidentiality and integrity guaranties shall be brought all along the full lifecycle of the data in transit, process and storage.

Table 2: INSPIRE-5Gplus Security Requirements

The initial list of high-level security requirements will be revisited, refined and fully detailed in subsequent deliverable, D2.2 Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security which is due on M18.

3.3 Stakeholders' security requirements of 5G

The established process for eliciting requirements from stakeholders is through interviews and meetings. To gather the requirements from the stakeholders in INSPIRE-5Gplus, the consortium developed a questionnaire and distributed it among the relevant stakeholders. The questionnaire is comprised by 12 questions. The questions have been divided into three categories: business and organisational; regulatory compliance and repudiation; and other aspects.

The survey has been disseminated to stakeholders with expertise into 5G services. These stakeholders will highlight some key requirements and needs that 5G security enablers need to fulfil. The results of the survey will be presented in the D2.2 (Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security), which is due on M18.

The questionnaire can be found in Appendix C. Questionnaire.

4 Current Security Status of 5G

4.1 State of the Art Solutions

In this section, we present the state of the art of the current security solutions in 5G which are largely applicable to softwarized, cognitive and service-based future networks. The solutions/schemes are organized into three groups, namely Infrastructure/Platform, Management/Automation and Service/Vertical Level. Although some presented solutions may serve multiple domains (i.e. are cross-cutting domains); in our classification, we describe them in the most relevant subsection. The description of State of the Art (SotA) is optimized with respect to INSPIRE-5Gplus scope for the sake of brevity. In other words, the SotA description is neither mutually exclusive nor collectively exhaustive. Moreover, for a very detailed description of related work and solutions, the reader is referred to comprehensive surveys published in the literature where appropriate. In Table 3, we summarize our approach on how the multifaceted 5G security is treated in this section.

Segment	Rationale	Specific SotA elements
Infrastructure/Platform Level	Focus on core 5G technologies for 5G networks (e.g. SDN or NFV security)	RAN, network softwarisation, MEC domain, Trusted Execution Environment (TEE) as an enabler in the infrastructure
Management/Automation Level	Soft techniques and enablers, more generally applicable impacting general ICT security (e.g. AI/ML security)	Zero touch Service Management (ZSM), DLT, trust and liability, cyber threat intelligence, security via AI/ML and security for AI/ML
Service/Vertical Level	Service and end user perspectives, verticals, use-case driven security solutions	Verticals, services, IoT as a key service domain

Table 3: The organization of SotA analysis for 5G security

4.1.1 Infrastructure/Platform Level

This subsection is divided in three parts. The first part describes the secure 5G radio access; the second part details the security of softwarised network and slides; and the third part describes the security of Trusted Execution Environments (TEE).

4.1.1.1 Secure 5G radio access

For secure 5G radio access, efficient and robust key management and AAA (Authentication, Authorization and Accounting) functionalities are important. The security functions in this domain has the main purpose of enabling a user device to authenticate and access the network securely. 5G design and specifications have considered 4G security limitations such as security architectural deficiencies, weak home control, user privacy leakage and radio interface risks, and set out to overcome those challenges for secure 5G access network security [34]. New vertical industries and their mMTC and URLLC based applications also complicate the security landscape in the radio access network. Moreover, the attack resistance of radio networks is a key design consideration in 5G, analysing threats such as Distributed Denial of Service (DDoS) from potentially misbehaving devices and adding mitigation measures to radio protocol design. These challenges are exacerbated with the evolved threat landscape and new capabilities that provide users with low-cost alternatives to

program their own devices (even at radio access level).

AAA in 5G radio network: 3GPP introduces two 5G authentication processes, e.g. the primary authentication and the secondary authentication at release 15 [35]. The primary authentication is used to establish the trust between UE and network, which is similar to that of the 4G system. The primary authentication method can be 5G AKA Authentication and Key Agreement (AKA) or Extensible Authentication Protocol - AKA (EAP-AKA). Depending on the requirement of the 3rd party service providers, the secondary authentication may be performed between the UE and the (Data Network - AAA (DN-AAA) server in the external data network. The secondary authentication is used to establish trust between UE and the external data network.

The Application System (AS) level signalling data protection is provided by UE and Next Generation NodeB (gNB) at Packet Data Convergence Protocol (PDCP) layer. As for user plane data security protection, in contrast to 4G with only confidentiality protection, both confidentiality and integrity protections between 5G gNB and UE can be activated. Despite integrity and replay protection for signalling traffic is mandatory, the integrity protection for the user plane between UE and gNB is optional because it increases the overhead of the packet size, and the packet processing load and time.

Key management: 5G radio access contains a new set of technologies or tighter integration of advanced techniques considered in 4G such as Device to Device (D2D) communications, full-duplex communications, ultra-dense Heterogeneous Networks (HetNets) and 5G New Radio (NR). For D2D communications security [36], key management is a challenging issue since key agreement between mobile devices in dynamic groups need to be scalable. For that purpose, in addition to conventional key management techniques, physical layer based key generation techniques can be used. Another issue is the security of the 5G radio in idle mode. Radio Resource Control (RRC) idle mode in 4G had various limitations. To address those, the public-private key can be introduced in 5G BS and UE allowing 5G UE in RRC idle mode validate the authenticity of received system information. 5G NR with full-duplex communications also opens new attack surfaces and potential threats.

Open Questions: In addition to confidentiality-targeted cryptographic protection, protection against modifying or injecting user plane traffic is a critical requirement [37]. For instance, with 5G verticals such as industrial IoT or mission-critical use cases, the integrity protection becomes much more important. Similarly, physical layer techniques and scalable security as also mentioned in Section 4.1.3 are important research directions.

4.1.1.2 Security of softwarised network and slices

4.1.1.2.1 NFVI, VNF, MANO and interface security

Softwarisation technologies (e.g., SDN, NFV) are key enablers for fully automated security management systems in next-generation networks, thanks to their flexibility and dynamism. However, NFV and SDN elements themselves may become malicious causing performance degradation or even network outage [38]. According to Microsoft's STRIDE model, threats against SDN are categorized into six categories: spoofing, tampering, repudiation, information disclosure, DoS, and privilege escalation [39]. On the other side, ETSI has identified the threat surface of NFV as the union of generic virtualisation threats (memory leakage, interrupt isolation, etc.), generic networking threats (flooding attacks, routing security, etc.), and the threats due to combining virtualisation technology with networking [40]. Thus, new methods and mechanisms to build and assess the trustworthiness of software components (e.g., VNFs, micro-services, etc.) along their lifecycle across multi-domains are needed.

VNF software security and remote attestation. An important security challenge comes from softwarisation itself: VNFs are subject to software vulnerabilities including both implementation and design flaws as software constructs. Moreover, the promised flexibility and openness of service environment via VNFs raises security concerns since data and NFV software are not directly controlled by the more risk-aware enterprises due to introspection risk by a malicious actor with a total control on the execution environment entailing memory, storage and processing elements.

Several techniques [41] have been proposed to ensure software (code and data) confidentiality and/or integrity in cloud platforms. ETSI suggests leveraging Hardware Security Module (HSM), Trusted Platform Module (TPM) and virtual TPM (vTPM) to provide trusted protection for VNFs. These modules are used to shelter integrity measurements (i.e., hash values), cryptographic keys and certificates that are required to empower remote attestation of VNF components. Indeed, remote attestation guarantees the integrity of VNF instances at load time. TEE is an important enabler for that goal as described in Section 5.2. Nevertheless, it fails to prevent introspection risk [42], where an attacker (e.g.; supplier that have install some Trojan in its VNF supply to attack others co-hosted VNF) aims to break the confidentiality and integrity of a software (code + data) once it is launched. Software obfuscation [43][44] is a software protection technique based on the concept of security by obscurity, which applies transformations to code in order to make it more complex to analysis and tampering, while preserving its functionality. However, obfuscation does not guarantee its integrity and confidentiality. Moreover, it results in performance losses incurred by obfuscating transformations. Tamper-proofing techniques enable software integrity preservation through causing an altered software to fail. Nevertheless, these techniques can be defeated by an advanced attacker (e.g.,[45]). Fully Homomorphic Encryption (FHE) [46] guarantees data integrity by performing computations directly on encrypted data. The major drawback of FHE is its impractical use due to its computation overhead.

Formal Methods. Several formal methods and tools (e.g., model-based specification [47], Abstract State Machines [48], Model Checking[49], and Automated Theorem Provers [50]) have been proposed to deal with software and system reliability. Basile et al. [51] proposed a geometric model to assess the correct enforcement of network authorization policies based on reachability analysis. The reachability queries are expressed in Structured Reachability Query Language (SRQL). Panda et al. [52] used Z3 SMT solver [53] to verify isolation properties in networks that contains virtual or physical middleboxes (e.g., firewalls). Spinoso et al. [54] generalized the approach to formally verify VNF chains modelled as network function forwarding graphs. Flittner et al. [55] proposed ChainGuard; a tool to verify Service Function Chaining (SFC) by detecting if the actual SFC overlay and traffic steering complies with the SFC configuration.

Existing formal methods and tools to model, verify and validate the efficiency and correctness of the infrastructure and envisioned security solutions need to be extended and adapted to reflect the new requirements of trust management in multi-tenant/multi-domain environments with the integration of new enablers such as Distributed AI. For instance, how to verify the valid operation of a multi-VNF security implementation comprising distributed AI is an open question.

4.1.1.2.2 SDN security, SD-SEC and SECaaS

As physical and software resources involved in management tasks and belonging to different administrative domains can be compromised by both insider and outsider attackers, security question it is required further exploration to protect those assets and make fully autonomous management in a secured way a reality. Software-defined security (SD-SEC) models enabling security-as-a-service (SECaaS) delivery models are vital to support cost-effective and agile security reinforcement in fully virtualised infrastructure [57]. In that regard, network softwarisation becomes a security facilitator (security via softwarisation) in contrast to security for network softwarisation described in Section 4.1.1.2.1. The contribution in [56] proposes an architecture that takes advantage of SDN/NFV capabilities to empower SECaaS in inter-domain environments. The proposed architecture focuses on enforcing security within 5G slices by enabling predictive auto-scaling of Virtual Security Functions (VSFs) according to the predefined policies and the VSFs' performance metrics. Authors in [57] devised a security architecture that supports network slice management with built-in security features leveraging on SD-SEC and SECaaS mechanisms. The architecture enables per-tenant security enforcement in a multi-tenant, multi-provider infrastructure with dynamic placement and chaining of network security functions. Similarly, Xu et al. propose a hierarchical centralized software defined security scheme based on SDN environment, which implements the pooling of the security resources in [58]. It combines SDN controller with the coordination work of security Application Publishing Protocol (APP), security controller and security devices for attack

detection and then according to the security policy, it provides analysis and rapid response to protect the network. In [59], Farahmandian et al. introduce a software-defined security service (SDS_2) for protecting cloud infrastructures. SDS_2 focuses on defining security concerns regarding physical and virtual boundaries of data, resources, tenants and detecting security breaches through violations of boundaries, which are defined by security policies and security violations by attackers.

However, contributions made so far were limited to a single domain and/or partially covered the whole cybersecurity spectrum (i.e., Identify, Protect, Detect, Respond and Recover). Thus, advanced SD-SEC models, leveraging on flexibility and dynamism provided by virtualization (NFV) and programmability (SDN), are required to cover the whole cybersecurity spectrum in a multi-domain/multi-tenant environment. Besides, network programmability enables the end-to-end orchestration of the network and its resources, namely, micro-services, VNF, etc., following the security-policies defined for protecting the architecture and its tenants [60].

4.1.1.2.3 MEC security

MEC is an integral part of 5G networks. MEC itself needs to ensure as well as provide an environment in where a multi-tiered security framework can be constructed starting from the edge network [61]. The high concentration of data information leaves the cloud highly susceptible to violent attacks, and data offloaded to the cloud through wireless environments can be compromised in terms of confidentiality. MEC can be collocated with different heterogeneous network elements, thus making the application of conventional privacy and security mechanisms for theses ystems non-trivial. This situation asks for orchestration of diverse security solutions from the edge to the core cloud functions [62]. It is possible that a large-scale edge computing system can be severely affected by the security threats of just a network component. The inherent task offloading over wireless channels may not be secure since confidentiality may be compromised, and computation tasks can be overheard by malicious eavesdroppers [63]. Finally, data exchange and computational burden of securing MEC and MEC-resident security functions should be minimized considering the characteristics of MEC environment [64][65].

The transfer of compute-intensive applications can be secured by encryption at the user side and decryption at the destination server side. This, however, can increase the propagation delay as well as execution delay, thus reducing the application performance [66]. Physical layer security and blockchain have emerged as effective solutions to secure MEC systems [67][68]. Finally, the sharing of the same storage and computation resources among multiple mobile users raises issues of private data leakage and loss. Recently, ML-based security and privacy in MEC have been studied from various perspectives. The use of ML for cyber-attack detection in edge networks was considered in [69], where the experiments demonstrate that the DL based model is better than that with shallow model in terms of learning accuracy, detection rate, and false alarm rate.

In addition to security of MEC using security functions, i.e., addressing increased attack surface and diversified threats, there are also questions related to feasibility and practicality of MEC-resident security solutions. One open question is related to resource-efficient security solutions in MEC based on security requirements and application/vertical scenarios. There are also research challenges regarding enablers in MEC environment such as distributed AI/ML or overhead of distributed ledger-based solutions.

4.1.1.3 TEE secured multitenant virtualised networks

A key design rationale of 5G architecture is to have multitenant virtualised infrastructure serving different vertical use cases and operators. TEEs, i.e. secure zones, integrity-protected processing environment, consisting of processing, memory and storage capabilities [70]. These environments, in suitable network elements, are crucial to protect sensitive material such as keys and prevent unauthorized access to, and manipulation of VNFs, applications or sensitive data. This is more important when we have multi-tenant networks where disparate service providers utilized a shared resource pool, i.e. physical and virtual systems for providing 5G services.

To overcome limitations of software-only based techniques mentioned in other sections, TEEs (e.g.,

Intel's Software Guard Extensions (SGX) [71], AMD's Secure Encrypted Virtualisation (SEV) [72]) are recognized as a best practice guaranteeing higher security and trust for software while minimizing impact on performance. TEEs are hardware-based solutions that have been specifically designed for providing total integrity and confidentiality even in adverse conditions in presence of a high privileged malicious operator or even a malicious kernel. Schuster et al.[73] proposed Verifiable Confidentiality Cloud Computing (VC3), an SGX-based MapReduce framework that enables trustworthy data analytics in untrusted cloud environment. S-NFV [74] relies on Intel SGX's isolation feature to enforce integrity and confidentiality of VNF states and the code accessing these states. The first prototype TruSDN [77] relies on Intel's SGX enclaves to provide isolation and allow remote integrity attestation of virtual switches to establish bootstrapping trust in virtual switches and VNFs prior to their deployment. Like VC3 and S-NFV, TruSDN is implemented using an SGX emulator, namely OpenSGX [78], rather than real hardware. The second work by Paladi et al. [79] provides integrity attestation of VNFs running in Docker containers, leveraging Linux Integrity Measurement Architecture (IMA) [80] to collect integrity measurements of security-critical Docker assets and Intel's SGX TEE running a trust agent to verify their integrity. Since TEEs are native to processor architecture, application portability between different TEEs is hindered. To overcome this limitation, Lefebvre et al. [79] defined a conceptual blueprint of a TEE versatile solution that bridges both Intel SGX and AMD SEV TEEs by use of code interpretation. While code interpretation enables portability feature between TEE implementations, it may come with performance degradation. TEEshift [79] is a tool suite that enforces code's confidentiality and integrity by shifting selected functions into TEEs. TEEshift relies on Google's Asylo framework to support different TEEs and consequently provide platform independence.

TEEs are instrumental for mitigating various security related issues such as introspection and supporting both security and trustworthiness of VNFs. However, the adoption of TEEs is challenged by being processor-bounded and by their relatively complex use and performance overhead. Thus, new mechanisms are needed to ease their use and agile integration in highly dynamic virtual environments with minimal impact on performance. Generally applicable solutions are desired to avoid technology lock-ins and enjoy economies of scale.

4.1.2 Management/Automation Level

4.1.2.1 Automated network security management and solutions exploiting ZSM paradigm

The foreseen increased complexity in operating and managing next generation networks has stimulated the current trend toward closed-loop automation of network and service management operations in these networks. The aim is to enable end-to-end (E2E) smart and fully automated network and service management. To this end, ETSI established the Zero Touch network and Service Management Industry Specification Group (ZSM ISG). The ZSM framework is envisaged as a next-generation management system that aims to have all operational processes and tasks (e.g., planning and design, delivery, deployment, provisioning, monitoring and optimization) executed automatically, ideally with 100% automation and without human intervention. Thus, machines will be able to learn and take decisions on behalf of human beings. ZSM relies on SDN and NFV capabilities and builds on the premise of fully automated network management in 5G systems. This paradigm also has an impact on security solutions and management in 5G networks.

Since ZSM is a specification in progress, the solutions exploiting ZSM can be basically interpreted as security solutions which employ closed-loop and automated security functions (prevention, detection, countermeasures) in softwarised networks. Such schemes evidently rely on smart and self-driven mechanisms to attain those goals. Therefore, there is an implicit connection to AI/ML driven techniques in Section 4.1.2.5. However, there is still a wide gap in terms of theory and practice regarding the deployment of E2E closed-loop solutions in the SotA security solutions for 5G networks.

ZSM provides a blueprint for implementing E2E closed-loop automated network management. However, the availability and injection of enablers in the 5G infrastructure are practical issues. There

is also “the calamity of over-arching solutions”, where the proposed architecture becomes too big and complex to be practical. Therefore, minimal viable implementations of ZSM should be pursued for beneficial security scenarios, i.e. providing the most protection gains.

4.1.2.2 DLT based solutions in 5G Security

DLT based solutions in 5G (Beyond 5G) exploit the key attributes of DLT, namely decentralization, immutability and transparency and availability. Specifically,

- **Decentralized security management structures:** The decentralized blockchain-based network management will provide better resource management and more efficient system management [81]. Rodrigues et al. [82] presented a DDoS prevention mechanism with the support of blockchain. Sharma et al. [83] proposed the applicability of blockchain and SDN for the enforcement of significant security services including DDoS attack prevention, data protection, and access control
- **Authentication, Authorization and Accounting (AAA)**: When massive scale connectivity with heterogeneous and fragmented network elements are in place in 5G networks, AAA functions need to be decentralised and much more robust for service continuity [84]. For instance, (group) key management and access control mechanisms can be offloaded to blockchain platforms for better scalability (especially for resource-constrained end points) and transparency. Yang et al. [84] presented blockchain based authentication and access control mechanisms for cloud radio over fibber network in 5G.
- **Service Level Agreement (SLA) management:** 5G networks build on virtualised and sliced network architecture. Moreover, these networks are expected to serve a very wide spectrum of use cases with diverse service level guarantees. Therefore, SLA management is an important system requirement. Blockchains may enable decentralized and secure SLA management in this complex setting.

The most apparent implications in 5G security emerges in different enablers and solutions based on these attributes. Such cross-cutting integration is evident in the following security goals:

- Securing AI/ML [85]
- Secure and trusted decentralized resource management [86]
- Secure data sharing, e.g. in IoT or MEC [87]

In the context of multi-operator composition, there are some lines in which DLT can play a key role. Smart contracts can be applied to 5G to help with the deployment, expansion and in general providing with an extra security layer. If an operator cell expansion is registered in the DLT while in the multiparty, third parties can check the trustiness of other party cells. DLT can help in detecting and avoiding attacks addressed to the IoT devices connected to the 5G network. Taking into account that 5G will manage these IoT devices by some kind of trusted intermediary centralized operators the DLT, will help operators with the device authentication tasks through the use of Smart Contracts. These pieces of code could handle multiple operations in terms of validating data, identities, or behaviour of the IoT devices. In that sense, the trustiness between operators is increased.

DLT can solve end to end performance issues in multi-operator scenarios serving as a conflict resolution mechanism between devices with transaction problems or smart contract conditions. But where the main achievements can be reached in multi-operator environments using DLT may introduce transparency in higher level operations by defining smart contracts that in the end are auditable and can be trusted, therefore reducing the time from concept to business.

4.1.2.3 Trust models and liability analysis in 5G

Trust models and mechanisms in 5G: According to NIST [88], trust is defined as “the belief that an entity will behave in a predictable manner in specified circumstances.” It is related to the risk of encountering behaviour that is unexpected and, potentially, damaging to the goals of the system in

question [89]. Trust is often derived from certain feedback ratings through experience and trust aggregation. There is a need for robust and effective trust management in 5G networks since it is a multi-tenant, heterogeneous and service-based system. Moreover, different security problems result in different requirements to the design of trust management [90]. There has been trust modelling and management related solutions in different network technologies including softwarised networks. In [91], Artych et al. proposed a security enabler to process technical information present in the network in order to provide trustworthiness information that can facilitate necessary trust decisions. In [92], Fan et al. presented alternative designs of decentralised trust management and their efficiency and robustness from threat models, trust metrics and trust aggregation methods perspectives. Those can be utilized in 5G context.

Liability: Although efficient mechanisms to build trust in a 5G ecosystem (for AI/ML mechanisms or softwarized services or networking) can be adopted and put into effect, that does not automatically result in prevention of its breaches and failures since they might be compromised as well. There are also unseen zero-day vulnerabilities and attacks. Identifying the responsibility of agents in the case of violations is a fundamental part of security and it is critical to the determination of liability and sanctions [93]. Therefore, how to identify liability and responsibility for failures of systems themselves or the provided security schemes needs to be addressed. Trust with liability is a new, yet important concept that needs to be empowered to ensure end-to-end delivery of 5G services in trustable as well as liable way. The liability assertions should also be devised in a provable way to have genuine validity. In fact, liability and liability management is a relatively new area in security research. In cloud technologies, security researchers have provided accountability mechanisms [94], investigated the concept of forwarding accountability [95], and established that accountability is not a sufficient condition for trust and proposed the concept of strong accountability to improve trustworthiness [96]. A specific language [97] has been proposed to express accountability rules close to sentences in laws, data directives and contracts (human readable), but with some limitation. Regarding responsibility and concept of responsibilities delegation, some interesting works have investigated issues with delegation of obligation [98][99] but without addressing issues of responsibilities delegation [100]. Ghorbel et al. [100] investigated the difference between functional responsibility and liability, with an application of their framework to software contracts and responsibilities for defective software. Authors in [101] addressed the security challenges specific of Critical Information Infrastructures (CII) by proposing PolyOrBAC; a collaborative access control framework that provided each organization taking part in the CII the capacity of collaborating with the other organizations, while maintaining a control on its own resources and on its own internal security policy. Olaleye et al. in [102] provide a good legal panorama regarding algorithm liability based on real disputes. Liability issues arising from the use of AI has also been investigated. Karnow [103] proposed the “Turing Registry” framework to address liability issue for Distributed Artificial Intelligence (DAI). Kingston [104] discussed the criminal liability for AI-driven system. For more details on algorithm liability concerns due to use of AI and ML, please refer to Section 4.1.2.5.

Proof of Transit (POT): Another important aspect of security in 5G networks is proof of traffic isolation or processing points. Furthermore, regulatory obligations or a compliance policy require operators to prove that all packets that are supposed to follow a specific path are indeed being forwarded across and exact set of pre-determined nodes [105]. Solutions that provide "proof of transit" for packets traversing a specific path are investigated for that purpose. The method relies on adding POT data to all packets that traverse a path. The added POT data allows a verifier node (potentially, an egress node) to check whether a packet traversed the identified set of nodes on a path as expected or not. In the proposed scheme, security mechanisms are natively built into the generation of the POT data to protect against misuse and compromises (e.g., configuration mistakes). The underlying mechanism for POT leverages "Shamir's Secret Sharing" scheme [106].

Open questions: Farris et.al. [224] highlight various challenges for future research in the domain of SDN and NFV-based security frameworks. They show that the management of security in slices will be challenged by 1) the heterogeneous nature of objects to be considered (VNFs, IOTs), 2) the need to secure the data and the control plan and by the potential high number of slice components. In this

context, new models and tools are required to manage the granularity of security requirements, rules, security measures and the optimization of placement of security solutions within a slice. A complementary challenge for trust and liability management systems is the ability of identifying, defining and characterizing what are the expected behaviour, duty or needs of a slice component. Existing approaches such as MUD profiles [225] exist for IoT devices but cover only behaviour definition and are not applicable to VNFs for example.

Regarding the Proof of Transit, one of its limitations is that it does not prove the exact path that transmitted the packet. For certain VNFs or IoT objects which have distinct behaviours, a proof of transit could be an identification means and open the opportunity for fingerprinting attacks. Finally, managing the scalability or the granularity requires new models and tools.

4.1.2.4 Threat intelligence solutions supporting security management

Threat intelligence (TI) is the recognition of prevailing or emerging malicious activities. For that purpose, ICT systems generate the security knowledge base by associating different threat feeds and thereby forming their security analytics. In addition, cyber-security vendors establish common languages and standards to rationalize and standardize the delivery of the available threat feeds [107].

Threat Intelligence is a critical enabler for any effective 5G security strategy. As the security solutions gear towards more cognitive and smart capabilities, the crucial actionable intelligence relies on data gathered from a diverse set of sources (especially across boundaries) in a timely and efficient manner (scalability and feasibility). Furthermore, TI enables security management to identify which vulnerabilities are actively being exploited. As a result, security management can prioritize their resources based on risk and circumstances. Therefore, 5G system operators should try to get intelligence from the widest range of sources possible, i.e. from peer operators, edge devices, open-source intelligence (OSINT) and different segments of the networks [108]. This activity requires participation in threat intelligence partnerships with other operators and sharing information such as suspect device information or suspicious large-scale traffic activities (e.g. IoT botnets)[109].

Since TI is an enabler for security monitoring and more effective security management, situational awareness can be acquired through adoption of threat intelligence platforms such as MISP - Open Source Threat Intelligence Platform and open standards for threat information sharing [110]. However, the integration of cyber threat intelligence (especially OSINT) still requires more attention since 5G is integral part of the Internet.

Evaluation & quantification of risks in ICT systems.

The current state of the art includes multiple contributions to evaluate and quantify risks in ICT systems. Among the models that exist in the literature, one can mention the attack graphs [226][227] and dependency graphs [228][229]. The formers rely on graph theory to describe how existing exploits may be chained to get root access to a system (also called an *attack path*). This kind of mathematical model offers several advantages such as providing a compact way to express the different possible attack scenarios on a system. Furthermore, the use of a graph offers a rather intuitive support for justifying the provided countermeasures or assessment measures to non-experts.

Regarding the dependency graphs, they are also based on graph theory and aim at modelling the inter-dependencies of the different components of a system. These types of graphs are mostly used to decide what would be the best answer against ongoing attacks, while attack graphs are used to give a risk assessment measure of the system.

Open Questions: Most of these approaches consist of static models build during the design phase and do not consider threats that could occur during the lifecycle of a system. In order to cope with this issue, a new risk assessment framework to supervise the state of complex ICT systems has been proposed in [230]. The concept of the Risk Assessment Graphs (RAGs) and a quantitative risk evaluation approach have been developed.

Finally, it is worth mentioning that the moving target defence (MTD) [231] framework, is a recent paradigm that aims to broke the static nature of ICT systems by making them dynamic. Indeed, nowadays networks are static, and a potential hacker has plenty of time to study the system and discover its vulnerabilities. In the context of 5G networks and slicing, the task of making the system dynamic is even more complex because it must be flexible enough to encompass the countless number of ways that slices can be deployed. One technical lock with this kind of approach is to define an MTD procedure that is robust with respect to network slicing.

4.1.2.5 ML/AI driven security frameworks

ML/AI driven solutions, a "toolbox" which can impact other discussed elements: data analytics for threat intelligence, enabler of ZSM for security, countermeasure selection and enforcement for agile security. In other words, AI plays an important role in enabling security self-managing functionalities, resulting in improved robustness and lower operational costs. To achieve autonomic security management, recent academic research contributions [111][112] and Software Defined Operations (SDO) initiatives such as the one proposed in [113] have been working on the development of AI-driven SD-SEC solutions that are able to intelligently empower key security functions (e.g., prediction, detection, mitigation, etc.). In [113], an anomaly detection system is devised to spot cyberthreats in 5G networks based on deep learning techniques, particularly Deep Belief Networks (DBN), Stacked Auto-Encoders (SAE) and Long Short-Term Memory (LSTM). The anomaly detection is achieved in two stages: Anomaly Symptoms Detection (ASD) and Network Anomaly Detection (NAD). The ASD module, deployed at Radio Access Network (RAN) level, focuses on quick detection of anomaly symptoms by analysing network flows using DBN and SAE. Meanwhile, the NAD module, located at Core Network (CN) level, uses a LSTM Recurrent Network to identify temporal patterns of cyberattacks based on collected symptoms. Authors in [111][112] proposed an anomaly detection and diagnosis solution for RANs self-healing in 5G networks. The anomaly diagnosis process relies on Case-Based Reasoning (CBR), transfer learning and active learning techniques to allow for autonomous self-healing actions.

Despite the growing interest, the integration of AI techniques in SD-SEC models to empower self-managing security operations is still in its infancy, relying on basic ML algorithms and/or targeting single domain. Hence, further developments are required to provide smart and closed-loop end-to-end security enforcement for 5G and beyond networks in near real-time. Emerging AI/ML techniques, namely deep Learning, distributed learning, transfer learning, federated learning, and outputs of SDOs initiatives focusing on enabling intelligent mechanisms in future networks, and empowering zero touch management (e.g., ETSI ZSM) can be leveraged to build up advanced smart AI-driven SD-SEC solutions that enable fully autonomous, proactive and sustainable cybersecurity management and that cover the whole cybersecurity spectrum while fulfilling the Service Level Agreement (SLA) requirements.

4.1.2.6 MTD and Cyber Mimic Defence Techniques

Moving Target Defence (MTD): MTD aims at modifying (parts of) the infrastructure or their fingerprint to make it hard for an attacker to execute precision strikes on specific vulnerabilities [114]. Such parts could be the network (e.g., its topology to make eavesdropping on specific traffic difficult), technology stack (e.g., the network equipment that processes a packet to make it hard for an attacker to execute precision strikes on specific vulnerabilities), execution environment (e.g., randomize the underlying VM technology on which a certain service runs when an instance is started) or the software (e.g., use different implementations of the same functionality). For instance, OpenFlow random host mutation (RHM) [115] is the moving target defence technology based on OpenFlow. OpenFlow RHM can complete transformation between the real IP address (rIP) and virtual IP address (vIP) of a host in a fixed time interval at a high frequency, while maintaining a high unpredictability.

Cyber Mimic Defence (CMD): Cyber Mimic Defence is a concept [116] based on Dynamic Heterogeneous Redundancy Architecture (DHR). DHR is a concept from reliability engineering which makes use of dissimilar redundancy structures (DRS) to make sure that faults/problems that exist in

only one of them (regarding a certain input/state) can be detected. Cyber Mimic Defence takes this concept and extends it to the domain of cyber security. However, for now, it has not yet been investigated what applying such a concept in the real world would mean in terms of 1) resources/complexity; 2) cost/benefit, and therefore for which security levels/requirements it could be beneficial; 3) protocols/standards required to make CMD an inherent future at different 5G infrastructure levels (e.g., platform, management, services) and more.

MTD and CMD are promising techniques. However, their integration into 5G based on ZSM architecture and optimization regarding cost-benefit trade-offs are open research questions. For multi-tenant systems and cross-slice scenarios, these techniques may cause a lot of complexity in network management and security operation. AI-controlled schemes and softwarization-induced capabilities are worthwhile research directions.

4.1.3 Service/Vertical Level

The softwarization in 5G and new service delivery models require new security solutions Apparently, the use of clouds and virtualization emphasizes the dependency on secure software and leads to other effects on security. When operators host third-party applications in their telecom clouds, executing on the same hardware as native telecom services, there are increased demands on virtualization with strong isolation properties. This is also applicable to the network side where traffic (data and control) needs to be isolated to the extent possible to enforce security requirements.

4.1.3.1 Security solutions oriented towards verticals

5G has significant security challenges for envisaged verticals in the specifications [117]. First, there is the changing trust and threat models. In addition to slice-specific threats and trust models, there are cases such as Operational Technology (OT) industries where non-public network with varying degrees of isolation and a multitude of end point types and owners are also part of the vertical. In verticals, existence of separate hardware roots of trust for connectivity and applications increase the scalability challenge. Moreover, securing high-risk, low-resource massive IoT deployments is extremely challenging for scalability since mMTC is a key network mode in 5G services and verticals. Finally, network slicing and virtualization has security peculiarities. Network slicing is essential for facilitating verticals as well as addressing isolation scenarios for security and performance requirements. In that regard, effective slice security mechanisms and co-existence with hardware roots of trust need to be well-established as described in Section 4.1.1.3.

Overall, when security of 5G verticals are elaborated, there are two key aspects: 1) vertical specific security solutions exploiting the general techniques described in other subsections (those may be quite information security general solutions), and 2) network slice security since network slices are fundamental to serve verticals in 5G. Therefore, in this section we focus on network slice security.

In 5G, the same physical network is shared among several network slices and tenants, leading to different virtual networks and assigned resources. One security impact of network slicing architecture is the potential expansion of the attack surface through which malware can be introduced [117]. Since network slices serve different types of services for different verticals, they may have different levels of security and privacy policy requirements. To maintain an acceptable level of security, tenants should not be able to interfere with each other's networks, and it is not needed to be aware that they are sharing network resources with others. Slice and possibly tenant isolation (the separation of one tenant's resources and actions from another) is an important feature of 5G security [118]. For instance, isolation considered as security enabler depends on the quality of isolation mechanisms used in the various components of the network [119]. For network traffic, that may include data plane isolation and control plane isolation. In addition to logical isolation, traffic may be encrypted with specific tenant keys. This guarantees that in the case of logical encapsulation violation, the data traffic remains isolated and information cannot be leaked.

To serve multiple verticals securely, security policy and efficient coordination mechanisms among different administrative domains infrastructure in 5G systems must be designed and developed

[120]. Isolation also refers to security incidents: efficient mechanisms must be developed to ensure that any attacks or faults occurring in one slice must not have an impact on other slice.

Slice isolation (paths, functions and resources) issues need to be resolved by considering into the aspect of resource consumption and overheads [247][248]. While traffic isolation can help with data leakage, shared resource usage also requires resource isolation. For example, the existence of a forwarding loop within one tenant may potentially impact all tenants, as the problem overloads the underlying network equipment. Moreover, the final logical 5G network becomes much more complicated in terms of management and security provisioning. For security management, another important research question is the interplay between pure isolation versus cross-slice operating security functions [249][250]. The latter provides a much better situational awareness (e.g. ML-driven security functions consuming a much better training and operational dataset) and a broader toolkit to mitigate security calamities and handle attacks.

4.2 Standards

Open standards are not only essential to guarantee interoperability among the different components in a network, but to achieve their security as well. Without open standards, it is overly complicated to assess security properties or validate practices in any given network infrastructure or service. Therefore, it is one of the project strategic goals to transform the developed solutions and frameworks into standards, and to create consensus among global players to use the technologies developed by the project. A comprehensive security framework suitable for next-generation networks must be committed to a tight collaboration with standardization bodies.

Furthermore, the consortium is aware of the relevance of open-source communities to achieve standardization, by means of their interaction with standards-development organizations, either direct or indirect, and by means of their ability to produce reference implementations of those standards.

This section describes the key standardization fora, in the wider sense mentioned above, that have been identified by the project partners, including the most relevant documents and work in progress in each case.

4.2.1 European Telecommunication Standard Institute - ETSI

4.2.1.1 Zero-touch network and Service Management - ZSM

The *Industry Specification Group Zero-touch network and Service Management* (ISG ZSM) is focused on the definition of a new, future-proof, horizontal and vertical end-to-end operable framework and solutions to enable agile, efficient and qualitative management and automation of emerging and future networks and services. Horizontal end-to-end refers to cross-domain, cross-technology aspects. Vertical end-to-end refers to cross-layer aspects, from the resource-oriented up to the customer-oriented layers. The ZSM automation framework constitute an essential ground for the enforcement of security properties and the provision of security services in next-generation networks.

In addition, in its recently approved second two-year term, the ISG include plans to consolidate the security aspects related to the ZSM framework and solutions for network and service automation, and work to ensure that the automated processes are secured and deliver the intended business outcomes. This is essential to increase the level of trust in automation and for ensuring that security holes are not accelerated with AI/ML.

4.2.1.2 Securing Artificial Intelligence - SAI

The *Industry Specification Group Securing Artificial Intelligence* (ISG SAI)[13] is committed to develop technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. Created in the last quarter of 2019, and well aware of the novelty of fields of action, it is especially focused on pre-standardisation activities, especially on framing the security concerns arising from AI and to build the foundation of a longer-term response to the threats to AI in sponsoring the future development of normative technical specifications. The first work items are focused on aspects such as a formal problem statement for the securing AI issue, the definition of an AI threat ontology and the analysis of the data supply chains.

The underlying rationale for ISG SAI is that autonomous mechanical and computing entities may make decisions that act against the relying parties, either by design or as a result of malicious intent. The conventional cycle of risk analysis and countermeasure deployment represented by the Identify-Protect-Detect-Respond cycle needs to be re-assessed when an autonomous machine is involved. The pervasive application of AI that is envisaged for next-generation networks at all levels, and explicitly including security, makes the goals of SAI totally aligned with one of the key aspects to be considered by the project.

At the time of writing this deliverable, the main activities of the group revolve around the following three Work Items:

AI Threat Ontology (SAI-001): This Work Item[14] will undertake the work of defining what is considered an AI threat and align the terminology across the involved stakeholders and industries in the context of cyber and physical security. The narrative of the AI Threat Ontology deliverable will be accessible by anyone involved, including experts and less informed audiences coming from multiple ICT fields. This activity will also investigate the ways an AI threat might be created hosted and propagated and whether it differs from threats to traditional systems. The AI Threat Ontology will consider AI as an attacker, defender and system.

Securing AI Problem Statement, Data Supply Chain Report (SAI-002): Data is significant in the development of AI systems since they can be used to change the function of the system[15]. This holds true for both raw data as well as for information and feedback received from other systems or humans in the loop. Compromising the training data has been proven to be a viable attack vector against an AI system; however, access to suitable data is often limited, resorting to less suitable sources of data. This report summarizes the methods currently utilized to collect source data for training AI, along with a review of the existing regulations, standards and protocols controlling the handling and sharing of that data. It will also analyse requirements for standards for ensuring traceability, integrity and confidentiality of the shared data, associated attributes, information and feedback.

Security Testing of AI (SAI-003): This Work Item[16] will define objectives, methods and techniques for security testing of AI-based components, considering the new challenges introduced by AI compared to traditional systems. Such challenges include differences between symbolic and subsymbolic AI, non-determinism, the test oracle problem, as well as the fact that data form the behaviour of subsymbolic AI. This activity will start with a gap analysis to identify the possibilities and limitations regarding security testing of AI-based systems in coordination with the Technical Committee (TC) Methods for Testing and Specification (MTS). It will also provide guidelines on relevant topics of securing AI, including but not limited to testing data, security test oracles, test adequacy criteria,

[13] https://www.etsi.org/committee/1640-sai
[14] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856
[15] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857
[16] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860

security testing approaches for AI, by utilizing the results of the Work Item “AI Threat Ontology” to cover relevant threats for AI through security testing.

4.2.1.3 NFV-SEC - The status for ETSI NFV Security Group

This WG holds several experts on cybersecurity, privacy, hardware security with an interest on the application of these security domains on NFV infrastructures. This group works for studying appropriate measures for operational efficiency and features to support regulatory requirements, e.g., Lawful Intercept, Privacy and Data Protection.

API Access Token Spec (SEC 022): This ETSI-GS specifies the access tokens and related metadata for APIs defined between VNFs, VNFM, NFVO and VIM. The work consists on addressing these three aspects: 1) defining security requirements for API access tokens, 2) Analysing the tokens specifications (e.g. Openstack Keystone, OpenID Connect Id-Token, IETF OAuth token Binding, 3GPP TS 33.179), 3) defining an NFV token request and generation profile, the access token format and the associated metadata. The specification will refer to existing specifications of access tokens if the NFV requirements are met by these specifications. 4) Defining the process for the token verification by the API Producer. This will produce a new GS SEC022 revision.

Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference point-Interface and Information Model Specification (IFA 033): The objective of this document is to define security requirements on the interfaces between MANO and the Security Controller (defined in IFA 026).

Container Security Specification (SEC 023): This document is at a draft version and publicly available. The document specifies the security and hardening requirement for running NFV software (e.g. VNFs) in containerised environments. This work item will produce a new specification covering as a minimum; threat analysis; state of the art; isolation (namespaces); Attack surface reduction and privilege limitation; Security model and properties; Resource limitations (cgroups); Hardware protections (HMEE); Container hardening (i.e. patching); Containers in VMs and containers on bare metal. The work will consider alignment with existing IFA specifications and reports (e.g. IFA 029).

Supporting companies: Orange, THALES, Ericsson LM, Nokia Corporation, TELEFONICA S.A., OTD, BT plc, Ministère Economie, et Finances. Orange is the editor for this document.

Report on Certificate Management (SEC005): This document provides guidance to NFV on the use of certificates and certificate authorities. It looks at various certificate deployment scenarios and describes certificate specific use cases, threats to the certificate management structure, and resulting requirements for NFV.

Package Security Specification (SEC021): This document outlines the requirements for integrity and authenticity protection by signing VNF Package artefacts and verifying these artefacts during instantiation. This specification document also considers the confidentiality of VNF Package artefacts and outlines a process for the service provider to provide confidentiality during onboarding. The present document expands on requirements for security and integrity of a VNF Package that is defined in ETSI GS NFV-IFA 011 [14], clause 6.2.4 and ETSI GS NFV-SOL 004 [11], clause 5.

Report on NFV Remote Attestation Architecture (SEC018): This document identifies and studies Remote Attestation architectures applicable to NFV systems, including the definition of attestation scope, stakeholders, interfaces and protocols required to support them. Additionally, the present document identifies and discusses functional and non-functional capabilities to be supported in an NFV system and provides a set of recommendations.

In the current state of this document, even though TPM is not explicitly mentioned, all the described architectures follow TPM paradigm. The idea is to add implicit attestation on the document to make it less TPM specific.

Management and Orchestration; Architecture enhancement for Security Management Specification (IFA 026): The objective of this document is to define security requirements on the interfaces between MANO and a Security controller. These requirements are defined while taking

into consideration Lawful Interception requirements. This document is based on SEC 013 document where the Security Manager is defined. It is responsible for analysing information passed to it from MANO and where necessary instructing MANO to take actions accordingly (e.g. applying security policy to a VNF being initiated). In addition, when the SM becomes aware of a security event (e.g. VNF compromise) the SM is responsible to instructing MANO to take appropriate mitigating actions (e.g. terminate a VNF or quarantine a VNF).

Three monitoring modes are defined for the interaction between the Security Manager and MANO functional Block: active, semi active and passive. Most of the requirements defined are inherited from SEC 013 document. Passive mode is the implementation of the LI mode. The security manager in this mode only consumes information provided by MANO regarding all VNF lifecycle management and all required information for LI. The SM in this mode is not allowed to advocate any security policies. Next step on this document consists on working with SOL and IFA to refine security of the implementation of three interfaces between MANO and SM.

Networks Functions Virtualisation (NFV); NFV Security; Problem Statement (ETSI GS NFV-SEC 001): This Group Specification [251] is part of the first set of documents published during the first two years of the ISG NFV and formed a basis for common understanding regarding NFV concepts and technical requirements. It is considered pre-standardization work and has been influential in NFV security efforts. This document identifies potential security vulnerabilities of NFV, determines whether they represent new or already existing problems and defines a reference framework to define these vulnerabilities. It is also worth noting that "ETSI SAI-002 – Securing AI Problem Statement" specification will be modelled on NFV-SEC 001.

Networks Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance (ETSI GS NFV-SEC 003): This Group Specification[17] is also part of the "pre-standardization" ETSI documents published in 2014. It describes the security and trust guidance that is unique to NFV development, architecture and operation. Guidance consists of items to consider that may be unique to the environment or deployment and is based on use cases, defined in this document and derived from ETSI GS NFV-SEC 001.

4.2.1.4 Experiential Networked Intelligence - ENI

The *Industry Specification Group Experiential Networked Intelligence* (ISG ENI) focuses on improving the network management experience, adding closed-loop artificial intelligence mechanisms based on context-aware, metadata-driven policies to more quickly recognize and incorporate new and changed knowledge, and hence, make actionable decisions. ENI has explored a set of use cases, and defined the architecture, for a network supervisory assistant system based on the 'observe-orient-decide-act' control loop model. This model can assist decision-making systems, such as network control and management systems, to adjust services and resources offered based on changes in user needs, environmental conditions and business goals.

AI applicability to security enforcement and service provisioning would greatly benefit from a detailed assessment of this model, including the opportunities to achieve its integration with a zero-touch multi-domain architecture as defined by ZSM.

4.2.2 3GPP SAx

SA3 is the specific *service area* focused on security aspects within 3GPP. Apart from maintaining the current security specifications for 5G and former generations of mobile networks, SA3 is especially focused on all security challenges and opportunities related to the implications of current *network softwarisation* trends. This includes security orchestration opportunities, and how to combine local detection and mitigation with a global view of threats and attacks, the implications of a SBA (Service

[17] https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf

Based Architecture) on the threat surface and the mitigation strategy, and the incorporation of attestation methods in alignment with the work performed in the SEC WG within ETSI NFV.

Since 3GPP specifications constitute the base reference for mobile networks, the works of SA3 constitute one of the essential starting points, as well as a very relevant target for further contribution of project results.

4.2.3 Internet Engineering Task Force - IETF

The IETF is the body acting as producer and maintainer of the core Internet specifications, from IP to HTTP, and explicitly referenced by many other bodies in their standardization activities. Security matters are explicitly dealt with within the Security Directorate, coordinating the different working groups and activities of any other nature related to Internet security. Among these activities, the project has identified the following ones as the most relevant ones in the present moment:

- In matters related to security management and orchestration, the Interface to Network Security Function (I2NSF[18]) (dealing with interfaces and models for security control and monitoring) and Automatic Certificate Management Environment (ACME[19]) (dealing with automated certificate management) working groups
- In matters related to trust and attestation, the Remote ATtestation ProcedureS[20] (dealing with attestation evidences and protocols to convey them), Trusted Execution Environment Provisioning (TEEP[21]) (dealing with lifecycle and security domain management) and Software Updates for Internet of Things (SUIT[22]) (dealing with updates and manifests in constrained environments) working groups.
- The Manufacturer Usage Description (MUD[23]) activity, dealing with device-network signalling on access and network functionality, and the Stopping Malware and Researching Threats (SMART[24]) initiative on external endpoint protection.
- The recently started discussions on the evolution of the Internet threat model, under the auspices of the IAB (Internet Architecture Board).

4.2.4 Institute of Electrical and Electronics Engineers - IEEE

Although IEEE is more involved in the specification of local-area networks compared to wide-area network, it has various standardisation efforts in security and network softwarisation and future communication systems:

- **IEEE P1915.1 Standard for Software Defined Networking and Network Function Virtualisation (SDN/NFV) Security:** This standard provides a framework for network operators, service/content providers, and end users to build and operate secure SDN/NFV environments. In that regard, it specifies a security framework, models, analytics, and requirements for SDN/NFV.
- **IEEE P1917.1 Standard for Software Defined Networking and Network Function Virtualisation Reliability:** This standard provides a framework to build and operate SDN/NFV service delivery infrastructure under reliability requirements of network operators,

[18] https://datatracker.ietf.org/wg/i2nsf/about/
[19] https://datatracker.ietf.org/wg/acme/about/
[20] https://datatracker.ietf.org/wg/rats/about/
[21] https://datatracker.ietf.org/wg/teep/about/
[22] https://datatracker.ietf.org/wg/suit/about/
[23] https://tools.ietf.org/html/rfc8520
[24] https://datatracker.ietf.org/group/smart/about/

service/content providers, and end users. It specifies various aspects such as reliability framework, models, analytics, and requirements for SDN/NFV.

- **IEEE P1913.1 (Draft) Standard for Software-Defined Quantum Communication (SDQC):** This standard defines the SDQC protocol that enables configuration of quantum endpoints in a communication network in order to dynamically create, modify, or remove quantum protocols or applications. It aims to define a well-defined interface to quantum communication devices so that such devices can be reconfigured to implement a variety of protocols and measurements. This protocol resides at the application layer and communicates over TCP/IP. The protocol design facilitates future integration with network softwarisation related standards.
- **IEEE P1920.1 Standard for Aerial Communications and Networking Standards** This standard enhances the situational awareness of aircraft to communicate in an adhoc aerial network. It defines air-to-air communications for self-organized adhoc aerial networks (manned and unmanned, small and large, and civil and commercial aircraft systems). Networking for autonomous vehicles is an important use-case for 5G networks. The standardization aims to be independent of the type of network (cellular, point-to-point or satellite). The standard also elaborates on the security of the communication infrastructure in this environment.

4.3 Relevant 5G Projects/Initiatives

4.3.1 5GPPP Program Current Status

The 5GPPP program is, at the time of this writing, at the second part of its third phase. The third phase is the last phase of the program. The third phase addresses the following efforts[25]: ICT-52-2020 – Smart Connectivity beyond 5G; ICT-41-2020 – 5G Innovations for Verticals with Third Party Services; ICT-42-2020 – 5G Core Technology Innovations; and ICT-53-2020 – 5G for Connected and Automated Mobility (CAM). Phase 3 is targeting specific verticals for 5G networks. To facilitate the development of applications for the vertical, several technologies have been identified. Some examples of such technologies are radio technologies for cell-free networks, resilient networking for support of improved and elastic reliability, AI/ML-powered for adaptive network operations, and edge-to-edge low latency, security and energy efficiently. One of the aims of phase 3 is to avoid duplication ("hype-effect") and coverage of issues from the previous phases.

4.3.2 ICT-17 Projects

The EC selected 5G EVE, 5G-VINNI and 5GENESIS as the three projects for implementing and testing advanced 5G infrastructures in Europe, in response to the 5G-PPP ICT-17-2018 call. All projects were launched on July 2018 with a duration of 3 years. The following subsections describe in summary the scope of each project. Additionally, they offer a preliminary description on the security mechanisms of each project based on the publicly available information when available.

4.3.2.1 5G EVE

5G EVE[26] stands for "5G European Validation Platform for Extensive Trials" and its main concept is interconnecting and further developing four existing European sites, in order to form a unique 5G end-to-end facility. The four sites are located in France, Greece, Italy and Spain, containing both indoor and outdoor facilities. The addressed use cases include Smart Transport, Tourism and Cities, Industry 4.0, Media and Entertainment, while the technologies under use include heterogeneous access, MEC, as well as multi-site/domain/technology slicing/orchestration. 5GEVE security is focused

[25] https://5g-ppp.eu/wp-content/uploads/2019/09/190712_5GInfraPPP_PSM-Phase3.II_V2.0_Final.pdf
[26] https://5g-ppp.eu/5g-eve/

on providing a centralized authentication and control access to develop 5G experimentation infrastructure. The project defines and enforces different roles: Verticals, Vertical's developers, experiment developer, experimenters, and site administration.

4.3.2.2 5G VINNI

5G VINNI[27] stands for "5G Verticals INNovation Infrastructure" and aims at developing an E2E 5G facility for demonstrating the practical implementation of infrastructure to support the key 5G KPIs. It will then allow vertical industries to test and validate specific applications that are dependent upon those KPIs. 5G VINNI includes four main sites in Norway, UK, Spain and Greece, providing services with well-defined Service Level Agreements, as well as experimentation sites in Portugal and Germany, providing environments for advanced testing and experimentation. There is also a moving experimentation facility enabled by a satellite connected vehicle for satellite integration into 5G. The technologies under use include network slicing, MEC, NFV, as well satellite backhaul options. No specific security research has been proposed in 5GVINNI, but a network telemetry framework has been design to cope with 5G KPIs measurements. This framework opens the opportunity to be leverage this telemetry to develop security AI/ML models based on the data collected.

4.3.2.3 5GENESIS

5GENESIS[28] stands for "5th Generation End-to-end Network, Experimentation, System Integration, and Showcasing" and its main goal is validating 5G KPIs for various 5G use cases in both controlled setups and large-scale events. The project brings together results from a considerable number of EU projects as well as the partners' internal R&D activities in order to realise an integrated end-to-end 5G Facility. There are five main facilities across Europe that are under development in the context of 5GENESIS, each covering a different set of 5G KPIs in a complementary manner: Athens, Malaga, Berlin, Surrey and Limassol Platforms, plus a Portable Demonstrator. Each platform will validate 5G KPIs in a different set of Use Cases, including but not limited to Media and Entertainment, Transportation, Public Safety, Factory of the Future/Industry 4.0, eHealth and Smart Cities. Technologies under use include network slicing, MEC, SDN/NFV, orchestration, as well as multiple radio access technologies. 5GENESIS is an infrastructure project focusing on providing a unified experimentation framework over End-to-end 5G facilities. As such, the project adopts security features addressing both the security of the deployed infrastructure, as well as the security and privacy of the experimenters accessing its facilities. Each platform shall provide the means for authentication and authorization of experimenters in the form of security functions for user authentication and access control.

In addition, 5GENESIS includes an Anomaly Detection Framework [254], currently allowing the detection of anomalies, which may correspond to either malfunctions or security incidents. The framework uses the Data Analysis and Remediation Engine (DARE) developed in the SHIELD[29] project and leverages Big Data technologies based on Apache Spot, Hadoop Distributed Filesystem (HDFS), Kafka and Spark. It consists of a main data analytics engine and distributed data collection components, implementing Data acquisition, transformation and storage, Data analysis, as well as visualization and export.

Finally, the Katana Slice Manager[30] is under development in the context of 5GENESIS and is used for deploying services across multiple network domains (edge, core, ran, etc.), while managing the resources' reservations. During Phase 3 of the project, the Katana Slice Manager will be integrated with ERICSSON's APEX Policy Engine [255] and will leverage the 5GENESIS "Analytics and Monitoring Framework" [256], in order to apply security related mitigation policies across the infrastructure.

[27] https://5g-ppp.eu/5g-vinni/
[28] https://5g-ppp.eu/5genesis/
[29] https://www.shield-h2020.eu/
[30] https://github.com/medianetlab/katana-slice_manager

4.3.3 ICT-18 Projects

Three projects have been selected in the automotive call. They have started in November 2018 and will last for three years with the aim of implementing and testing advanced cross-border 5G infrastructures in Europe. More information is provided for each of the projects in the following subsections.

4.3.3.1 5G-CroCo

5G-CroCo[31] is a cross-border project connecting the cities of Metz-Merzig-Luxembourg, traversing the borders between France, Germany and Luxembourg. The objective is to validate advanced 5G features, such as New Radio, MEC-enabled distributed computing, predictive QoS, Network Slicing, and improved positioning systems, all combined to enable innovative use cases for CCAM. 5GCroCo aims at defining new business models that can be built on top of this unprecedented connectivity and service provisioning capacity, also ensuring that relevant standardization bodies from the two involved industries are impacted. In the context of 5G-CroCo, a thorough security analysis at an architectural and implementation level for the automated driving related use cases is performed. In particular, the following components are analysed: i) Security assessment of essential involved communication protocols (on-board communication, vehicle-to-vehicle communication and any other vehicle to third-party communication channel); ii) Security assessment of essential involved hardware devices (on-board and off-board); and iii) Security assessment of essential involved software components (on-board and off-board). As the 5G-CroCo use cases open up entirely new questions from a security and privacy perspective that have not been asked in a similar context before, the alignment with INSPIRE-5Gplus objectives will contribute to the creation of secure 5G networks supporting connected and automated mobility services in cross-border settings, that are designed according to the best practices regarding security, privacy and compliance.

4.3.3.2 5G-CARMEN

5G-CARMEN[32] stands for “5G for Connected and Automated Road Mobility in the European union”. Focusing on the Bologna-Munich corridor (600 km, over three countries) the objective of 5G-CARMEN is to leverage on the most recent 5G advances to provide a multi-tenant platform that can support the automotive sector delivering safer, greener, and more intelligent transportation with the ultimate goal of enabling self-driving cars. The key innovations are centred around developing an autonomously managed hybrid network, combining direct short range V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) communications with long-range V2N (vehicle to network) communications. The platform employs different enabling technologies such as 5G New Radio, C-V2X (Cellular vehicle to everything), and secure, multi-domain, and cross-border service orchestration system to provide end-
to-end 5G enabled CARMEN services. The security mechanisms of 5G-CARMEN are divided into two categories, i.e. a) access control mechanisms and b) threat identification and mitigation mechanisms. The use cases in 5G-CARMEN require all the involved parties to authenticate themselves before being able to access and use the provided services. The access control mechanisms in 5G-CARMEN make use of secure elements to authenticate services and devices without human supervision. This is done by introducing an additional authorization layer that ensures service continuity in cross-border scenarios. For threat identification, 5G-CARMEN makes use of a domain-specific language to express systems in a way that facilitates reasoning about their security posture. Several automated processes are defined to improve the security analysis, such as the proposition of security mechanisms, and the identification of vulnerabilities.

[31] https://5gcroco.eu
[32] https://5gcarmen.eu

4.3.3.3 5G-MOBIX

5G-MOBIX[33] will develop and test automated vehicle functionalities using 5G core technological innovations along multiple cross-border corridors and urban trial sites, under conditions of vehicular traffic, network coverage, service demand, as well as considering the inherently distinct legal, business and social local aspects. The project will evaluate benefits in the CCAM context as well as define deployment scenarios and identify and respond to standardisation and spectrum gaps. The expected benefit of 5G will be tested during trials on 5G corridors in different EU countries as well as China and Korea. Several automated mobility use cases are potential candidates to benefit from 5G such as cooperative overtake, highway lane merging, truck platooning, valet parking, urban environment driving, road user detection, vehicle remote control, see through, HD map update, media & entertainment. In the context of 5G-Mobix requirements related to ITS systems were identified to produce secure environments in Vehicular environments. In a second phase, those requirements have been addressed in three main areas, protection of ETSI ITS messages, HDMap transmissions and data privacy protection in relation with GDPR.

4.3.4 ICT-19 Projects

4.3.4.1 5G!Drones

5G!Drones[34] stands for "Unmanned Aerial Vehicle Vertical Applications' Trials Leveraging Advanced 5G Facilities" and aims to validate 5G KPIs for UAV related Use Cases. The project will utilize existing 5G facilities provided by ICT-17 Projects and will cover a multitude of services, including eMBB, URLLC and mMTC. The key component technology of the project is Network Slicing, allowing the simultaneous provision of the three types of UAV services on the same 5G infrastructure and demonstrating that each UAV application runs independently without affecting other Unmanned Aerial Vehicle (UAV) applications. The project will provide an automated framework for executing trials by the verticals, according to a specified scenario. The considered use cases[35] include UAV Traffic Management, Public Safety, Situation Awareness and Connectivity during crowded events. Security focus of 5GDrones is on E2E network slice security the way needed to cover UAV Use Cases requirements. 5G!Drones project considers security at two levels, namely the trial controller level, and the 5G facilities level. The trial controller is responsible for dialoguing with the verticals and running their trials on the top of the 5G facilities. The access to the trial controller's functionalities need to be controlled depending on the role of the user (e.g., experimenter, facility owner, etc.). An identity and access management (IAM) system are envisaged to meet this requirement. For the 5G facilities level, the slice manager is required to connect with a security policy orchestrator to enforce slice security.

4.3.4.2 5G-VICTORI

5G-VICTORI[36] stands for "VertIcal demos over Common large-scale field Trials fOr Rail, energy and media Industries" and aims at conducting large scale trials for advanced use cases, focusing on Transportation, Energy, Media, Factories of the Future, as well as cross-vertical use cases. The project will build upon the existing facilities of all ICT-17 projects and will utilize technologies developed in 5G-PPP Phase 1 and Phase 2 projects. 5G-VICTORI will adopt a flexible architecture to accommodate technologies from multiple domains and will focus on these specific Use Cases[37]: Enhanced Mobile broadband under high speed mobility, Digital Mobility, Critical Services for railway systems, Smart Energy Metering, digitization of Power Plants and Content Delivery Network services in dense, static and mobile environments.

[33] https://www.5g-mobix.com
[34] https://5g-ppp.eu/5gdrones/
[35] https://5gdrones.eu/use-case-scenarios/
[36] https://5g-ppp.eu/5g-victori/
[37] https://www.5g-victori-project.eu/about-5g-victori/motivation/

4.3.4.3 5G SMART

5G SMART[38] stands for "5G for smart manufacturing" and aims at demonstrating and validating the potential of 5G in real manufacturing environments, addressing the needs of the Industry 4.0 vertical. The project will utilize three trial sites dispersed in Sweden and Germany for conducting the validation and demonstration of advanced manufacturing applications. Such applications include digital twins, industrial robots and machine vision based remote operations. From a technical perspective, 5G SMART will study electromagnetic compatibility issues, as well as the coexistence between public and private networks in manufacturing environments, while they are opting for developing new 5G features for manufacturing use cases, such as time synchronization and positioning, while exploring new business models.

4.3.4.4 5G-TOURS

5G-TOURS[39] stands for "SmarT mObility, media and e-health for toURists and citizenS" and aims at providing services for tourists, citizens and patients through end-to-end 5G trials. The project will demonstrate thirteen use cases over three cities: Rennes, focusing on e-health; Turin, focusing on media and broadcast and Athens, focusing on transportation. The key component technologies of the project include network slicing, orchestration, virtualization and broadcasting, in order to provide seamlessly different types of services, while deploying pre-commercial 5G technologies at a large scale.

4.3.4.5 5G-SOLUTIONS

Aims to prove and validate that 5G provides prominent industry verticals with ubiquitous access to a wide range of forward-looking services with orders of magnitude of improvement over 4G, through conducting advanced field-trials of innovative use cases across five significant industry vertical domains: factories of the future, smart energy, smart cities, smart ports, and media and entertainment[40].

4.3.4.6 5G-HEART

The 5G-HEART[41] validation trials will focus on vertical use-cases of healthcare, transport and aquaculture. In the health area, 5G-HEART will validate pill cameras for automatic detection in screening of colon cancer and vital-sign patches with advanced geo-localization as well as 5G AR/VR paramedic services. In the transport area, 5G-HEART will validate autonomous/assisted/remote driving and vehicle data services. Regarding food, the focus will be on 5G-based transformation of the aquaculture sector.

4.3.4.7 5GROWTH

The vision of the 5Growth[42] project is to empower verticals industries such as industry 4.0, transportation, and energy with an AI-driven automated and sharable 5G end-to-end solution. Towards this vision, 5Growth will automate the process for supporting diverse industry verticals through closed-loop automation and SLA control for vertical services lifecycle management, and AI-driven end-to-end network solutions to jointly optimize access, transport, core, cloud, edge and fog resources. 5Growth focuses on making the platform for vertical industries a verifiable and trustable stack. To this end, the platform shall be able to support the exchange of request and response messages involving multiple actors. Moreover, the platform will integrate non-repudiation mechanisms complemented with advanced security methodologies.

[38] https://5g-ppp.eu/5g-smart/
[39] https://5g-ppp.eu/5g-tours/
[40] https://5g-ppp.eu/5g-solutions/
[41] https://5g-ppp.eu/5g-heart/
[42] https://5g-ppp.eu/5growth/

4.4 Open Source Initiatives

Since open source has become a reference for the networking industry, as a way of consolidating or even directly produce standard solutions, there are many different open source initiatives to be considered at all levels, from the cloud and infrastructural foundations (OpenStack, Kubernetes, CNCF, O-RAN, TIP, CNTT) to the orchestration and automation aspects addressed by the ONAP and OSM platforms. For all of these, their security mechanisms, together with the facilities they provide for supporting enforcement frameworks, must be used as starting point, analysed and updated accordingly. Advancing in the alignment of these security mechanisms to avoid *impedance mismatches* that extend threat surfaces will become an essential goal.

In addition, there are several open source initiative categories suitable to be directly leveraged by the project:

- Attestation frameworks, supporting the application of these technologies for different combinations of infrastructural and management bases. The main reference among these frameworks is Keylime[43], a TPM-based remote boot attestation and runtime integrity measurement environment, adhering to the Trusted Computing Group TPM 2.0 specification and built on top of the Linux TPM2 Software Stack
- Programmable dataplanes, supporting a much more efficient enforcement of advanced security policies by pushing them down the dataplane. This is a trend that has been recently fostered by the programmable packet forwarding abstractions defined by P4[44], and the evolution of the Linux in-kernel implementation of the eBPF virtual CPU[45].

4.5 Lessons Learned

The evolution and development of 5G is taking place across various domains and institutions. This type of development fosters rapid growth and experimentation of novel technologies and concepts. However, significant effort is duplicated across the different domains, causing the “reinvention of the wheel” of technologies that will later be used as the backbone of 5G networks. This duplication of effort not only reduces the amount of work is spent on novel features but reduces the competitive advantage of European organizations. The more each institution and organization is focussed on promoting their own bespoke solution, the more difficult it becomes to collaborate and contribute to holistic approaches.

In the early development of 5G, individual research and development enabled the exploration of different ideas. This allowed organizations and institutions to test, benchmark and compare each idea with the benefits and requirements of 5G vertical. However, as 5G technology is reaching a vast deployment, the developed solutions need to begin converging into standardized approaches. The convergence will allow organizations to focus their development on improving the most optimal solutions and reduce the need for replication.

The convergence of security solutions is of vital importance for 5G networks. 5G networks increasingly connect services from different providers to a vast number of interconnected consumer devices. This interconnection of million/billion endpoints significantly increases the attack surface of individual systems. To address this issue, security solutions of 5G networks need to be developed and deployed in a collaborative manner. This can be greatly aided with the use of open and standardised interfaces and enablers. This will facilitate collaboration between different stakeholders to combat

[43] https://keylime.dev
[44] https://p4.org
[45] https://lwn.net/Articles /599755/

and address security incidents, without affecting the availability, the confidentiality, and the integrity of 5G networks. This is the stance that the project will encourage.

5 Future Trends and Technologies

The ever-evolving threat landscape facing 5G and beyond networks and the anticipated increasing complexity in operating and managing those networks demand for advancements in the current security management achievements to cope with the new cybersecurity requirements while taking advantage of the promising concepts/technologies, such as ZSM, AI/ML, Blockchain, TEE, that are gaining momentum due to their ability to deliver actionable results for a better, safer and smarter security for 5G. This section will explore the potential of those concepts/technologies to come up with fully new breed of security solutions in support of 5G security.

5.1 Automation & Zero-touch Service Management

The paradigm of automation is crucial in 5G networks due to the burgeoning complexity of services and infrastructure, and stringent requirements such as timeliness of management actions (responsiveness and low latency) and reduced costs. Beyond the necessity of network deployment, Google has disclosed their need for network automation, where 70% of failures happen when a management operation is in progress. In order to automate network behaviour while fulfilling the necessary consistency and resiliency, a new approach to network control is appearing in the form of ZSM.

5.1.1 Challenges in network automation

Three main challenges arise in order to support network automation:

- The need for defining the **architecture** (i.e., functions, interfaces, protocols, etc.) to enable the deployment of autonomous workflows and mechanisms with streaming telemetry and the service orchestration entities.
- The devising of novel **autonomous workflows and algorithms** that adopt local domain and E2E decisions and actions to enhance/ensure the E2Eglobal objectives demanded by each network.
- For the security context, the integration and implementation of security mechanisms in network automation paradigm to work with more general automation solutions as well as to come up with more effective and advanced security solutions

Apart from this, it is evident that there is a lack of implementations in terms of open source or proprietary solutions, as well as protocols adoptions to facilitate the E2E service management.

5.1.2 Trends and Technologies of Network Automation

ETSI has been actively defining autonomous networks architecture by the promotion of Generic Autonomic Networking Architecture (GANA) [40]. GANA implements the autonomic management and control paradigm by introducing Decision-making Elements (DE) as autonomic function (i.e., control loops) with learning and reasoning used to effect advanced adaptation (i.e., cognition). Moreover, in 2017, ETSI promoted a novel ISG with the purpose to provide zero-touch network and service management[46]. ZSM aims to provide a network architecture that can autonomously respond to all requirements of a network slice life-cycle management in terms of assurance and performance.

In relation with ZSM and the challenge of lack of real frameworks, two initiatives have demonstrated interest and initial alignment on the adoption of ZSM, namely: Open Network Automation Platform

[46] https://www.etsi.org/technologies/zero-touch-network-service-management

(ONAP[47]) and Open Source MANO (OSM)[48]. Both technologies could be suitable for ZSM adoption into INSPIRE-5Gplus.

Another active research challenge, directly linked to the necessity of network slice management automation, is slice elasticity in post deployment or operational phases; directly translated dynamic network resources allocation and/or addition of removal of network and service functions from a slice. To this end, intelligent network slicing management mechanisms using analytics at the service orchestration platform could enable a much more informed elastic network management and orchestration, which allows proactive resource allocation decisions based on heuristics rather reactive approaches. This approach would be in line with the goal of a new ETSI ISG called Experiential Network Intelligence (ENI)[49], which proposes an engine that adds closed-loop AI mechanisms based on context-aware and metadata-driven policies to more quickly recognize and incorporate new and changed knowledge, and make actionable decisions. In fact, it is worth highlighting that there is a use case currently being developed in ETSI ENI that focuses on intelligent network slicing management, placing or adjusting the network slice instance (e.g., reconfiguration, VNF scale in/out) to achieve an optimized resource utilization with a changing context.

5.1.2.1 APIs between orchestrators, data and control planes

The interface between orchestrators and the control planes is referred to as the NorthBound Interface. Most of current projects and solutions aim to exploit the REST-based API to provide this Interface. For example, OpenMANO [121] provides two northbound interfaces based on REST, namely OpenVim-API and OpenMano-API to offer the creation, deletion, and management of VNF, instances, and networks. Moreover, JOX [122], an orchestrator for 5G network slicing, also exposes a REST-based northbound API to enable management and monitoring of each slice. JOX exposes a set of APIs in support of slice and subslice life-cycle management and their monitoring with service and machine granularity as well as APIs for on-boarding and store management. On the other hand, the Open Network Foundation (ONF) [123] aims to apply SDN architecture to 5G network slicing. For this, a specific Northbound Interface for a transport SDN controller called Transport API (TAPI) [124][125] is proposed. TAPI allows a transport SDN controller to control a domain of transport network equipment as well as a customer's application or a carrier's orchestration platform to retrieve information from a transport SDN controller. TAPI also allows the integration of control and monitoring of optical transport networks with higher-level applications.

Regarding SouthBound Interface, the interface between control planes and data planes, several protocols have been proposed. OpenFlow protocol [126] is the most popular implementation. The authors in [127] demonstrate how to modify the 4G architecture towards the 5G architecture, by using the SDN concept with OpenFlow (OF) as protocol. However, several issues are listed in [128], e.g. the scalability of OF switches that have limits on table sizes and event control processing. NETCONF [129] is also another protocol, which provides mechanisms for installing, manipulating, and removing configuration from network devices. It uses an extensible mark-up language (XML) encoding configuration data as well as protocol messages. NETCONF can be extended in the context of 5G; for instance, the authors in [130] proposed and demonstrated a NETCONF-based low latency cross-connect for 5G C-RAN architectures. On the other hand, in the context of 5G, the most critical criterion is the real-time constraint. The authors in [131] argue that available Southbound APIs and protocols like NETCONF and Openflow will not work and propose a novel SouthBound control protocol called FlexRAN, using OAI-based LTE systems.

[47] https://wiki.onap.org/display/DW/TCC+Generic+Network+Management?preview=%2F71839655%2F71839760%2FONAP+in+ETSI+ZSM+Architecture_version4.pdf

[48] https://docbox.etsi.org/ISG/ZSM/05-Contributions/2020/ZSM(20)000044r1_On_ZSM_relationship_with_OSM.pptx (Restricted to ETSI members)

[49] https://www.etsi.org/technologies/experiential-networked-intelligence

5.2 Trusted Execution Environments

5.2.1 Challenges in Trusted Execution Environments

Virtualisation comes with inherent isolation as each VM-/container is memory-isolated from others with an allocated memory space that cannot be scrutinized by others using a direct memory access. However, the host Operating System (OS) has access to all of them. Thus, the isolation can be indirectly broken through the host.

The urban legend “There is no cloud, it is just someone else computer” is a concern shared to anyone considering cloud operation. The associated threat is known as "introspection" and is a specific attack mentioned by ETSI NFV security working group report [131], which defines Introspection as the associated risk as: “The hypervisor is fully aware of the current state of each guest OS it controls. As such, the hypervisor may have the ability to monitor each guest OS as it is running”. In addition to monitoring ability, a malicious operator, with a root access on the host, can access and modify each VM memory space, resulting in violation of data and code confidentiality and integrity. A second security threat comes from the payloads themselves. VM-escape or container-escape attack starts with a vulnerability exploit, then drills the kernel layer underneath to get access to another isolated payload being a VM or a container.

TEE is aimed at answering these security threats, by making sure the host OS cannot access to the VM or container memory space.

Additional risk exists in virtualisation techniques, particularly with the adoption of NFV for 5G networks. In fact, the software components (OS, hypervisor and applications) can be tampered to alter network functions in order conduct malicious activities ranging, from illegal traffic eavesdropping to routing or filtering manipulation. These situations reduce the trust and liability of the NFV infrastructure and VNFs, caused by the additional attack surfaces.

Integrity and verification of the software components during their whole life cycle is recommended, to provide trust in the execution of cloudified 5G network functions. Remote attestation provides to the costumer (of NFVI provider) the evidence that infrastructure and function policies are correctly enforced. Moreover, this remote attestation concept is fully extensible to SDN technologies where attestation of flows rules, allows to trust in the traffic paths over networks when the control plane is decoupled from the devices.

5.2.2 Trends and Technologies of Trusted Execution Environments

From the experience and background of INSPIRE-5Gplus consortium members, we draw a list of pragmatic key operational criteria before considering the use of any TEE technology in the perspective of network implementation. We then enumerate and categorize the handful TEE technologies potentially present on cloud-located or edge computing servers, in the light of the definition and key operational criteria.

5.2.2.1 Trusted Execution Environments definition

TEE concept is a vast and highly documented subject as it actually defines what ought to be done or offered for creating a safeguard, delivering confidentiality and integrity to both code and data, in any opened and exposed standard IT execution environment, including a malicious host or operator with root access to the machine. The concept of TEE is nothing less than the cornerstone for building edge device security and cloud security. It is therefore one of strongest pillars of modern information technology security, orthogonal and independent to vulnerability remediation (i.e., a vulnerable software placed inside a TEE remains vulnerable). TEE concept covers a vast domain of possible usages and is implemented and materialized in several competing TEE architectural implementations vary from software-based and hardware-based implementations, the TEE concept is not precisely defined with one unique, shared and accepted definition. This brings the opportunity to set our own

vision and definition here, considering first what are the needs and expectations. For that, we consider an historical point of view on isolation kernel, the relative positioning of hardware-based TEE against TPM and against software-based solutions. Finally, we list the key security guarantees for hardware-based TEEs, as they correspond to what is generally considered as a TEE and as we are considering their use in this project.

5.2.2.1.1.1 Legacy kernel isolation

In [131] , the authors stress the absence of a common definition, opposing various definitions in this field, emitted by different standardization groups. The "separation kernel" concept is not defined by [133]. The authors referred to work in [134], [135] and another reference who already defined this concept. Because the TEE will need to exchange with the other parts, the kernel shall also bring a highly secured and controlled inter-partition communication channel.

The separation kernel concept has ancient roots back from the 70's. In the early 80's, [131]kernel-driven process isolation. More than two decades later, the US National Security Agency streamlined in [131] their recommendations. This US administration specification document defines the basic need of separation kernel as being capable to establish, isolate and control information flow between those partitions. The reading of this document reflects that the isolation kernel is defined as a separate kernel function, with limited functionalities processed separately and in coordination with the OS. The isolation-partitioning kernel is thus incremental to any OS.

In [131], the authors also define the different security functionalities a TEE must bring:

- Secure boot of the software placed inside;
- Secure scheduling as a mean to optimize the TEE execution without penalizing the rest of the system;
- Secure channel between both sides;
- Secure storage as a mean to deliver full data confidentiality, integrity and freshness;
- Secure I/O.

For a use in telecom industry, where performance is crucial, the "secure scheduling" is on top of the wish list. Meanwhile, we would consider secure I/O as too specifically oriented on smartphones. It is worth reminding that ARM's TEE (i.e., TrustZone) was the first marketed and deployed hardware TEE implementation, aimed at securing mobile payment and other security-privacy sensitive user transactions. In this context, the whole chain of data processing (including I/O such as keyboard and screen data), must be secured. In a general perspective, we would not generalize this I/O security requirement as one of the few must-haves. These security services-functions are shown in Figure 5.

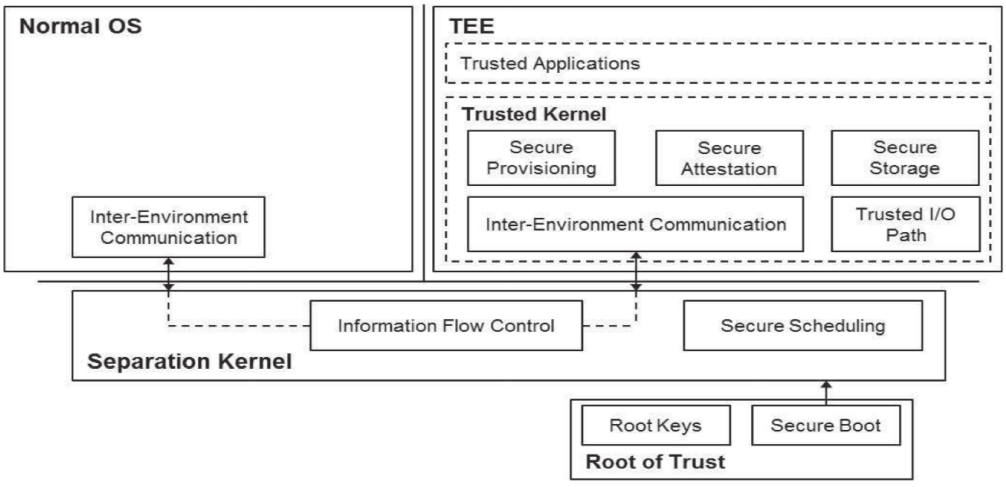

Figure 5: Vision TEE with security functions [133]

A domain expert could notice that this picture depicts a “Trusted Kernel” as offered in the TrustZone. However, not all hardware-based TEE necessarily integrate such kernel. For instance, Intel's SGX microcode handles the different security functions of SGX, but without being called a kernel. The expert would also notice that Figure 5 depicts correctly software-based elaborated hypervisors. Additionally, the shown security functions can be viewed as an exhaustive list which is not necessarily supported in its enterity by by the hardware processor vendors. To illustrate this, the “secure I/O” function is provided by ARM’s TrustZone but not Intel SGX enclave TEE.

5.2.2.1.1.2 TEE promise by partial remote execution

Figure 5 depicts a one-site configuration (all elements of the figure are all located in one single execution platform). However, one can also consider that the TEE concept can be implemented in the most efficient way by using two different execution platforms with an ad hoc split of function execution. The idea is to extract from a possibly abused platform (in the hands of a possible attacker) security-sensitive portions of the software and get them executed at another platform, located in a safe place under visual and full control. To illustrate this, this security method is used in online games, where the game logic is executed in a server at the game publisher. The emote code execution extraction has proven to be the only efficient Digital Rights Management (DRM) solution and it brings security by principle. A fair evaluation of this split execution calls for the need of being able to unambiguously identify the calling parties (e.g., gamers individually), an unforgeable transmission link, a tied internet link and the acceptability of the transmission latency. For the least, the combination of these requirements does not comply in all use cases. Hardware TEE just make that concept easier to reach by localizing the secure part on the same machine.

5.2.2.1.1.3 Software based TEE and Isolation

VM isolation is a common approach in cloud processing. Indeed, virtualisation offers de-facto isolation: the VM user spaces are clearly separated and managed by the virtual memory management unit, under the secure control of the hypervisor. In practice, each VM embarks a complete guest OS, thus exposing a large attack surface where vulnerabilities may reside covertly. By exploiting these vulnerabilities, VM-escape attacks can drill the guest OS layer through system calls to reach the host OS and elevate rights to access to other VM content, resulting in thus isolation breaking. It is worth mentioning that isolation only holds if no vulnerability lies inside one partition or if all system calls are policy-filtered and vetted.

Rule-based execution, such as in [131] [131] [131], allows the specification of a fine-grained security policy for an application or container. These schemes typically rely on hooks implemented inside the host kernel to enforce the rules. If the surface can be made small enough (i.e., a sufficiently complete policy defined), then this is an excellent way to sandbox applications and maintain native performance. However, in practice it can be extremely difficult (if not impossible) to reliably define a policy for arbitrary, previously unknown applications, making this approach challenging to apply universally. Reversely, Google’s gVisor[50] intercepts application system calls and acts as the guest kernel, without the need for translation through virtualized hardware. This architecture allows to provide a flexible resource footprint (i.e., one based on threads and memory mappings, not fixed guest physical resources) while lowering the fixed costs of virtualisation. However, this comes at the price of reduced application compatibility and higher per-system call overhead. Kernel-based virtualisation solutions represent by themselves a vast technical domain, with a lot of competing solutions and their trade off in terms of performance, easy configuration and security. They bring isolation between VMs or containers, but not against the host OS. These rule-based software solutions cannot be referred as TEE as they cannot directly stop introspection attacks.

5.2.2.1.1.4 Positioning hardware-based TEE against TPM

[50] https://gvisor.dev/docs/

Figure 5 shows a secure boot function, which is the core usage of Trusted Processing Module (TPM) [131]. One could view that hardware-based TEE came as the next generation of TPM, bringing more capabilities. If they show some similarities (e.g., processor vendor delivered assets, ability to natively deal with signatures, key generation, etc.), they are aimed at delivering different and complementary services. To make it simple, TEE do not replace TPM. The latter works in ring 0 (kernel) and gets access to all kernel module memory, while some TEE such as the Intel SGX works only at ring 3 (user space) with application memory access only. AMD's SEV works at ring 0 but its ability to deliver a chain of trust is still to be demonstrated. Therefore, if TEE (such as Intel SGX) do not access to ring 0, they will not be able to provide the same software attestation a TPM does. Conversely, the TEE can attest the integrity of the software arbitrarily placed inside it. This integrity attestation does not expand to kernel core parts of the system where TPM do the job. However, TEE have more to sell than the secure boot and chain of trust, a by-product for them. Their main function is isolation where TPM brings natively nothing. Isolation implies that arbitrary codes and the data they process, can reach the secured place and be isolated from the other partitions. Hardware TEE indeed permit to place arbitrary software (user mode software) inside them. Conversely, TPM are only capable to process their hard-coded routines (cryptographic and communication routines for exchanging code signatures, encrypting-decrypting datasets) and finally storing these elements in their Platform Configuration Registers (PCRs), which exist in a restricted number. All TPM routines and data are secured from integrity and confidentiality perspectives, however these guaranties apply only to a closed and restricted perimeter, not to user space software.

5.2.2.2 Remote attestation definition

Remote attestation is a technique that has gained momentum in Telco NFV environment [140] because it generates trust and liability for the NFVI and VNFs. Indeed, this technology has been standardized by ETSI NFV-SEC group [141] as a clear statement of intentions to be adopted.

Remote attestation involves the use of the above mentioned TPM, and it extends the chain of trust outside of the execution platform to involve a trusted third party, who verifies that the conditions are still valid. Figure 6 shows the general concept, where the "Trust assessor" is in possession of a set of good known values or "golden values", that are nothing else than Processor Capacity Reservation (PCR) registers stored in a database of the "Target platform". "Remote verifier" triggers the remote attestation to check the integrity and trust of the platform and upper layers (hypervisor and VNFs). This is as simple as requesting an integrity measurement report to the "target platform" and comparing the values obtained with the golden values. This application remote attestation is possible thanks to the extensions defined by Integrity Measurement Architecture (IMA) [142]. If there is no match, the "remote verifier" will lose the trust in the platform and software. In the NFV ecosystem, the role of "Remote verifier" can be delegated or taken by several entities, from the NFVI provider to the tenant of the VNFs, to the Network Service provider.

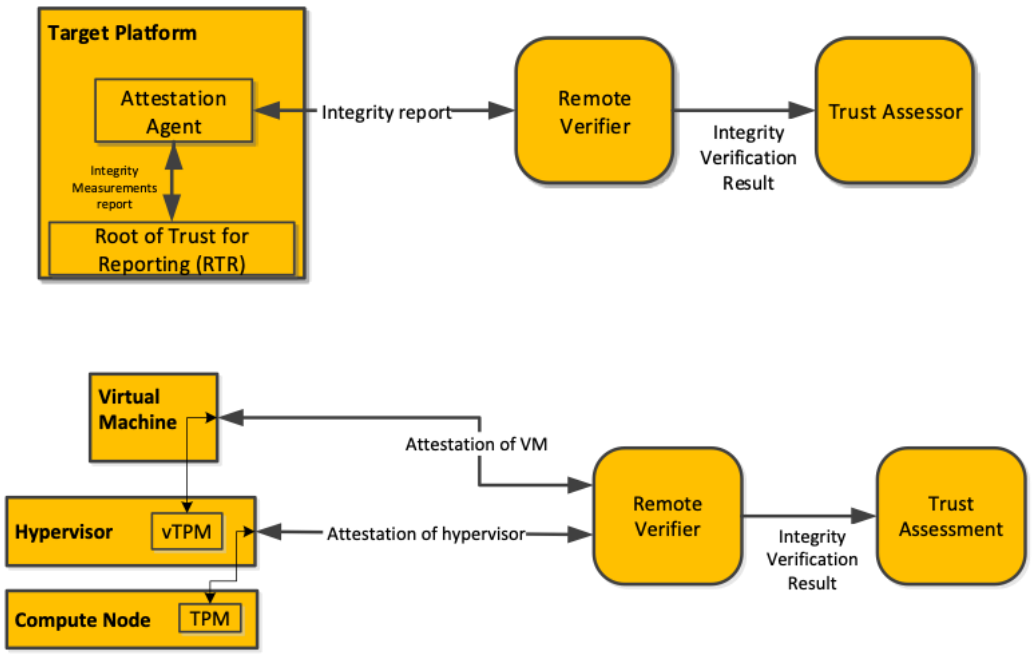

Figure 6: Remote attestation for NFVI and VNFs.

3GPPP adoption of the Service Base Architecture (SBA) and the microservices approach for 5G networks, has generated a lot of attraction in the Containers technology, e.g., Dockers, mainly by its efficiency in resource demand and instantiation deployment. Precisely, the security exposure for this light virtualisation technology, that share kernel functions, demands technologies to provide trust. There are already initiatives [143] in progress to extend the remote attestation to the containers technology to address this lack of trust problems.

One of the most attractive aspects for Remote attestation technology is that it is based on TPM standard [144] (currently in version 2) led by Trust Computing Group, and not dependent on proprietary implementations, such as intel SGX Enclave or AMD trust Zones.

5.2.3 Key Security Functions of Trusted Execution Environments

The early definition of “trusted execution” has appeared in [131]Therein, TEE is defined as a dedicated closed virtual machine that is isolated from the rest of the platform. Through hardware memory protection and cryptographic protection of storage, its contents are protected from observation and tampering by unauthorized parties.” It is worth noting that the definition was proposed before the emergence of hardware-based TEE. Thus, it applies only to pure software based (VM) techniques.

For the industry standardization group GlobalPlatform[131], a TEE is an execution environment that runs alongside but isolated from the device main OS. It protects its assets against general software attacks. It can be implemented using multiple technologies, and its level of security varies accordingly. This definition, although vague regarding to the threats, matches well with the incremental vision of the U.S National Security Agency as cited above. Their statement that several technologies may compete was a good anticipation for the X-86 hardware-based TEEs released thereafter.

For the mobile industry [131], “the set of features intended to enable trusted execution are the following: isolated execution, secure storage, remote attestation, secure provisioning and trusted

path to the on-board NFC radio." This definition is tainted by the mobile phone security and typically the last term refers exclusively to a smartphone.

In view of using a TEE for securing SDN-NFV or 5G software components, the work in [131] identifies the minimal security requirements which needs to be supported by TEEs in order to protect NFV software in a unified setting. The authors define seven key functions, namely: isolation, attestation, sealing, dynamic root of trust, multiple containers, and software and data integrity and confidentiality. Some of these key functions relate only to TPM and are therefore not relevant for TEE. However, the paper brings a concise view of available TEE and TPM (Intel SGX enclave, AMD SEV, ARM TrustZone, TPM 2.0) according to these criteria and this comparison still applies today.

Our definition of a TEE would be to ideally cover a large part of the security functions:

- Isolation (memory partitioning, and access restriction)
- Code confidentiality
- Data confidentiality
- Code integrity
- Data integrity
- Remote attestation of PCB (meaning software authenticity and integrity must be checked before loading)
- Secure provisioning of Hardware TEE (i.e., the genuine TEE-enabled check)
- Secure data sealing-storage.

First, it is worth noting that these guaranties can be all met by a single TEE. Our knowledge and work on Intel SGX 2.0 enclave confirm that statement.

A secondary important wish-list for the adoption of a TEE includes:

- Reduced performance loss.
- Restricted size of the Trusted Computer Base (TCB): A big size hides more potential vulnerabilities to exploit.
- Easy setup workflow: preferably no source code change, ideally automatic.
- Ability to protect several "domains" from the outside world and between them.

This second list is of course of main importance for a use in the telecom industry. Finally, remote attestation from platform to VNFs techniques based on TPM for hypervisors and containers are part of the definition.

5.2.4 State of the art hardware-based TEEs

Appendix B. Survey of existing TEEs makes a deep technical survey of all known TEE technologies as well as associated frameworks offering either a simplified setup workflow or bridging several vendor technologies for a processor independent TEE. This survey investigates the key TEE security functions as listed just above.

5.2.5 Lessons Learned

In the context of INSPIRE-5Gplus, we would prioritize the needs as follows:

- Isolation is provided by software (kernel level) techniques whatever types of virtualization be offered (hardware based (VM based) or OS level based (containers)). They essentially protect the host from a malicious payload (VM or container escape type of attack).
- Introspection attack is defined as the opposite (meaning that the payload must be protected against the host) and is harder to stop. It is the security threat of TEE where the host (or anyone with a grip on the host memory) is malicious against the supported payloads of any type (VM or container). Software based isolation solutions are not capable there. Hardware-based TEE (notably X-86 encryption-based TEEs) deliver a crypto-proven (fully satisfactory) remediation.

- TPM-based remote attestation mechanisms (either hardware based or software based TPM) have a 360° scanning range over the deployed software, from the first executed kernel module at machine start-up to the last application loaded). The code integrity verification is made at load time and not processed at runtime. The TEE reversely operates only at user space (with no access on kernel level code) and deliver integrity per-se for any code run inside. Both security solutions are complementary and exclusive on their abilities.
- Performance (latency) is key and the first selling criteria of any player of the value chain. The new frameworks that tend to ease SGX implementation break Intel's low TCB guidance and show significant performance loss;
- Complex workflow is a strong obstacle in the multi-party open and evolving value chain (Infrastructure provider, network operator, virtual network operator or tenant, VNF vendors, etc.). A third-party TEE implementation on behalf of the code developer-owner is viewed as an enabler. There is a smart solution to devise here in INSPIRE5GPlus, articulating both performance and easy workflow.

5.3 Artificial Intelligence

Although ML and AI, an overarching paradigm, have been utilized in security context for a relatively long time, potential synergies and the realization of these approaches are still at an early stage for massive-scale, diverse and ubiquitous systems such as 5G. Some potential benefits of AI/ML for security provisioning (also leading to some open technical questions) are:

- More effective and efficient security solutions in the cognitive network management;
- Predictive or proactive security functions in the anticipatory networking context;
- Capabilities to cope with a massively increased complexity in 5G network;
- More robust decisions compared to conventional schemes with less measurements during inference stages;
- Inherent support for network automation and ZSM from the security perspective.

Although these are promising for attaining security in 5G networks, there are also technical and practical challenges as discussed below.

5.3.1 Challenges in Artificial Intelligence

Fully autonomous networks: The ZSM framework is envisaged as a next-generation management system that aims to have all operational processes and tasks (e.g., planning and design, delivery, deployment, provisioning, monitoring and optimization) executed automatically, ideally with 100% automation and without human intervention. AI, supported by ML and Big Data analytics, is a key enabler to empower fully autonomous networks.

Challenging threat landscape: The future wireless networks will be characterized by underpinning diverse technologies (e.g., SDN, NFV) and services, the ultra-high traffic volume, the increasing number of vulnerabilities, and the growth in cyber-threats sophistication. Thus, traditional security management approaches may not be enough and need to be rethought to deal with this challenging landscape. By using AI/ML techniques to enable adaptive, intelligent, and autonomous security management, it will allow a timely and cost-effective detection and remediation of cyber-threats.

Access to real data: Due to the tight regulations on data protection, it is not an easy task gaining access to real data. Currently, this issue is addressed by making use of a limited dataset of reference. However, the design, training and validation of AI/ML algorithms highly depend on the availability of datasets. Therefore, the lack of new datasets can impact on how ML algorithms respond to changes over time or as traffic behaviour evolves. In order to prepare the future networks to the multiple scenarios that will be handled, it is important to have mechanisms to generate new and "real" data.

Useful data for ML: The data used for training and validating AI/ML algorithms, even whether it is real or from the limited reference datasets, needs to include some labels. The lack of labelled data

makes infeasible the use of supervised and unsupervised[51] AI/ML algorithms. In the context of future networks, where there will be a huge amount of data, it is impractical to manually label a dataset. Currently, a combination of network security devices is used to identify attacks and label the related flow. However, this process introduces bias to the AL/ML algorithms during the training process, resulting in loss of the expected generality for detecting threats unknown to that tools.

Multiple threat's scenarios: To cover all the possible threats that could be detected by AI/ML algorithms, it is needed to train and validate them with the specific data related to that threat. There are some network-oriented security tools that can be applied to generate the specific data for malware threat identification, network attacks, volumetric Distributed Denial of Service (DDoS), traffic tunnelling, cache poisoning, or Cross site scripting (XSS) threats. However, those tools need specific traffic profiles to be setup to solve concrete problems. Deploying complex enough scenarios to cover all previous cases in a realistic way is extremely expensive in time and effort. This problem is aggravated when new types of threats, malware binaries, targets clients and servers need to be considered.

5.3.2 Trends and Technologies in AI

5.3.2.1 AI for Network Automation

While the use of AI in previous mobile network generations was constrained by resource60 availability, the introduction of virtualisation and edge computing (i.e., Cloud infrastructures, SDN, NFV and MEC) fosters its adoption in the upcoming 5G and beyond networks. To enable zero-touch automation of network and service management in 5G environments, AI is envisioned to support management services for closed loop, such as predictive detection, root cause analysis and decision making [244]. Indeed, AI has the power of unveiling hidden patterns from a large-scale and time-varying data, while providing faster and accurate decisions. The trend of adopting AI, especially ML, into telecommunication networks drives the ITU-T Focus Group on Machine Learning for Future Networks including 5G FG-ML5G[52] to propose a unified architectural framework for ML in future networks. As shown in Figure 6, the unified high-level architecture includes the following components:

- ML pipeline: It is a logical representation of an ML-based network application. The ML pipeline is a set of logical nodes that may include source, Collector (C), pre-processor (PP), model (M), policy (P), distributor (D), and sink;
- ML Sandbox: It is an isolated domain which serves to train, test and evaluate ML models before their deployment into production environment;
- ML Function Orchestrator (MLFO): It manages and orchestrates the nodes in the ML pipeline based on ML intent and/or dynamic network conditions.

[51] In the case of unsupervised algorithms, labels are still needed for validation task
[52] https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx

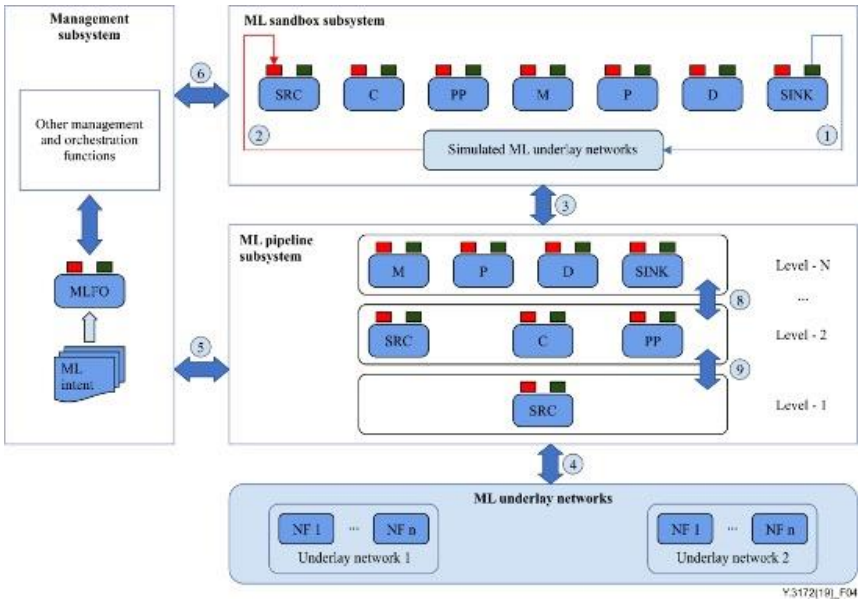

Figure 6: Unified architectural framework for ML in future networks.

The ML algorithms can be leveraged by ZSM to enhance the intelligence of domain and E2E service management [245]. ML techniques can be divided into four main categories, namely:

1. **Supervised:** These techniques require fully labelled training dataset where each sample is considered as normal or abnormal. Anomalies need to be known beforehand, and can be used for the estimation, prediction, and classification of features. The most commonly used algorithms are k-Nearest Neighbours (k-NN), Generalized Linear Models (GLM), Bayesian Networks (BN), Support Vector Machines (SVMs), Artificial Neural Network (ANN), Decision Trees (DT), Hidden Markov Model (HMM), and methods that combine the predictions of multiple learning algorithms;
2. **Semi-Supervised:** Here, training dataset consists of a mixture of labelled and unlabelled samples;
3. **Unsupervised:** These techniques do not need training dataset. Nothing needs to be known about the samples in advance, and these techniques can help identify anomalous behaviours, recognize patterns or reduce the dimensionality of the data. The techniques rely on estimating what is normal and what is abnormal. Legitimate changes in behaviour will have the tendency to generate false positives. Different techniques are used for:
    a. clustering: non-overlapping (e.g., K-means, Self-Organizing Maps), hierarchical (e.g., cluster trees) and overlapping (e.g., Fuzzy C-means, Gaussian mixture models);
    b. Dimensionality Reduction: Feature Extraction (FE), Feature Selection (FS) using, for instance, Principal component analysis (PCA) and Sparse Principal Component Analysis (SPCA);
    c. Anomaly Detection: Rule based systems and Pruning techniques;
    d. Latent Variable models: non-negative matrix factorization;
4. **Reinforcement Learning (RL):** These techniques are based on rewards or cost evaluations to determine if the results reach a certain goal. They learn from the interactions on how to achieve a certain goal and are useful when it is not possible to determine the right answer to a problem. They are based on Markov Decision Process (MDP) that can be model-based (e.g. Dynamic Programming and Monte Carlo) methods and model-free (e.g. Temporal Difference methods such as Qlearning, Sarsa and Actor Critic).

5.3.2.2 AI for Cyber Security

AI is seen as a key enabler for many security-critical applications in 5G and beyond wireless networks [155]. The potential applications of AI/ML techniques in cyber security include the threat detection in

distributed environments (i.e., Cloud, Edge, SDN/NFV); traffic classification (e.g., encrypted traffic); and detection of novel attacks (e.g. differentiating from normal and abnormal network traffic behaviour, as well as behaviour of users, hosts, target systems, business activity). Furthermore, AI/ML techniques are instrumental for: (i) feature selection for improving the performance by reducing the amount of redundant information used during the detection process; (ii) reputation-based detection that detects threats using reputation scores; (iii) decision support and automated response that often rely on AI techniques for improved efficiency and accuracy; (iv) managing alarms (e.g., reducing the number of false positives); (v) detection and prevention of detection evasion techniques; and (vi) improving other functionality such as root cause and risk-based analysis. In what follows, some prospective applications of AI for security in future networks are discussed.

AI/ML for anomaly/intrusion detection: A key security requirement addressed by ML techniques and AI building on them is anomaly/intrusion detection (AID) [149][150][151]. With the huge volume of data generated by 5G infrastructure and users, AID schemes will face challenges to realize context awareness, timely response and decision quality for 5G systems [152]. While addressing these issues, AID schemes will require unified orchestration of the network resources such as computing, networking and storage. AI will be helpful to control and manage computing and communication in this environment, whereas ML can be used to analyse high level statistics for context description, real-time observations, and user feedback, and support these control frameworks. AI approaches can assist the processing of packet-level and flow-level data by supporting efficient classification in the application and network levels. AI-based control and self-learning systems will be useful for analysis of encrypted network data in addition to access and activity detection for intrusion detection [153]. Moreover, ML techniques such as RL is promising for adaptive and robust security schemes against intrusions [154]. The use of AI for the detection of anomalies and security breaches is being studied by many academic and industrial researchers. In what follows, recent advances in research work are reviewed.

In [156] the authors propose an Intrusion Detection System (IDS) for SDN 5G networks that uses ML methods in two critical steps of the detection process: 1) Random Forest (RF) to select optimal subset of flow features by calculating their importance; and, 2) Hybrid clustering that combines K-means++ with Adaptive Boosting for classifying the traffic into different classes of attacks using the previously selected features as input. Random Forest (RF) is a collection of uncorrelated structured decision trees. The importance of a feature is calculated using reference datasets. Adaptive Boosting (AdaBoost) is a ML meta-algorithm that improves performance of other ML algorithms (called weak learners) by combining their output into a weighted sum that determines the final output. It is an adaptive technique in that subsequent weak learners are adjusted in favour of those instances previously misclassified. K-means++ allows choosing the initial values (or "seeds") for the k-means clustering algorithm. K-means clustering partitions *n* observations into *k* clusters with each observation belonging to the cluster with the nearest mean.

The survey in [157] presents three examples illustrating the use of ML for anomaly detection to identify unusual, unexpected or abnormal system behaviour in wireless sensor networks. The authors observed that the use of supervised or unsupervised learning for identifying abnormal behaviours depends on the amount of knowledge, in other words, if the available training data is labelled or not. The examples are:

- a secure MAC protocol based on neural networks to counter DoS attacks in Wireless Sensor Networks (WSN) [158]. The training process uses collision rate, average waiting time of a packet in MAC buffer, and the arrival rate of Request to Send (RTS) and Reject RTS packets (RRTS). An anomaly is detected when the monitored traffic variations exceeds a pre-set threshold. This allows temporarily switching off the affected WSN node to prevent flooding of the entire network;
- online learning techniques to incrementally train a neural network for in-node anomaly detection [159]. It uses Extreme Learning Machine (EML) algorithm that can rapidly train a single-hidden-layer feed forward neural network. The weights between the input layer and the hidden layer and the bias of hidden layer neurons are randomly initialised. The least-

squares method is then used to calculate the weights between the hidden layer and the output layer.

- [160] studies wireless spectrum anomaly detection and proposes using Power Spectral Density (PSD) data to detect and localize anomalies (unwanted or missing signals) in the wireless spectrum using a combination of Adversarial Autoencoders (AAEs), Convolutional Neural Networks (CNN) and Long Short-Term Memory Networks (LSTM);

Work in [161] proposes a MEC-based solution for detecting network anomalies in real-time. It uses deep learning techniques to analyse network flows and policies for providing efficient management of the computing resources needed. To optimize the anomaly detection processes and resource usage, new virtualised resources can be deployed, the deep learning techniques and detection models can be changed, and new functionality deployed such as Deep Packet Inspection (DPI). The solution divides the problem into two modules: first using Deep Neural Networks (DNN) for a first analysis by the Anomaly Symptom Detection module to identify suspicious symptoms; and, then LSTM Recurrent Networks used by the Network Anomaly Detection module to determine if a sequence-of-symptoms is an attack.

[162] devises a solution for improving network monitoring and proactive cell anomaly detection based on dimension reduction and fuzzy classification techniques. Principal Component Analysis (PCA) is used to select the pertinent metrics, kernel-based semi-supervised fuzzy c-means (FCM) algorithm for semi-supervised clustering of SON use cases, and fuzzy classification for anomaly detection. Semi-supervised classification allows considering new behaviour patterns and using priori knowledge.[163] It proposes a strategy for the detection and mitigation of DDoS attacks in 5G network based on the study of variations of the entropy of the network traffic.[164] proposes a deep learning based system to analyse network traffic by extracting features from network flows to identify cyber threats in 5G mobile networks. The proposed system is self-adaptable to the volume of the network flows in real time. An IDS framework deployed at the VMM (Virtual Machine Monitor) in the cloud is proposed in [165]. It uses a fuzzy c-mean clustering mechanism with ANN (Artificial Neural Network) to learn attacks patterns. [166] proposes an approach to attack detection by recognising flow patterns, where network flows are labelled as a benign or attacks using Snort and a learning algorithm is used to classify unlabelled traffic. [167] proposes the use of SVM (Support Vector Machines) and K-means to classify SDN traffic. Other similar works are presented in [168][169][170][171][172][173] and [174].

A major issue that is still not sufficiently investigated by researchers is anomaly detection in encrypted network traffic. According to Cisco [175], currently about half of all traffic on the Internet is encrypted and this will increase over the next few years. End-to-end encryption-based security will probably be included in the beyond 5G standardisation which will mean wide-spread use of encryption. ML and other techniques (e.g., privacy-enhancing technologies, homomorphic encryption) are needed to monitor and detect anomalies in the traffic flows while preserving privacy.

Some works concerning encrypted traffic are starting to be published, such as [176][177][178][179][180]. In [176], the authors investigate the use of supervised learning techniques for traffic classification based on multilayer perceptron, SAE, CNN, and dataset that has over 200,000 encrypted data samples from 15 applications. Similarly, [177] proposes a semi-supervised technique for classifying encrypted traffic. The work in [178] proposes an encrypted malicious traffic detection system based on a sandbox for traffic data collection and labelling malicious and normal flows, and multilayer networks of AEs for feature extraction and training of the classifier model. [179] analyses HTTPS traffic on the client-side using Neural Networks. Similarly, [180] adopts CNN, LSTM and SAE for encrypted traffic classification and intrusion detection.

AI for Moving Target Defence

The static nature of network/service configurations gives the adversaries the advantage of time to explore and exploit the unvarying vulnerability surface. The Moving Target Defence (MTD) has emerged as an effective proactive security countermeasure to address this issue. Indeed, NIST

[181] has identified MTD as an enhanced security requirement for system and communications protection. MTD approaches consist in dynamically changing the attack surface over time in order to increase the attacker's effort and cost. The MTD strategy can be implemented through various approaches including, VM migration, IP address shuffling, replication of software/network resources, and network path diversification. The flexibility and dynamicity brought by virtualization and programmability will facilitate the integration of MTD techniques in 5G and beyond networks, increasing their resiliency to security threats. Nevertheless, it is worth noting that the security benefits of MTD increases the reconfiguration cost and may lead to service unavailability. Hence, finding the balance between the security effectiveness of MTD and the moving cost is essential for their application in 5G networks. The use of AI/ML techniques are considered a promising direction to develop smart MTD mechanisms that can intelligently decide changes to make on the network and service configuration in order to achieve the desired security/performance balance [182]. For example, the authors in [183] leveraged RL to devise an MTD strategy that resist stealthy botnets by periodically altering the placement of detectors.

AI for security classification

Supervised machine learning family use pre-existing labels in the dataset to generate more accurate algorithms. In the cyber security domain and, more specifically, in the case of network attacks, supervised learning has demonstrated to be very useful to classify different attack types [184]. Also, classification can be part of a serialization of algorithms models, starting with anomaly base models and then apply the classification for the abnormal output.

Network Digital Twin

The network digital twin concept refers to a digital emulated copy of the network to simulate network traffic flows and events. The digital twin can be used to generate the specific scenarios for different cyber-attacks, and therefore training and validating AI/ML algorithms properly before using it in a real environment [185]. To this end, the network digital twin is usually composed of the interplay among the communication protocol, device configurations, network topology, application traffic, the physical environment. This new trend allows to have a controlled environment for running experiments that will generate realistic labelled datasets for training supervised AI/ML components and help validate supervised and unsupervised solutions. Apart from that, having a digital emulated copy of the network enables to run and reproduce the experiments as many times as needed in an easy way, only having to choose the models to be deployed, decreasing the complexity of deploying many different threat scenarios.

Telemetry

Regarding the collection of data from the network devices there is a trend called streaming telemetry, also referred as simply telemetry. It is a new approach in which data is streamed from network devices continuously using a push model, providing near real-time access to operational statistics. The main difference between this approach, (being gRPC apparently, the most suitable protocol for this) and the one traditionally used (as Netflow[53]) is that the information retrieved from the devices are defined in standard data models (YANG-based). These data models allow to subscribe to specific data items as it is needed, filtering only the required information from the devices. Therefore, telemetry allows to get data from the devices with a much higher frequency, more efficiently, as well as data on-change streaming, reducing the overhead in the network traffic. This new trend in getting information from the devices is necessity to have more datasets for training and validating AI/ML algorithms and improve the security incident detection in networks.

[53] IETF RFC 3954

5.4 Advanced cybersecurity techniques

5.4.1 Security monitoring optimisation

5G and beyond networks plan to support three specific use cases: extreme mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable and low-latency communications (URLLC). By introducing disruptive concepts, such as SDN and NFV, to the communication network, it promises integrating telecom and information technology into a universal infrastructure by connecting mobile and fixed access networks [186]. We summarize below three principal axes for optimizing the security monitoring in such 5G networks:

- **Optimizing usage resources**: 5G will provide a significant increase in the number of devices connected to the internet, producing a vast amount of data. Security monitoring evidently requires huge resources. It is required to rigorously reduce the number of monitors as well as their resources usage. This can be considered as the prerequisite condition for other optimisations;
- **Optimizing deployment and delivery**: New technologies, for example, SDN/NFV, anything-as-a-service, allow reducing dramatically the time and cost in deployment and delivery security-as-a-service (SaaS). As security-related risks or bugs are identified, new releases can be quickly on-boarded and tested again through full automation in a continuous integration/continuous deployment (CI/CD) chain. Optimizing SaaS depends also on location awareness, content adaptation and caching;
- **Optimizing incident verdicts**: Security incident alerts are traditionally prioritised by classifying into severities, such as critical, high, medium and low. But this does not help to determine what should be resolved first. It is necessary to find the root cause of an incident, since resolving it will eliminate several of the alerts. Detection combined with root cause analysis in SDN/NFV environments is still a big challenge;

We outline three main trends that will help optimize security monitoring:

- Networking Programmability: Programmable networking devices, like routers or switches, can satisfy some of the security monitoring and reaction requirements. They can be used in early abnormality detection, as well as in network traffic classification and optimization [187];
- Intelligence-driven security: Analytics for enhanced security operations using ML/AI to develop intelligence-driven security capabilities can provide more accurate detections. Fast big data technologies can help real time-security monitoring deal with the massive collection and analysis of information [188];
- Zero-trust model: Multi slicing concept allowing different network slices that share the same infrastructure including heterogeneous devices from untrusted providers. One UE may even belong to different slices depending on the application running on it. Security monitoring in such a network must effectively have zero trust: everything inside or outside of the network perimeters need to be verified. The zero-trust model, with the principle of "never trust, always verify", addresses all threats, not just the ones that are easy to articulate.

5.4.2 Cyber Threat Intelligence and threat data sharing

ENISA has issued a recommendation for the creation of 5G Cyber Threat Intelligence (CTI) and collaborations between stakeholders as a basis for future knowledge capturing and knowledge dissemination in the area of 5G threat analysis[54]. Softwarization, programmability, AI, massive IoT, etc. all introduce new vulnerabilities. These are even more important due to the expected increase of

[54] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport

bandwidth and the enabling of new critical applications. The sharing of CTI is necessary, as well as improving the automated use of it, to prevent and better respond to these new menaces. These subjects have not been investigated in the context of 5G or beyond.

For gathering CTI, several methods and techniques can be used that include honeypots and deceptive technologies [189]; darknet or network telescopes [190]; social and darknet mining [191]; intelligence sharing [192] and SIEMs (log monitoring and analysis) [193] [232]. These different techniques need to be rethought and adapted for capturing CTI considering the requirements and architecture of 5G and beyond networks.

For sharing CTI, the most popular formalism is the STIX standard I[55] for describing the threats (promoted by ENISA[56]) and the TAXII protocol[57].

5.4.3 Security and Service Level Agreements

One of the key objectives of 5G technology based on SDN/NFV paradigms is the provision of services guaranteeing a certain level of quality (including reliability, availability, performance, security, privacy, etc). Insufficient performance or resiliency within these services have been identified as major obstacles for the deployment of 5G networks. These guarantees are in general reflected in Service Level Agreements (SLAs) signed by the customers and service providers, or between different stakeholders and tenants. SLAs are formal contracts documenting the features of delivered services and related quality expectations, called Service Level Objectives (SLOs). Moreover, they explicitly consider responsibilities, obligations, service pricing and penalties in case of agreement violations. Security SLAs is a subset of the global SLA that tackle the security and compliance engagements for both parties including, in the case of 5G networks [194], aspects related to both the infrastructure and the provisioned services (e.g. infrastructure security, resiliency controls, data protection).

These SLAs are typically written in natural language (often in a strict legal notation). Despite the strong interest in security and the existing efforts towards standardization, Security-oriented SLAs (SSLAs) are still far from being adopted. A shared format for Security SLAs including the representation of security attributes and security guarantees is not yet available. A machine-readable format of security SLA (e.g. the SPECS XML SLA Framework[58]) is a challenging task that can be very useful during development and deployment phases to ensure that deployed 5G services respect the specified security requirements. This same Security SLA can also be the input for an automated and adaptive security monitoring solution that can assess the security of deployed 5G services and detect any potential violation at runtime.

This automation in Security SLA management can increase business opportunities of 5G service providers and operators and better manage their customer expectations. Service providers and operators are being constantly compared and evaluated to competitive organizations that a customer works with. One way to stand out from all other organizations is by providing excellent customer service reinforced by a solid SSLAs that can be easily checked. Besides, if machine readable, they will allow to specify clear and measurable guidelines that can be audited in more accurate manner and enhance responsiveness to potential security incidents.

5.5 Distributed Ledger Technologies

Vulnerability of personal data and individual identities is becoming an issue for European entities involved in worldwide businesses. The missing trustiness is partly produced by the low levels of

[55] https://stixproject.github.io/
[56] https://www.enisa.europa.eu/publications/improving-recognition-of-ict-security-standards/at_download/fullReport
[57] https://taxiiproject.github.io/
[58] https://bitbucket.org/specs-team/specs-utility-xml-sla-framework

authentication assurance, as well as the low impact of trusted enrolment and identification technologies and processes. Recording and the ability of tracing the events, also known as data provenance, becomes a key characteristic.

Certified provenance can help detect access violations to systems whereas containing sensitive information about the data sources and the users. Obtaining certified/trusted/assured provenance is still a critical issue in terms of securing not only the data but the provenance data associated to it.

Even in privacy-preserving scenarios, accounting is a feature that is needed for several reasons. In these scenarios and thanks to data provenance, the original identity of the data owner can be revealed under certain requirements or policies. Therefore, data and provenance data need to be hard linked so that the tracking and audition can be applied under any circumstances. There is in general a lack of data provenance mechanisms for privacy-preserving applications. On the other hand, these future mechanisms can be also used to audit control-plane in order to provide a calculation on the amount of trust and liability of the architecture per se; in particular, of each element supporting it.

Some previous H2020 European Research projects like ReliAble euRopean Identity EcoSystem (ARIES)[59] provide user-friendly and efficient authentication mechanisms while preserving user privacy and data protection rights by means of mobile virtual identifiers (vIDs) and an Anonymous credential system. This way exchanged data can be fully accounted before sharing. In a Non-Interactive Zero Knowledge Proof (NI-ZKP) mechanism, the data can be processed while preserving the source privacy while offering the data provenance attached to the data as something trustable by a third party, therefore following a Self-sovereign identity management approach.

Due to its nature in terms of trustiness responsibility distribution based on harnessing the computational capabilities of honest nodes, blockchain technologies are now envisioned as the key enablers to avoid manipulations on the data exchanged, data provenance thanks to a shared, distributed and fault-tolerant database.

Blockchain network can be simplistically seen as a distributed public ledger where every transaction is witnessed and verified by the nodes in the chain. In addition, every single node in the chain acts as a service enabler which ensures scalability and robustness.

Among the well know platforms available for DLT one can find Corda Enterprise R3[60], hyperledger[61] or the Ethereum Alliance[62]. Others like Xeniro [63] are more related to NFV and 5G technologies, also the research community has started to relate DLT to the 5G environment [246].

5.6 Dynamic Liability and Root Cause Analysis

In future networks, trust and liability will be fostered through integration of novel mechanisms supporting confidence between parties, liability for security incidents and compliance with regulation. These mechanisms will provide the means for liability contextualization, imputability and verifiability at different stages of 5G services (pre/post issuance, during service operation, and for post mortem forensic investigations). In particular, they will form a framework in which each party is aware of its own liability level regarding the other parties and is able in the same way to deliver post-issue evidences (or post mortem in case of major failure) to qualify which party has not delivered its duties.

[59] https://www.aries-project.eu
[60] https://www.r3.com/
[61] https://www.hyperledger.org/
[62] https://entethalliance.org/
[63] https://www.xeniro.io/

5.6.1 Dynamic liability mechanisms for multi-tenant environments

While trust modelling and management provide the needed confidence in communication systems and their security management in next-generation networks, it does not prevent their breach and failure and does not render what happened due to whom. Thus, it is crucial to address the question of liability and responsibility for faults and failures in 5G networks. In such distributed and cooperative context, two levels of liability can be considered, (i) liability between cooperative entities, and (ii) the joint liability of cooperative entities regarding service customer. Novel solutions for defining liabilities and detecting the causes of security breaches need to be developed for ensuring liable E2E delivery of 5G services.

Liability management mechanisms need to be devised by investigating graph-theoretic techniques to dynamically investigate the coverage of security objectives by systems in 5G networks. This framework may use Risk Assessment Graphs (RAGs) as a model of risk analysis (which is a graph-based model adaptable to the system evolutions or dynamicity over the time). It delivers mathematical propagation of impacts and risks expositions between components and allows dynamic modelling and re-evaluation of security exposure of the global infrastructure. Furthermore, dynamic liability chains will be developed (for the multi-tenant environment case) and analysed for their usability and impact on security, the effectiveness of the dynamic approach on liability, and the compliance with the regulatory policies in future networks.

These mechanisms are coupled with complementary approaches discussed in other sections, namely: (i) Root Cause Analysis potentially combined with Remote Attestation; (ii)Path Proof techniques and smart 5G security management to establish which component (in case of security incident) may have exposed one or more of its security objectives (accountability); and (iii) technologies available around the smart contract and Trust Level Agreement (TLA) based schemes to establish which commitment has been broken.

5.6.2 Novel VNF labelling and manifest extensions for characterization of VNF commitments and liabilities

To support and facilitate liability in system components (e.g. VNFs, IoT devices), new labelling schemes for high-dimensional secure and trusted NFV-based solutions fostering the crucial user and market confidence in their deployment, adaptation and usage are important tools. Such MANIFEST designs may be extended to describe commitments of each actor within the component life cycle in 5G and Beyond. Such a labelling scheme with proper MANIFEST extension(s) will support different roles and functions in a component lifecycle and formalize the condition of usage in terms of delivery, qualification and operation of a specific component:

- The supplier can define the embedded features and API available for its proposed VNF or IoT device and descriptions in the labelling syntax.
- The entity in charge of qualification can describe how the VNF is consistent against injection of system call errors or fuzzing of its interfaces (i.e. how to describe the qualification of software stability and propagation level of its instability to other chained components). Qualification entities can also describe how the IoT device is protected against eavesdropping or recommend rules or functions that can be hosted by surrounding object or edge devices in order to enhance the security of IoT.
- The entity in charge of VNF operation can describe and provide commitments regarding the way it will orchestrate and chain VNFs to address the potential instability challenges (e.g., the usage of some APIs could be restricted to keep the VNF in nominal state).

Such techniques will provide fundamental liability analysis capabilities. When faults occur in production for a Service or a Vertical due to major failures (e.g., hidden API, undetected instability, restriction of usage not applied, parameter range outside recommended values, etc.), this embedded contract will serve as a basis for liability imputation.

5.6.3 Smart contracts, Proof of Transit and TLA compliance schemes for liability

Although MANIFEST extension(s) and labelling are important fundamental tools for defining and monitoring liability, novel complementary techniques are essential. Smart contracts working with MANIFEST extension(s) and labelling is a potential technology to establish TLA and responsibility of each party or between components in case of TLA violation. The TLA requires new Remote Attestation and Path Proof protocols that aim to deliver compliance evidences with specific constraints in a feasible and efficient manner. Therefore, new proof of transit methods in 5G networks, for critical vertical sectors, are important future technologies. They should verify the isolation of the security solutions for the tenant maintaining the coherence and security within each domain. These techniques work hand in hand with Root Cause Analysis (RCA) techniques that identify the cause and determine the responsibilities as described in the next section.

5.6.4 Root Cause Analysis (RCA)

Understanding the root cause of an observed symptoms in the context of security or fault identification/mitigation, in a complex and distributed system like 5G networks, has been a challenge for a long time. The main issues revolve around development and implementation of appropriate mechanisms pinpointing root causes, which can handle large amounts of data and may provide timely and actionable feedback. There are two critical dimensions of RCA in that regards: scalability and timely reaction (sometimes even real-time).
The main elements of RCA operation are as follows (shown in [195]):

- **Model construction**, where the RCA model is constructed by integrating domain knowledge, system knowledge and observations. there are two broad families of RCA models: deterministic vs probabilistic. The latter considers the uncertainty in the observations, domain knowledge and outcomes in the RCA process [196]. Models have their characteristics such as size, inference structure, and manual vs automated generation.
- **Inference**, where explanations are generated based on observations of the root-cause(s),
- **Model update**, where the model is updated based on the evolution of the diagnosed system and observations.

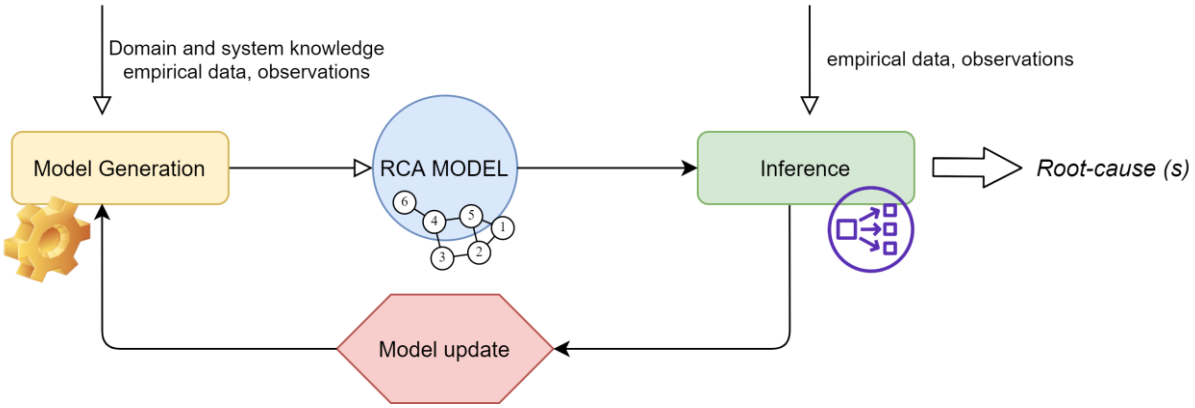

Figure 7: RCA process.

5.6.5 General RCA Challenges

RCA has various challenges when considering their application in 5G security.

- **Fast online root-cause analysis:** Although there are several very effective RCA techniques, RCA schemes for 5G security should be fast and compatible with online event processing in multiple use cases. This is crucial for rapid and timely response based on RCA outcome(s). However, this is not a trivial objective;

- **Complexity and fast evolving systems:** Another challenge is the changing system structure which needs to be reflected in the RCA model. For 5G systems, the evolution pace can be fast and may cause a drift between the model representation and actual system in the field. There is a trade-off between how often the model update should be updated and the related performance overhead;
- **Learning techniques:** Learning approaches are helpful for the cases where no domain knowledge is available to construct an RCA model. In that case, they can process the raw data of the monitored system to come up with an appropriate model. Learning algorithms can learn both structure and parameters or one of them as described in the following subsections;
- **Efficient graphical models relying on Bayesian networks (BN):** Probabilistic models in the form of BN or derivatives are popular tools for RCA. However, they do not have specific advantages over classifier-based models: learning Bayesian Networks is NP-complete [197]. Therefore, efficient approximate models are necessary in that domain.

Current status of the use of ML for RCA in 5G

RCA is a common method used for identifying the root causes of faults or problems. RCA in 5G networks certainly inherits the RCA-related works performed for traditional cellular/wireless networks. However, the actual analysis remains a slow and manual (or partly manual) process often carried out by the operators' experts who are the main actors analysing and correlating multiple data sources, such as network traces, alerts, logs, key performance indicators. Different ML approaches have been applied, namely Artificial Neural Networks, Fuzzy Set Theory, Rule Based Systems and Bayesian Networks [198]. Common network indicators that can be used for the analysis are as follows:

- Reference Signal Received Power (RSRP): the power of the LTE Reference Signals spread over the full bandwidth and narrowband, measured in dBm.
- Reference Signal Received Quality (RSRQ): the ratio between RSRP and the wideband received signals from all base stations in the carrier bandwidth plus thermal noise, Received Signal Strength Indicator (RSSI), measured in dB.
- Handover Success Rate (HOSR): the ratio between successful handover attempts to the total number of handover attempts, measured in percentages.
- E_RAB_RET: the ratio of successful completed connections to the total number of connections, measured in percentages.
- Signal to Interference plus Noise Ratio (SINR): the ratio between the power of the desired data signal to the sum of the inter cell interference powers plus noise, measured in dB.
- AVG THROUGHPUT: the average user throughput, measured in bits/time interval.
- 50_PERC_DIST: depicting where the users are mostly located with respect to the cell base station.

The diagnostic accuracy remains relative because it depends highly on the learning data set as well as the selection of network indicators. The following paragraphs describes some of the work related to mobile networks.

The authors of [199] propose a detection and diagnosis framework based on automatically constructed profiles. They use monitoring radio measurements and other performance indicators for comparing them to the normal behaviour. A statistical learning process based on KPI levels allows determining how well the current behaviour corresponds to a profile. The diagnosis follows the reasoning of an operator that used previous fault cases and tries to find the best matching root cause.

In [200], the authors propose an automatic diagnosis system based on unsupervised techniques for Long-Term Evolution (LTE) networks. They use an iterative process based on self-organizing maps (SOMs) and Ward's hierarchical method. Statistical behaviour analysis allows determining the clusters and an adjustment process improves the accuracy of the diagnoses. The process is divided

into three steps: First, unsupervised SOM training is used for an initial classification of the high-dimensional KPIs. It is a neural network capable of learning from a set of unlabelled data reducing it to a two-dimensional map of neurons that preserves the topological properties of the input data and which can classify new KPI data by finding the closest neurons. Second, after applying SOM, all the neurons in the SOM will be clustered into a certain number of groups using an unsupervised algorithm based on Euclidean distance, i.e. Wards hierarchical method. Finally, experts need to analyse and identify the fault causes to label each cluster. In this way, new KPI input can be mapped to a neuron in SOM, and the label of the cluster the neuron belongs to will identify the fault and causes.

In [201], the same authors propose a self-healing algorithm that analyses time series of cell metrics under problematic situations to determine the fault cause. It considers the time dependence of network metrics and the impact of the fault on neighbouring cells and can learn from new fault occurrences.

Future trends of ML for RCA in 5G

The RCA is still a must for any cellular operator and should be an automated process. The future trend will be related to the following directions:

- Learning and diagnostic approaches: ML approaches will be continuously integrated, especially Deep learning algorithms.
- "Good" datasets for the learning phase: Once 5G reaches a wide deployment, the dataset sources will become more abundant. The operators will thus have more datasets for the learning phases and tests.
- Selection of the most relevant network indicators: The release of new tools, applications and hardware devices are providing more relevant network indicators which will be very useful. In the case where there are too many indicators, and the decision of the algorithms or the experts become too time-consuming, PCA (Principal Component Analysis) can be considered.

All of these will provide improved analysis capabilities with a higher accuracy for identifying the root causes of security and performance issues.

5.6.6 Root Cause Analysis for SDN-NFV based infrastructures

The advent of programmable networks, with SDN and NFV is accelerating faster and faster the transformation of current network, leading to rethink network and service management and operations.

SDN and NFV are thought to be "better together" by the IT and telecommunication industry. Nevertheless, the introduction of the SDN controller within the NFV is still under discussion, evidenced by the lack of consensus on the position of the SDN controller within the NFV framework [202].

Fault management operations particularly emerge as cornerstone to provide the SDN and NFV promises. In fact, the SDN controller whether it is centralized or distributed is a point of failure, and thus its underlying network is impacted.

Moreover, networking services will rely on a dynamic placement and migration of the VNFs as well as an elastic usage of the compute, storage and networking resources.

Therefore, in SDN and NFV, the high network dynamicity provided by SDN becomes even higher when combined with NFV, since the VNF can be scaled, instantiated, deleted, and migrated. Thus, service dependencies from the underlying resources are in a continuous change and need dynamic management. In response to these challenges, we focus here on the diagnosis as a key operation among others to ensure the smooth functioning of networking services relying on SDN and NFV principles.

5.7 Identified limitations and gaps: prioritization

During the analysis of the trends and technologies, we identified specific gaps. The identified gaps will be addressed in the course of INSPIRE-5Gplus project. Section 3 describes the security requirements of the various 5G verticals that are considered. The use cases that are being developed have been grouped into specific domains to offer high-level view on their specific security needs. Throughout the analysis and description of prior work, the following gaps will be addressed with the development of INSPIRE-5Gplus security enablers. Table 4 summarizes the most critical for 5G services:

Technology	Security Gap. Progress axis
Artificial Intelligence and Machine Learning	• Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats. • Investigate one unexplored space: AI-based threat detection over encrypted data flows (as 50% of today traffic is encrypted). • Tackle with the concept of Network Digital Twins. • Tackle with the concept of (data) streaming telemetry (based on Yang-based model) to ease and experiment the selection and processing of most relevant and restricted data flow (best qualifiers).
Authentication	• Lack of coordinated authentication processes for services and consumers for multi-domain applications
Automation and Zero-touch Service Management	• Define a minimal viable ZSM, avoiding the "calamity of over-arching solutions", which spans over a complete E2E slice over several domains. Practical implementations delivering measured improved security are to be drawn and implemented. • Comprehend the research and standardization works by ETSI and ITU-T: GANA architecture, ZSM concept and its derivations at ONAP and OSM frameworks, ENI working group, ITU FG-ML5G and its unified high-level architecture (ML pipeline, ML sandbox and ML function orchestrator).
Cyber threat intelligence and data sharing	• Define the ad hoc usable sources for cyber threats to operators. • Devise how to move from a static threat landscape to evolving or new threats. • Consider the benefits of new risk assessment frameworks of complex ICT systems with notably the progress on risk assessment graph.
DLT	• Devise pragmatic paths to DLT usage over the networks over three possible implementations: DDoS attacks, AAA and SLA management.
Dynamic Liability and Root Cause Analysis (based on ML)	• Deliver fast and timely faulty source information. • Ability of the RCA to grasp the network structure (model representation) ever evolving. • Devise the most relevant learning and diagnostic methods-approaches with a special focus on Deep learning • Reduce the domain space to highly signing datasets only. • Define the most relevant network status indicators, possibly with the help of Principal Component Analysis.
Formal method applied to network authorization enforcement	• Devise and define how these techniques (as defined in the SoTA) can be deployed in a multi VNF where security is AI-defined. • Confront and define possible convergence (associated use) for the paradigms of formal method and AI processing.
MEC security	• More exposed to introspection, MEC security is a main concern. Devise a resource-efficient security solutions resident in the MEC
MTD and Cyber Mimic Defence Techniques	• Devise the real benefits of these techniques (which by-default generate network structure automatic variations and instabilities) when applied in a complex multi-domain, multi-operator, multi-tenant and cross slice scenario (with their set of security constraints). • AI for MTD

Multi-MEC Security	• Lack of integration and inter-working of MEC and associated MEC platform management
NFVI, VNF, MANO and interface security (API	• Investigate the security and the performance of latest controller North Bound and South Bound APIs including NETCONF, TAPI, JOX
SDN security, SD-SEC and SECaaS	• Investigate how software security service (dealing with Identify, Protect, Detect, Respond and Recover) can be expanded in a multi domain/multi-tenant environment.
Secure 5G radio access	• Devise and define a smart (more secure for delivering both confidentiality and integrity, performance acceptable, easy workflow) E2E data flow encryption.
Securing Artificial Intelligence - SAI	• Embrace, comprehend and advance the works made at ETSI Industry Specification Group on securing artificial intelligence 3ISG SAI)
Security service level agreement	• Define an open (i.e., adaptive to any liable parties of the agreement), dynamic (i.e., QoS or security rules can evolve) and secure SLA template management framework enabling SLA in the context of the varying 5G services and of the complexity and size of a service value chain (made up of several suppliers).
Security solutions oriented towards verticals	• Devise solutions for securing network slicing and hardware root of trust (when highly security-sensitive OT in vital infrastructure are concerned)
Service isolation	• Lack of secure hardware infrastructure to deploy isolated services.
Trust models and liability analysis in 5G	• Devise a trust management solution and its associated processed metrics, inputs, aggregation methods delivering accurate and pertaining trust level assessment in the context of 5G complex service value chain. • Grasp the concept of forwarding accountability and strong accountability concepts to elaborate trustworthiness. • Grasp the work related to liability expressiveness (and associated domain specific language) as well as delegation of obligation • Grasp the practical aspects on defective algorithm accountability, packet proof of transit (how effective, benefits and trustworthiness of brought information.
Trusted Execution Environments	• Define a smart way to bring to network functions provable integrity and confidentiality guaranties, through a by-default, zero-touch workflow, generating low overhead.
Vertical CCAM	• Lack of integration and leveraging CCAM customized AI/ML for greater Quality of Experience and Service Availability

Table 4: Identified limitations and gaps

6 Conclusions and next steps

In this deliverable, we presented the current security landscape of 5G networks as well as the evolution of trends, focussed on their security and requirements. The analysis was divided into domain-specific sections. Each section addressed a specific topic related to the threat landscape of 5G networks.

Section 1 described the objective of this deliverable and its role for other work packages in the INSPIRE-5Gplus project.

Section 2 detailed the current security landscape of 5G networks. The section described the classification criteria, the architectural requirements, the key enabling technologies, the 5G vertical domains. It concluded with the description of the threat taxonomy that will be used within the project.

Section 3 described the security requirements of 5G networks. The section started with a brief introduction to the definition of security requirements, as well as the security requirements elicitation process. The different types of security requirements were defined and then were related to the project. We grouped the use cases of the project into domain-specific vertical to offer an initial security analysis. Additionally, we developed a questionnaire for eliciting the security requirements from stakeholders in 5G. We began the process of the dissemination of the questionnaire to the relevant stakeholders. The results of the analysis will be presented in D2.2 (Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security).

Section 4 presented the current status of 5G. The section started with a description of the state-of-the-art solution for 5G networks. Then, we described the relevant standardization efforts that address the security of 5G networks. Finally, we gave an overview of the relevant 5G projects of the European Commission divided into the research phases of 5G.

Section 5 described the future trends and technologies that are motivating the development and deployment of 5G networks. We described the following trends and technologies:

- Automation and Zero-touch Service Management
- Trusted Execution Environments
- Artificial Intelligence and Machine Learning
- Advanced cybersecurity techniques, such as security monitoring optimization, cyber threat intelligence and data sharing, security and service level agreements
- Dynamic Liability and Root Cause Analysis

The section concluded with a description of the identified limitation and gaps of such technologies in the domain of 5G networks.

The work that has been carried out in the scope of Work Package 2 during the first 6 months of the INSPIRE-5Gplus project that covers security requirements elicitation and investigation of research aspects that need to be addressed in the context of this project. In most cases, the partners involved have been able to identify security issues and technical challenges that can be addressed by the novel security enablers that the project envisages developing.

REFERENCES

[1] Bernardo, D. V., & Chua, B. B. (2015, March). Introduction and analysis of SDN and NFV security architecture (SN-SECA). In 2015 IEEE 29th international conference on advanced information networking and applications (pp. 796-801). IEEE.

[2] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. IEEE Communications Magazine, 55(8), 211-217.

[3] Yang, W., & Fung, C. (2016, June). A survey on security in network functions virtualization. In 2016 IEEE NetSoft Conference and Workshops (NetSoft) (pp. 15-19). IEEE.

[4] Hu, Z., Wang, M., Yan, X., Yin, Y., & Luo, Z. (2015, February). A comprehensive security architecture for SDN. In 2015 18th International Conference on Intelligence in Next Generation Networks (pp. 30-37). IEEE.

[5] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013, November). SDN security: A survey. In 2013 IEEE SDN For Future Networks and Services (SDN4FNS) (pp. 1-7). IEEE.

[6] Hussein, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2016, April). SDN security plane: An architecture for resilient security services. In 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW) (pp. 54-59). IEEE.

[7] Kreutz, D., Ramos, F. M., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55-60).

[8] Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). Survey on multi-access edge computing for internet of things realization. IEEE Communications Surveys & Tutorials, 20(4), 2961-2991.

[9] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698.

[10] Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657-1681.

[11] ETSI GS MEC, ETSI GS MEC 003 V2.1.1 (2019-01); Multi-access Edge Computing (MEC); Framework and Reference Architecture. ETSI, 2019.

[12] ETSI GS MEC, ETSI GS MEC 002 V2.1.1 (2018-10) ; Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements. ETSI, 2018.

[13] ETSI GS MEC, ETSI GS MEC 010-2 V1.1.1 (2017-07); Mobile Edge Computing (MEC); Mobile Edge Management; Part 2: Application lifecycle, rules and requirements management. ETSI, 2017.

[14] ETSI GS MEC, ETSI GS MEC 011 V1.1.1 (2017-07); Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement. ETSI, 2017.

[15] ETSI, MEC in 5G networks; ETSI White Paper No. 28. Jun-2018. on: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[16] S. Lal, T. Taleb, and A. Dutta, “NFV: Security Threats and Best Practices,” IEEE Communications Magazine, vol. 55, no. 8, pp. 211– 217, 2017.

[17] Giorgini, P. and Mouratidis, H. (2011). Secure tropos: A security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering, 17(02):285–309.

[18] Nuseibeh, B. and Easterbrook, S. M. (2000). Requirements engineering: a roadmap. In ICSE - Future of SE Track.

[19] Mead, N. R. and Abu-Nimeh, S. (2015). Security and privacy requirements engineering. Handbook of Research on Emerging Developments in Data Privacy, pages 199–215.

[20] Solms, B. (2005). Information security governance: Cobit or iso 17799 or both? Computers & Security, 24(2):99–104.

[21] Pohl, K. (2016). Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam-foundation level-IREB compliant. Rocky Nook, Inc.

[22] Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., and Sommerlad, P. (2013). Security Patterns: Integrating security and systems engineer- ing. John Wiley & Sons.

[23] Herrmann, D. S. (2002). Using the common criteria for IT security evaluation. Auerbach Publications, Boca Raton, FL.

[24] Mead, N. R. and Stehney, T. (2005). Security quality requirements engineering (square) methodology. ACM SIGSOFT Software Engineering Notes, 30(4):1–7.

[25] Tondel, I. A., Jaatun, M. G., and Meland, P. H. (2008a). Security requirements for the rest of us: A survey. IEEE software, 25(1).

[26] Viega, J. (2005). Building security requirements with clasp. ACM SIGSOFT Software Engineering Notes, 30(4):1–7.

[27] Giorgini, P. and Mouratidis, H. (2011). Secure tropos: A security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering, 17(02):285–309.

[28] Sánchez, O., Molina, F., Garcia-Molina, J., and Toval, A. (2009). Modelsec: a generative architecture for model-driven security. J. Univ. Comput. Sci, 15(15):2957– 2980.

[29] Ma, Q., Johnston, A. C., and Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. Information Management & Computer Security, 16(3):251–270.

[30] Teodoro, N., Goncalves, L., and Serrao, C. (2015). Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. 2015 IEEE Trustcom/BigDataSE/ISPA.

[31] Haley, C. B., Moffett, J. D., Laney, R., and Nuseibeh, B. (2006). A framework for security requirements engineering. Proceedings of the 2006 international workshop on Software engineering for secure systems - SESS ’06.

[32] Pourzandi, M. and Apvrille, A. (2005). Secure software development by example. IEEE Security and Privacy, pages 10–17.

[33] Bockelmann, Carsten, et al. "Massive machine-type communications in 5G: Physical and MAC-layer solutions." IEEE Communications Magazine 54.9 (2016): 59-65.

[34] Shunliang Zhang, Yongming Wang, Weihua Zhou, Towards secure 5G networks: A Survey, Computer Networks, Volume 162, 2019, 106871, https://doi.org/10.1016/j.comnet.2019.106871.

[35] 3GPP Security architecture and procedures for 5G system 3GPP TS33.501 Release 15 (2018)

[36] Wang, M., Yan, Z. A Survey on Security in D2D Communications. Mobile Netw. Appl 22, 195–208 (2017). https://doi.org/10.1007/s11036-016-0741-5

[37] EC NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, Oct 2019.

[38] B. Yigit, G. Gür, B. Tellenbach and F. Alagoz, "Secured Communication Channels in Software-Defined Networks," in IEEE Communications Magazine, vol. 57, no. 10, pp. 63-69, October 2019.

doi: 10.1109/MCOM.001.1900060.

[39] Open Networking Foundation, “Threat Analysis for the SDN Architecture,” TR-530, Version 1.0, July 2016

[40] ETSI GS NFV-SEC 001. NFV Security; Problem Statement. V1.1.1, Oct. 2014.

[41] V. Lefebvre, G. Santinelli, T. Muller, J. Gotzfried. Universal Trusted Execution Environments for Securing SDN/NFV Operations. ARES 2018, August 2018.

[42] ETSI GS NFV-SEC 003. Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance. V1.2.1, Aug. 2016

[43] M. Hataba and A. El-Mahdy, "Cloud Protection by Obfuscation: Techniques and Metrics," 2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Victoria, BC, 2012, pp. 369-372. doi: 10.1109/3PGCIC.2012.18

[44] C. S. Collberg and C. D. Thomborson. Watermarking, Tamper-Proofing, and Obfuscation: Tools for Software Protection. IEEE Transactions on Software Engineering, 28(8): 735 – 746, August 2002.

[45] G. Wurster, P. C. van Oorschot, A. Somayaji. A Generic Attack on Checksumming-based Software Tamper Resistance.

[46] C. Gentry. Fully homomorphic encryption using ideal lattices. (STOC’09), pp. 169 – 178, 2009.

[47] John Knight. 2012. Fundamentals of Dependable Computing for Software Engineers (1st. ed.). Chapman & Hall/CRC.

[48] E. Börger. The ASM method for system design and analysis. A tutorial introduction. In B. Gramlich, editor, Frontiers of Combining Systems, volume 3717 of Lecture Notes in Artificial Intelligence, pages 264–283. Springer, 2005.

[49] A.P. Ravn, S. Vighio and J. Srba. A Formal Analysis of the Web Services Atomic Transaction Protocol with UPPAAL. ISoLA 2010. Lecture Notes in Computer Science, vol. 6415, 2010. Springer, Berlin, Heidelberg

[50] B. Boyer, K. Corre, A. Legay, S. Sedwards. PLASMA-lab: a flexible, distributable statistical model checking library. QEST 2013. Lecture Notes in Computer Science, vol. 8054, 2013. Springer, Berlin, Heidelberg

[51] C. Basile, D. Canavese, C. Pitscheider, A. Lioy, F. Valenza. Assessing Network Authorization Policies via Reachability Analysis. Computers & Electrical Engineering, Vol. 64, pp. 110 – 131, Nov. 2017.

[52] A. Panda, O. Lahav, K.J. Argyraki, M. Sagiv, S. Shenker. Verifying isolation properties in the presence of middleboxes. CoRR abs/1409.7687, 2014.

[53] L. De Moura, N. Bjørner. Z3: An efficient SMT solver. In Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2008. Lecture Notes in Computer Science, vol. 4963, 2008. Springer, Berlin, Heidelberg

[54] S. Spinoso, M. Virgilio, et al. Formal Verification of Virtual Network Function Graphs in an SP-DevOps Context. ESOCC 2015. Lecture Notes in Computer Science, vol. 9306, 2015. Springer, Cham

[55] M. Flittner, J. M. Scheuermann, R. Bauer. ChainGuard: Controller-independent Verification of Service Function Chaining in Cloud Computing. In Proc. of the Conference on NFV and SDN (NFV-SDN), Nov. 2017.

[56] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, N. Toumi. Virtual Security as a Service for 5G Verticals. In Proc. of IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2018.

[57] G. Blanc, N. Kheir, D. Ayed, V. Lefebvre, E. Montes de Oca, P. Bisson. Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service. In Proc. of the 13th International Conference on Availability, Reliability and Security (ARES 2018), Article No. 47, Aug. 2018.

[58] X. Xu and L. Hu, "A Software Defined Security Scheme Based on SDN Environment," 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, 2017, pp. 504-512.doi: 10.1109/CyberC.2017.52

[59] S. Farahmandian and D. B. Hoang, "SDS2: A novel software-defined security service for protecting cloud computing infrastructure," 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, 2017, pp. 1-8. doi: 10.1109/NCA.2017.8171388

[60] Wang, S., Wu, J., Yang, W. et al. Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey. Frontiers Inf Technol Electronic Eng 19, 1500–1521 (2018). https://doi.org/10.1631/FITEE.1800575

[61] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,”Future Generation Computer Systems, vol. 78, pp. 680 – 698, Feb. 2018.

[62] N. Mkitalo, A. Ometov, J. Kannisto, S. Andreev, Y. Koucheryavy,and T. Mikkonen, “Safe, secure executions at the network edge: Coordinating cloud, edge, and fog computing,” IEEE Software, vol. 35,no. 1, pp. 30–37, Jan. 2018.

[63] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, “The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, Nov. 2017

[64] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: architecture, applications, and approaches,” Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, Dec. 2013.

[65] Quoc-Viet Pham, Fang Fang, Vu Nguyen Ha, Md. Jalil Piran, Mai Le, Long Bao Le, Won-Joo Hwang, Zhiguo Ding, A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art, arXiv preprint arXiv:1906.08452, 2019.

[66] E. Ahmed and M. H. Rehmani, “Mobile edge computing: Opportunities, solutions, and challenges,” Future Generation Computer Systems, vol. 70, pp. 59 – 63, May 2017.

[67] J. Xu and J. Yao, “Exploiting physical-layer security for multiuser multicarrier computation offloading,” IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 9–12, Feb. 2019.

[68] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of blockchain and cloud of things: Architecture, applications and challenges,” arXiv preprint arXiv:1908.09058, 2019.

[69] A. Abeshu and N. Chilamkurti, “Deep learning: The frontier for distributed attack detection in fog-to-things computing,” IEEE Communications Magazine, vol. 56, no. 2, pp. 169–175, Feb. 2018.

[70] J. Ekberg, K. Kostiainen and N. Asokan, "The Untapped Potential of Trusted Execution Environments on Mobile Devices," in IEEE Security & Privacy, vol. 12, no. 4, pp. 29-37, July-Aug. 2014. doi: 10.1109/MSP.2014.38

[71] Intel® Software Guard Extensions (Intel® SGX), https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

[72] AMD Secure Encrypted Virtualization (SEV), https://developer.amd.com/sev/

[73] F. Schuster, M. Costa, C. Fournet, C. Gkantsidis. VC3: Trustworthy Data Analytics in the Cloud using SGX. In Proc. of the IEEE Symposium on Security and Privacy, pp. 38 – 54, May 2015.

[74] M.-W. Shih, M. Kumar, et al. S-NFV: Securing NFV States by using SGX. SDN-NFVSec'16, March 2016.

[75] N. Paladi, C. Gehrmann. TruSDN: Bootstrapping Trust in Cloud Network Infrastructure. In: Security and Privacy in Communication Networks. SecureComm 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 198. Springer, Cham

[76] P. Jain, S. Desai, et al. OpenSGX: An Open Platform for SGX Research. (NDSS'16), Feb. 2016.

[77] N. Paladi, et al. Safeguarding VNF Credentials with Intel SGX. In Proc. of the SIGCOMM Posters and Demos'17.

[78] IMA project page: https://sourceforge.net/p/linux-ima/wiki/Home/

[79] T. Lazard, J. Gotzfried, et al. TEEshift: Protecting Code Confidentiality by Selectively Shifting Functions into TEEs. In the Proc. of the 3rdWorkshop on System Software for Trusted Execution (SysTEX'18), pp. 14 – 19, Oct. 2018.

[80] ETSI GS ZSM 002. Zero-touch Network & Service Management; Reference Architecture. Aug. 2019.

[81] T. Maksymyuk, J. Gazda, L. Han and M. Jo, "Blockchain-Based Intelligent Network Management for 5G and Beyond," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 36-39.

[82] Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in IFIP International Conference onAutonomous Infrastructure, Management and Security. Springer, Cham,2017, pp. 16–29.

[83] K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet:A Distributed Blockchains-based Secure SDN Architecture for IoT Networks,"IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017.

[84] Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G," in2017 16th International Conference on Optical Communications and Networks (ICOCN). IEEE, 2017, pp. 1–3.

[85] X. Chen, J. Ji, C. Luo, W. Liao and P. Li, "When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 1178-1187.

[86] Xu, Chenhan & Wang, Kun & Guo, Mingyi. (2018). Intelligent Resource Management in Blockchain-Based Cloud Datacenters. IEEE Cloud Computing. 4. 50-59. 10.1109/MCC.2018.1081060.

[87] E. F. Jesus, V. R. L. Chicarino, Célio V. N. de Albuquerque, and A. A. de A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," Security and Communication Networks vol 2018, Article ID 9675050.

[88] NIST, NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View, March 2011. https://csrc.nist.gov/publications/detail/sp/800-39/final

[89] Güneş, Taha D., Tran-Thanh, Long and Norman, Timothy J. (2018) Strategic attacks on trust models via bandit optimization. CEUR Workshop Proceedings, 2154, 87-95.

[90] Dongxia Wang, Tim Muller, Yang Liu, Jie Zhang, "Towards Robust and Effective Trust Management for Security: A Survey", Trust Security and Privacy in Computing and Communications (TrustCom) 2014 IEEE 13th International Conference on, pp. 511-518, 2014.

[91] Communication Papers of the 2017 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 13, pages 127–130 (2017)

[92] Fan, X., Liu, L., Zhang, R., et al., Decentralized Trust Management: Risk Analysis and Trust Aggregation, arXiv e-prints, arXiv:1909.11355

[93] Ben Ghorbel-Talbi M., Cuppens F., Cuppens-Boulahia N., Le Métayer D., Piolle G. (2011) Delegation of Obligations and Responsibility. In: Camenisch J., Fischer-Hübner S., Murayama Y., Portmann A., Rieder C. (eds) Future Challenges in Security and Privacy for Academia and Industry. SEC 2011. IFIP Advances in Information and Communication Technology, vol 354. Springer, Berlin, Heidelberg

[94] C. Fernandez-Gago, V. Tountopoulos, S. Fischer-Hübner, R. Alnemr, D. Nuñez, J. Angulo, T. Pulls, T. Koulouris. Tools for Cloud Accountability: A4Cloud Tutorial. Privacy and Identity Management for the Future Internet in the Age of Globalisation. Privacy and Identity 2014. IFIP Advances in Information and Communication Technology, vol. 457, 2015. Springer

[95] C. Pappas, R. Reischuk, A. Perrig. Forwarding Accountability: A Challenging Necessity of the Future Data Plane. International Workshop on Open Problems in Network Security (iNetSec), Oct 2015, Zurich, Switzerland. Lecture Notes in Computer Science, LNCS-9591, pp.3-10, 2016, Open Problems in Network Security.

[96] S. Pearson. Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. In Steghöfer JP., Esfandiari B. (eds) Trust Management XI. IFIPTM 2017. IFIP Advances in Information and Communication Technology, vol. 505, 2017. Springer, Cham

[97] W. Benghabrit, H. Grall, J.-C. Royer, M. Sellami, K. Bernsmed, A. S. De Oliveira. Abstract Accountability Language. In Zhou J., Gal-Oz N., Zhang J., Gudes E. (eds) Trust Management VIII. IFIPTM 2014. IFIP Advances in Information and Communication Technology, vol. 430, 2014. Springer, Berlin, Heidelberg

[98] O. Pacheco, F. Santos. Delegation in a Role-based Organization. In Lomuscio A., Nute D. (eds) Deontic Logic in Computer Science. DEON 2004. Lecture Notes in Computer Science, vol. 3065. Springer, Berlin, Heidelberg

[99] Schaad, A., Mo_ett, J.D.: Delegation of obligations. In: Policies for Distributed Systems and Networks. USA (2002)

[100] M. Ben Ghorbel, F. Cuppens, N. Cuppens-Boulahia, D. Le Métayer, G. Piolle. Delegation of Obligations and Responsibility. In: Camenisch J., Fischer-Hübner S., Murayama Y., Portmann A., Rieder C. (eds) Future Challenges in Security and Privacy for Academia and Industry. SEC 2011. IFIP Advances in Information and Communication Technology, vol. 354. Springer, Berlin, Heidelberg.

[101] Abou El Kalam, Y. Deswarte, A. Baïna, M. Kaâniche. PolyOrBAC: A Security Framework for Critical Infrastructures. In International Journal of Critical Infrastructure Protection, Vol. 2, No 4, pp. 154 – 169, Elsevier, 2009.

[102] O. Olaleye, T. Oliveira, A. Darie. Managing Emerging Risks and Liabilities in Data-Enabled Solutions. In the Proc. of IEEE 6th International Congress on Big Data, June 2017.

[103] C.E.A. Karnow. Liability for Distributed Artificial Intelligences. 11 Berkeley Tech. L.J. 147, 1996.

[104] J.K.C. Kingston. Artificial Intelligence and Legal Liability. In: Bramer M., Petridis M. (eds) Research and Development in Intelligent Systems XXXIII. SGAI 2016. Springer, Cham

[105] Brockners et al., IETF draft-ietf-sfc-proof-of-transit-04, https://datatracker.ietf.org/doc/draft-ietf-sfc-proof-of-transit/

[106] Shamir, Adi, "How to share a secret", Communications of the ACM, 22 (11): 612–613, doi:10.1145/359168.359176.

[107] ENISA Threat Landscape Report 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[108] Cisco Networks, 5 key requirements for a secure 5G network, https://www.cisco.com/c/m/en_us/network-intelligence/service-provider/digital-transformation/secure-5g-network.html

[109] GSMA, Mobile Telecommunications Security Threat Landscape, January 2019. https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf

[110] MISP project. https://www.misp-project.org/features.html

[111] L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez. A Self-Adaptive Deep Learning-based System for Anomaly Detection in 5G Networks. IEEE Access, vol. 6, pp. 7700 – 7712, Feb. 2018.

[112] J. Ali-Tolppa, et. al. Self-healing and Resilience in Future 5G Cognitive Autonomous Networks. In Proc. of the 10th ITU Academic Conf., Machine Learning for a 5G Future, pp. 35 – 42, Nov. 2018.

[113] ETSI ENI. https://www.etsi.org/technologies-clusters/technologies/experiential-networked-intelligence

[114] Cho, Jin-Hee, Dilli Prasad Sharma, Hooman Alavizadeh, Seunghyun Yoon, Noam Ben-Asher, Terrence J. Moore, Dong Seong Kim, Hyuk Lim and Frederica F. Nelson. “Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense.” ArXiv abs/1909.08092 (2019).

[115] Jafarian JH, Al-Shaer E, Duan Q, 2012. OpenFlow random host mutation: transparent moving target defense using software defined networking. 1st Workshop on Hot Topics in Software Defined Networks, p.127-132.

[116] Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61(8):081301, https://doi.org/10.1007/s11432-017-9426-4

[117] 5G Americas, “The Evolution of Security in 5G,” July 2019, https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf

[118] Kristian Slavov, Daniel Migault and Makan Pourzandi, Identifying and addressing the vulnerabilities and security issues of SDN, Ericsson technology review, 2015.

[119] Z. Kotulski et al., "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, 2017, pp. 783-792.doi: 10.15439/2017F228

[120] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, Andrew Hines, 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges, Computer Networks, Volume 167, 2020.

[121] Telefonica Research Institute, (https://github.com/nfvlabs/openmano). [Online: accessed 28-February-2019].

[122] JOX, (http://mosaic-5g.io/jox/). [Online: accessed 28-February-2019].

[123] ONF TR-526, Applying SDN Architecture to 5G Slicing (2016).

[124] ONF, Transport API (TAPI) 2.0 Overview Version 0.0 August, 2017, (https: //www.opennetworking.org/wp-content/uploads/2017/08/TAPI-2-WP_DRAFT. pdf). [Online: accessed 28-February-2019].

[125] Muñoz, R., Mayoral, A., Vilalta, R., Casellas, R., Martínez, R., & López, V. (2016, March). The need for a transport API in 5G networks: The control orchestration protocol. In Optical Fiber Communication Conference (pp. Th3K-4). Optical Society of America.

[126] MCKEOWN, Nick, ANDERSON, Tom, BALAKRISHNAN, Hari, et al. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 2008, vol. 38, no 2, p. 69-74.

[127] PAGÉ, Jérémy et DRICOT, Jean-Michel. Software-defined networking for low-latency 5G core network. In: 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, 2016. p. 1-7.

[128] CHAVES, Luciano Jerez, EICHEMBERGER, Vítor Marge, GARCIA, Islene Calciolari, et al. Integrating OpenFlow to LTE: Some issues toward software-defined mobile networks. In : 2015 7th International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2015. p. 1-5.

[129] ENNS, Rob, BJORKLUND, Martin, SCHOENWAELDER, Juergen, et al. Network configuration protocol (NETCONF). 2011.

[130] ANDRUS, B., AUTENRIETH, A., PACHNICKE, S., et al. Performance evaluation of NETCONF-based low latency cross-connect for 5G C-RAN architectures. In : 2018 20th International Conference on Transparent Optical Networks (ICTON). IEEE, 2018. p. 1-5.

[131] FOUKAS, Xenofon, NIKAEIN, Navid, KASSEM, Mohamed M., et al. FlexRAN: A flexible and programmable platform for software-defined radio access networks. In : Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies. 2016. p. 427-441

[132] ETSI NFV Security group report: https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/003/01.02.01_60/gr_nfv-sec003v010201p.pdf

[133] M. Sabt, M.Achemlal, “Trusted Execution Environment: What It is, What It is Not “, 14th IEEE International Conference on Trust, Security and Privacy In Computing Communications, Aug 2015, Helsinki, Finland.

[134] J. Ames, Stanley R., M. Gasser, and R. R. Schell, “Security kernel design and implementation: an introduction,” Computer, vol. 16, no. 7, pp. 14–22, Jul. 1983.

[135] U.S. government protection profile for separation kernels in environments requiring high robustness,” National Security Agency, Tech. Rep., Jun. 2007, version 1.03. [Online]. Available: https://www.niap-ccevs.org/ pp/pp skpp hr v1.03.pdf

[136] Wikipedia, SECCOMP definition page at https://en.wikipedia.org/wiki/Seccomp

[137] Wikipedia, SELINUX definition page at https://en.wikipedia.org/wiki/Security-Enhanced_Linux

[138] Ubuntu, Apparmor user’s guide at https://doc.ubuntu-fr.org/apparmor

[139] Wikipedia definition of a TPM, page available at https://en.wikipedia.org/wiki/Trusted_Platform_Module

[140] S. Ravidas, S. Lal, I. Oliver and L. Hippelainen, "Incorporating trust in NFV: Addressing the challenges," 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, 2017, pp. 87-91. doi: 10.1109/ICIN.2017.7899394

[141] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/018/01.01.01_60/gr_NFV-SEC018v010101p.pdf

[142] R. Sailer, X. Zhang, T. Jaeger, L. van Doorn, Design and implementation of a tcg-based integrity measurement architecture, in: Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, SSYM’04, USENIX Association, Berkeley, CA, USA, 2004, pp. 16–16. URL http://dl.acm.org/citation.cfm?id=1251375.1251391

[143] De Benedictis, M., & Lioy, A. (2019). Integrity verification of Docker containers for a lightweight cloud environment. Future Generation Computer Systems, 97, 236-246.

[144] TPM Library Specification 2.0. Trusted Computing Group. October 1, 2014. Retrieved April 21, 2018. https://trustedcomputinggroup.org/resource/tpm-library-specification/

[145] T. Garfinkel, B. Pfaff. “Terra: A Virtual Machine-Based Platform for Trusted Computing”, Stanford University, 2003

[146] GlobalPlatform, “TEE system architecture,” 2011. [Online]. Available at http://www.globalplatform.org/specificationsdevice.asp

[147] A. Vasudevan, J. M. McCune, and J. Newsome, Trustworthy execution on mobile devices. Springer Publishing Company, Incorporated, 2013.

[148] V. Lefebvre, T.Mueller, “Universal Trusted Execution Environments for Securing SDN/NFV Operations”, ARES conference, August 2018.

[149] Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang, A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, Expert Systems with Applications, Volume 37, Issue 9, 2010, Pages 6225-6232,

[150] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & Security, Volume 28, Issues 1–2, 2009, Pages 18-28,

[151] J. Li, Z. Zhao and R. Li, "Machine learning-based IDS for software-defined 5G network," in IET Networks, vol. 7, no. 2, pp. 53-60, 3 2018.doi: 10.1049/iet-net.2017.0212

[152] Othman, S.M., Ba-Alwi, F.M., Alsohybe, N.T. et al. Intrusion detection model using machine learning algorithm on Big Data environment. J Big Data 5, 34 (2018). https://doi.org/10.1186/s40537-018-0145-4

[153] Kumar, G., Thakur, K. & Ayyagari, M.R. MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review. J Supercomput (2020).

[154] Muhammad Ahsan, Muhammad Mashuri, Muhammad Hisyam Lee, Heri Kuswanto, Dedy Dwi Prastyo, Robust adaptive multivariate Hotelling's T2 control chart based on kernel density estimation for intrusion detection system, Expert Systems with Applications, Volume 145, 2020.

[155] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei V. Gurtov, Mika Ylianttila: Security for 5G and Beyond. IEEE Communications Surveys and Tutorials 21(4): 3682-3722 (2019)

[156] Jiaqi Li, Zhifeng Zhao, Rongpeng Li: A Machine Learning Based Intrusion Detection System for Software Defined 5G Network. CoRR abs/1708.04571 (2017)

[157] Merima Kulin, Tarik Kazaz, Ingrid Moerman, Eli De Poorter: A survey on Machine Learning-based Performance Improvement of Wireless Networks: PHY, MAC and Network layer. CoRR abs/2001.04561 (2020)

[158] R. V. Kulkarni, G. K. Venayagamoorthy, Neural network based secure media access control protocol for wireless sensor networks, in: Neural Networks, 2009. IJCNN 2009. International Joint Conference on, IEEE, 2009, pp. 1680–1687.

[159] H. H. Bosman, G. Iacca, A. Tejada, H. J.W¨ortche, A. Liotta, Ensembles of incremental learners to detect anomalies in ad hoc sensor networks, Ad Hoc Networks 35 (2015) 14–36.

[160] Sreeraj Rajendran, Wannes Meert, Vincent Lenders, Sofie Pollin: Unsupervised Wireless Spectrum Anomaly Detection With Interpretable Features. IEEE Trans. Cogn. Comm. & Networking 5(3): 637-647 (2019).

[161] Lorenzo Fernández Maimó, Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez: Dynamic management of a deep learning-based anomaly detection system for 5G networks. J. Ambient Intell. Humaniz. Comput. 10(8): 3083-3097 (2019)

[162] Qi Liao, Slawomir Stanczak: Network State Awareness and Proactive Anomaly Detection in Self-Organizing Networks. GLOBECOM Workshops 2015: 1-6

[163] J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, “Adaptive artificial immune networks for mitigating DoS flooding attacks,” Swarm Evol. Comput., vol. 38, pp. 94–108, Feb. 2018.

[164] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, “A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks,” IEEE Access, vol. 6, pp. 7700–7712, 2018.

[165] N. Pandeeswari and G. Kumar, “Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN,” Mob. Networks Appl., vol. 21, no. 3, pp. 494–505, Jun. 2016.

[166] T. Ding, A. AlEroud, and G. Karabatis, “Multi-granular aggregation of network flows for security analysis,” in 2015 IEEE International Conference on Intelligence and Security Informatics (ISI), 2015, pp. 173–175.

[167] Z. Fan and R. Liu, “Investigation of machine learning based network traffic classification,” in 2017 International Symposium on Wireless Communication Systems (ISWCS), 2017, pp. 1–6.

[168] Farah, Nutan and Avishek, Md. and Muhammad: ’Application of Machine Learning Approaches in Intrusion Detection System: A Survey’, International Journal of Advanced Research in Artificial Intelligence, 2015, 4

[169] Tjhai, Gina C. and Furnell, Steven M. and Papadaki: ‘A preliminary two-stage alarm correlation and filtering system using SOM neural network and K -means algorithm’, Computers and Security, 2010, 29, pp. 712–723

[170] Louvieris, Panos and Clewley, Natalie and Liu: ‘Effects-based feature identification for network intrusion detection’, Neurocomputing, 2013, 121, pp. 265–273

[171] Muniyandi, Amuthan Prabakar and Rajeswari, R. and Rajaram: ‘Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm’, Procedia Engineering, 2012, 30, pp. 174–182

[172] Sheikhan, Mansour and Jadidi, Zahra and Farrokhi: ‘Intrusion detection using reduced-size RNN based on feature grouping’, Neural Computing and Applications, 2012, 21, pp. 1185–1190

[173] Kim, Jihyun and Kim, Jaehyun and Thu: ‘Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection’, International Conference on Platform Technology and Service, 2016, pp. 1–5

[174] Zhang, Jiong and Zulkernine, Mohammad and Haque: ‘Random-Forests-Based Network Intrusion Detection Systems’, IEEE Transactions on Systems Man and Cybernetics Part C Applications and Reviews, 2008, 38, pp. 649–659

[175] Michael Geller and Pramod Nair. 5G Security Innovation with Cisco. Cisco Whitepaper. Online: https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf

[176] Pan Wang, Feng Ye, Xuejiao Chen, Yi Qian: Datanet: Deep Learning Based Encrypted Network Traffic Classification in SDN Home Gateway. IEEE Access 6: 55380-55391 (2018)

[177] Auwal Sani Iliyasu, Huifang Deng: Semi-Supervised Encrypted Traffic Classification With Deep Convolutional Generative Adversarial Networks. IEEE Access 8: 118-126 (2020)

[178] Tangda Yu, Futai Zou, Linsen Li, Ping Yi: An Encrypted Malicious Traffic Detection System Based on Neural Network. CyberC 2019: 62-70

[179] Paul Prasse, Lukás Machlica, Tomás Pevný, Jirí Havelka, Tobias Scheffer: Malware Detection by Analysing Encrypted Network Traffic with Neural Networks. ECML/PKDD (2) 2017: 73-88

[180] Yi Zeng, Huaxi Gu, Wenting Wei, Yantao Guo: Deep-Full-Range: A Deep Learning Based

Network Encrypted Traffic Classification and Intrusion Detection Framework. IEEE Access 7: 45182-45190 (2019)

[181] Ross, V. Pillitteri, G. Guissanie, R. Wagner, R. Graubart, and D. Bodeau, "Protecting controlled unclassified information in non-federal systems and organizations; enhanced security requirements for critical programs and high value assets" NIST 800-171B, June 2019.

[182] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J.Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," CoRR, vol.abs/1909.08092, 2019.

[183] M. Albanese, S. Jajodia, and S. Venkatesan, "Defending from stealthy botnets using moving target defenses," IEEE Security & Privacy, vol. 16, no. 1, pp. 92 – 97, January/February 2018.

[184] Hamza Attak, Marc Combalia, Georgios Gardikis, Bernat Gastón, Ludovic Jacquin, Dimitris Katsianis, Antonis Litke, Nikolaos Papadakis, Dimitris Papadopoulos, Antonio Pastor, Marc Roig, Olga Segou, Application of distributed computing and machine learning technologies to cybersecurity, Computer & Electronics Security Applications Rendez-vous (C&ESAR), Rennes (France), 19-21 November 2018 (https://torsec.github.io/shield-h2020/documents/scientific-papers/CESAR2018_paper.pdf)

[185] Pastor, Antonio, et al. "The Mouseworld, a security traffic analysis lab based on NFV/SDN." Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018.

[186] 5G PPP SN Working Group, "Vision on Software Networks and 5G," 2017.

[187] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, and P. Castoldi, "P4 Edge Node Enabling Stateful Traffic Engineering And Cyber Security," J. Opt. Commun. Netw., vol. 11, no. 1, pp. A84–A95, 2019.

[188] 5G PPP Security Work Group, "5G PPP Phase 1 Security Landscape," 2017.

[189] Daniel Fraunholz, Simon Duque Antón, Christoph Lipps, Daniel Reti, Daniel Krohmer, Frederic Pohl, Matthias Tammen, Hans Dieter Schotten: Demystifying Deception Technology: A Survey. CoRR abs/1804.06196 (2018)

[190] Samuel Oswald Hunter, Barry Irwin, Etienne Stalmans: Real-time distributed malicious traffic monitoring for honeypots and network telescopes. ISSA 2013: 1-9

[191] Eric Nunes, Ahmad Diab, Andrew T. Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, Paulo Shakarian: Darknet and deepnet mining for proactive cybersecurity threat intelligence. ISI 2016: 7-12

[192] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, Ali E. Abdallah: Cyber threat intelligence sharing: Survey and research directions. Comput. Secur. 87 (2019)

[193] Marcello Cinque, Domenico Cotroneo, Antonio Pecchia: Challenges and Directions in Security Information and Event Management (SIEM). ISSRE Workshops 2018: 95-99

[194] E. Kapassa, M. Touloupou, D. Kyriazis, "SLAs in 5G: A Complete Framework Facilitating VNF- and NS- Tailored SLAs Management", 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops (AINA), Krakow, Poland, 2018.

[195] Solé, Marc, Victor Muntés-Mulero, Annie Ibrahim Rana and Giovani Estrada. "Survey on Models and Techniques for Root-Cause Analysis." ArXiv abs/1701.08546 (2017).

[196] Kavulya S.P., Joshi K., Giandomenico F.D., Narasimhan P. (2012) Failure Diagnosis of Complex Systems. In: Wolter K., Avritzer A., Vieira M., van Moorsel A. (eds) Resilience Assessment and Evaluation of Computing Systems. Springer, Berlin, Heidelberg

[197] Chickering D.M. (1996) Learning Bayesian Networks is NP-Complete. In: Fisher D., Lenz HJ. (eds) Learning from Data. Lecture Notes in Statistics, vol 112. Springer, New York, NY

[198] Harrison Mfula, Jukka K. Nurminen: Adaptive Root Cause Analysis for Self-Healing in 5G Networks. HPCS 2017: 136-143

[199] Péter Szilágyi, Szabolcs Nováczki: An Automatic Detection and Diagnosis Framework for Mobile Communication Systems. IEEE Trans. Network and Service Management 9(2): 184-197 (2012)

[200] Ana Gómez-Andrades, Pablo Muñoz Luengo, Inmaculada Serrano, Raquel Barco: Automatic Root Cause Analysis for LTE Networks Based on Unsupervised Techniques. IEEE Trans. Vehicular Technology 65(4): 2369-2386 (2016)

[201] Pablo Muñoz Luengo, Isabel de la Bandera, Emil J. Khatib, Ana Gómez-Andrades, Inmaculada Serrano, Raquel Barco: Root Cause Analysis Based on Temporal Analysis of Metrics Toward Self-Organizing 5G Networks. IEEE Trans. Vehicular Technology 66(3): 2811-2824 (2017)

[202] ETSI NFV Group Specification Draft: "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework", Sept. 2015.

[203] J. Sanchez, I. Grida Ben Yahia, N. Crespi, "Self-Modeling Based Diagnosis of Software-Defined Networks," Workshop MISSION 2015 at 1st IEEE Conference on Network Softwarization, London, 13-17 April 2015.

[204] M. Steinder and A. S. Sethi. "End-to-end Service Failure Diagnosis Using Belief Networks". In Network Operations and Management Symposium, NOMS 2002, pages 375-390, 2002

[205] L. Bennacer, L. Ciavaglia, et.al., "Optimization of fault diagnosis based on the combination of Bayesian Networks and Case-Based Reasoning," in NOMS, 2012 IEEE , vol., no., pp.619,622, 16-20 April 2012.

[206] P. Bahl, R. Chandra, et. al., "Towards highly reliable enterprise networking services via inference of multi-level dependencies," in SIGCOMM, 2007.

[207] C. Hounkonnou, "Active Self-Diagnosis in Telecommunication Networks". PhD thesis. UniversitѴ© de Rennes 1. July 2013.

[208] D. Kreutz, F.M.V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE , vol.103, no.1, pp.14,76, Jan. 2015.

[209] P. Fonseca, R. Bennesby, E. Mota and A. Passito, "A replication component for resilient OpenFlow-based networking," Network Operations and Management Symposium (NOMS), 2012 IEEE, vol., no., pp.933,939, 16-20 April 2012

[210] M. Canini, D. Venzano, et. al., "A NICE way to test OpenFlow applications," in Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 10-10.

[211] N. Handigol, B. Heller, V. Jeyakumar, D. Mazieres, and N. McKeown,"Where is the debugger for my software-defined network?" in Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ser. HotSDN '12. New York, NY, USA: ACM, 2012, pp. 55-60.

[212] A. Wundsam, D. Levin, S. Seetharaman, and A. Feldmann, "OFRewind: Enabling Record and Replay Troubleshooting for Networks," in Proc. 2011 USENIX Conference on USENIX Annual Technical Conference, ser. USENIXATC'11. USENIX Association, 2011, pp. 29-29.

[213] N. Handigol, B. Heller, V. Jeyakumar, D. Mazieres, and N. McKeown,"I know what your packet did last hop: Using packet histories to troubleshoot networks," in 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14). Seattle, WA: USENIX Association, Apr. 2014, pp. 71-85.

[214] R.C. Turchetti, E. P. Duarte, "Implementation of Failure Detector Based on Network Function Virtualization," in Dependable Systems and Networks Workshops (DSN-W), 2015 IEEE International Conference on, vol., no., pp.19-25, 22-25 June 2015.

[215] G. Georghe; T. Avanesov, M.-R. Palattella, T. Engel, Popoviciu, C., "SDN-RADAR: Network troubleshooting combining user experience and SDN capabilities," in Network Softwarization (NetSoft), 2015 1st IEEE Conference on, vol., no., pp.1-5, 13-17 April 2015.

[216] R. Mijumbi, et.al., "Network Function Virtualization: State-of-the-art and Research Challenges," in Communications Surveys & Tutorials, IEEE, vol.PP, no.99, pp.1-1.

[217] R.P. Esteves, L.Z. Granville, R. Boutaba, "On the management of virtual networks," in Communications Magazine, IEEE, vol.51, no.7, pp.80,88, July 2013.

[218] N.M.M.K. Chowdhury, R. Boutaba, "Network virtualization: state of the art and research challenges," in Communications Magazine, IEEE, vol.47, no.7, pp.20-26, July 2009.

[219] S. Kandula, R. Mahajan, et. al, "Detailed diagnosis in enterprise networks," in SIGCOMM, 2010.

[220] ETSI NFV Group Specification: "Network Functions Virtualisation (NFV); Management And Orchestration", Dec. 2014

[221] Topology-Aware Self-Diagnosis framework, presented in Orange Labs Research exhibition 2015, Paris, France. Video available at: https://www.youtube.com/watch?v=xNudu48quRM

[222] M. Scholler et. al., "Resilient deployment of virtual network functions," in UltraModern Telecommunications and Control Systems and Workshops (ICUMT), 2013 5th International Congress on, vol., no., pp.208-214, 10-13 Sept. 2013

[223] M. Miyazawa et.al., "vNMF: Distributed fault detection using clustering approach for network function virtualization," in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, vol., no., pp.640-645, 11-15 May 2015

[224] A survey on emerging SDN and NFV Security Mechanisms for IoT Systems, IEEE Communications Surveys & Tutoriels, 2019.

[225] IETF RFC 8520, MUD Profiles, 2019

[226] Steven Noel, Lingyu Wang, Anoop Singhal, and Sushil Jajodia, “Measuring security risk of networks using attack graphs”. IJNGC, 1(1), 2010.

[227] Steven J. Templeton and Karl Levitt “A requires/provides model for computer attacks”. Proceedings of the 2000 workshop on New security paradigms, NSPW’00, New York, NY, USA, 2000. ACM.

[228] Steven Noel, Sushil Jajodia, Brian O’Berry, and Michael Jacobs. “Efficient minimum-cost network hardening via exploit dependency graphs”. Proceedings of the 19th Annual Computer Security Applications Conference, ACSAC’03, Washington, DC, USA, 2003. IEEE Computer Society.

[229] Kheir, N.; Debar, H.; Cuppens-Boulahia, N.; Cuppens, F.; Viinikka, J., "Cost Evaluation for Intrusion Response Using Dependency Graphs," Network and Service Security, 2009. N2S '09. International Conference on, vol., no., pp.1,6, 24-26 June 2009

[230] Kheir, N., Mahjoub, A. R., Naghmouchi, M. Y., Perrot, N., Wary, J. P: Assessing the risk of complex ICT systems. Annals of Telecommunications, 1-15 (2017)

[231] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and X. Sean Wang. 2011. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats (1st ed.). Springer (2011).

[232] Fabio Martinelli, Oleksii Osliak, Andrea Saracino: Towards General Scheme for Data Sharing Agreements Empowering Privacy-Preserving Data Analysis of Structured CTI. CyberICPS/SECPRE@ESORICS 2018: 192-212

[233] SGX: Intel developer guide at https://software.intel.com/en-us/documentation/sgx-developer-guide

[234] SMESEV: AMD developer guide at https://developer.amd.com/sev/

[235] SEV-SGX S.Mofrad, F.Zhang. “Comparison Study of Intel SGX and AMD Memory Encryption Technology”, published at HASP ’18, June 2, 2018, Los Angeles, CA, USA

[236] ASYLO: Intel SGX hardware release enclave at https://asylo.dev/docs/guides/sgx_release_enclaves.html

[237] OPENENCLAVE developer sdk available at https://openenclave.io/sdk/

[238] S.Shinde, D.Le.Tien, “PANOPLY: Low-TCB Linux Applications with SGX Enclaves », published at NDSS ’17, 26 February - 1 March 2017, San Diego, CA, USA

[239] C.Priebe, D.Muthukumaran, « SGX-LKL: Securing the Host OS Interface for Trusted Execution », submitted in August 2019 on arXiv.org

[240] S. Arnautov, B.Trach, “SCONE: Secure Linux Containers with Intel SGX”, November 2016, Savannah, USA

[241] ARM TRUSTZONE developer kit available at https://developer.arm.com/ip-products/security-ip/trustzone

[242] MULTIZONE: HEX-Five Security website available at https://github.com/hex-five/multizone-secure-iot-stack

[243] ENISA, Threat Landscape for 5G Networks, November 21, 2019, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[244] ETSI GS ZSM 001, “Zero-touch Network and Service Management (ZSM); Requirements based on Documented Scenarios,” Oct. 2019

[245] ETSI GS ZSM 004, “Zero-touch Network and Service Management (ZSM); Landscape,” March 2020.

[246] Yu, F. Richard. "vDLT: A service-oriented blockchain system with virtualization and decoupled management/control and execution." arXiv preprint arXiv:1809.00290 (2018).

[247] Kotulski, Zbigniew, et al. "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges." 2017 Federated conference on computer science and information systems (FedCSIS). IEEE, 2017.

[248] Schneider P, Mannweiler C, Kerboeuf S. Providing strong 5G mobile network slice isolation for highly sensitive third-party services. In2018 IEEE Wireless Communications and Networking Conference (WCNC) 2018 Apr 15 (pp. 1-6). IEEE.

[249] Sattar D, Matrawy A. Optimal slice allocation in 5G core networks. IEEE Networking Letters. 2019 Mar 29;1(2):48-51.

[250] Sattar D, Matrawy A. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices. In2019 IEEE Conference on Communications and Network Security (CNS) 2019 Jun 10 (pp. 82-90). IEEE.

[251] NFV, Network Functions Virtualisation. "ETSI GS NFV-SEC 001 V1. 1.1 (2014-10)." (2014).

[252] Mishra, Preeti, et al. "Intrusion detection techniques in cloud environment: A survey." Journal of Network and Computer Applications 77 (2017): 18-47.

[253] Barrett, Matthew P. Framework for improving critical infrastructure cybersecurity version 1.1. No. NIST Cybersecurity Framework. 2018.

[254] 5GENESIS 5G Security Framework (Release A), Deliverable 3.13, https://5genesis.eu/wp-content/uploads/2019/10/5GENESIS_D3.13_v1.0.pdf

[255] APEX Policy Engine, https://ericsson.github.io/apex-docs/index.html

[256] 5GENESIS Monitoring and Analytics (Release A), Deliverable D3.5, https://5genesis.eu/wp-content/uploads/2019/10/5GENESIS_D3.5_v1.0.pdf

[257] Molander, Julia A. "The Y2K Act." Kan. JL & Pub. Pol'y 9 (1999): 570.

Appendix A. ENISA Threat Landscape Terminology

The complete virtualisation of the Core network is a significant innovation in architecture of 5G. The 'softwarisation' of network functions is going to enable simpler portability and improved flexibility of networking systems and services (Control-User Plain Separation, CUPS). The Software Defined Network (SDN) brings simplified management together with innovation through abstraction. (NFV) provides the enabling technology for placing various network functions in different network components. The placement is made based on performance needs/requirements and eliminates the need for function-specific or service-specific hardware. SDN and NFV are complementing each other since they improve the network elasticity, simplify network control and management, break the barrier of vendor-specific or proprietary solutions. As a result, they are considered as highly important for future networks. These novel network technologies and concepts that rely on softwarisation and virtualisation of network functions will introduce new and complex threats.

Assets

An asset is anything that has value to an individual or organisation and requires protection. Due to its value, a digital asset becomes a target for threat agents. Threat agents are human or software agents, which may wish to abuse, compromise and/or damage assets. Threat agents may perform attacks, which create threats that pose risks to assets.

Assets relationship to the 5G architecture

Slicing: This asset group represents all 5G functions that are responsible for the creation and management of slicing. Slices are independent virtualised logical networks that carry out the network communication between the user equipment and 5G services. These slices form the end-to-end network communication links that are virtually multiplexed and mapped to resources of the virtualised physical network platform. While 4G allowed for APN (Access Point Name), in 5G, slicing is taking place initially on a static base and later a dynamic basis. Slicing is considered as one of the main advantages of 5G networks for enabling low network latency.

Management and orchestration (MANO): This asset group stands for the entire set of assets related to management and orchestration. MANO is the most critical part of the 5G infrastructure as it is responsible for managing the entire set of network functions, their virtualisation and entire software life cycle related hereto. The main parts of MANO are the Network Function Virtualisation (NFV) orchestrator, the Virtual Network Function (VNF) manager, and the virtualised infrastructure manager. Given its important role, MANO is vulnerable to numerous attacks with a potentially major impact on the entire managed 5G infrastructure.

Radio Access Network (RAN): This asset group represents the logical components making up the functions of the Radio Access Network (RAN hardware is not part of this asset group). It includes mainly distribution unit and control unit of radio access.

Network Functions Virtualisation (NFV): This asset group contains all network functions that are virtualised to depart from proprietary dedicated hardware. NFV is a 5G specific architecture that virtualises classes of network node functions and physical network functions (PNF) into blocks that take over the entire connectivity actions necessary for communication services. This asset group also includes all security functions, that is, functions that cope with all the required authentication, monitoring and subscription actions. Security functions are considered particularly sensitive, as they use key material to perform operations. As such, they will be exposed to attacks aiming at breaching this information and compromise the entire security part of the 5G network.

Software Defined Networks (SDN): This group contains the assets related to the SDN network controller, virtual network switches, data plane, application plane and control plane.

Data network: This asset group represents the connectivity to external data, content, services and other resources available outside the 5G network. The data network is also used to interconnect different 5G networks, operators and providers.

Lawful Interception (LI): Lawful Interception assets are concerned with the 5G functions implementing all provisions for performing lawful surveillance, providing legally sanctioned access to 5G private communications of all kinds. Though not analysed much further in this document, these functions deserve special attention as they do provide any information processed in 5G networks. Therefore, LI (related functions and data) is a target for manipulations and other malicious actions (e.g. unlawful surveillance, weaponization of interception, manipulation of information, etc.).

Virtualisation: The role of virtualisation functions in 5G is crucial. With this asset group, we summarise assets that are related to virtual machine technologies and the hypervisor. Due to the massive virtualisation in 5G, these two components are decisive for the functionality of the entire network. Given the trend of using common open-source software for these two components, new vulnerabilities, when exploited, will multiply attack impact in the underlying technology platform. It is expected that hypervisors will be subject to attacks. With the ability to access and manage computer memory, attackers may access cryptographic material in case of operations performed in this memory (i.e. absence of dedicated crypto hardware).

Cloud: Cloud technology will be extensively used within the 5G architecture, either through the provisioning of SaaS or IaaS. In the asset diagram, this group contains the logical cloud services. The hardware part, related to cloud, is covered in the physical infrastructure asset group. Cloud will be used as a platform by tenants to control storage and processing resources. Existing threats targeting cloud, when materialized, may unveil multiple confidential information, while, at the same time affect the availability of the entire 5G infrastructure.

Multi-access Edge Computing (MEC): This group consists of assets related to the decentralisation of cloud functions (storage of data and computing) located closer to the user or edge device.

Threat Agents (Threat Actors): According to ELT14 a threat agent is "*someone or something with decent capabilities, a clear intention to manifest a threat and a record of past activities in this regard*". The nature of 5G networks will attract the attention of existing and new threat agent groups with a large variety of motives. However, with the implementation of 5G, the attackers' profile is expected to shift to take advantage 5G's novel capabilities. Some examples are:

- The vulnerabilities of interconnected systems will expand the attack surface, and exposure of critical assets;
- Novel tools and methods for vulnerability exploitation will be developed;
- The interconnection of verticals will surface new targets for threat agents;
- Existing groups of threat agents will collaborate to exploit and target critical assets.

Threat agents can be categorised as follows:

Cyber-criminals: Given the vast presence of this threat agent group in cyber-space and the advanced capabilities that they continue evolving, it is likely that this threat agent group will keep its presence in 5G mobile networks. Given the statistics of activities of this threat agent group, it looks like their attacks that target multiple industries and governments, may be channelled to the emerging 5G mobile Networks. Even though, these attacks do not represent a significant monetizing vector, such attacks (or preparations hereto), will be part of their activities. The anticipated number of vulnerabilities, the complexity and low level of maturity of the 5G network are indicative for this shift. Legitimate access of cyber-criminals to the 5G network may exacerbate the threats posed by this group.

Insiders: Insiders are assumed to be a vital threat agent group in the 5G landscape mainly because these are MNOs employees, which were constant proximity with the core of the technology representing a vast number of individuals. Other reasons substantiate the importance of this group are the complexity of the network and several stakeholders engaged in its use and operation. While the skill issue and increased complexity will surge the amount of unintentional damages significantly, dishonest insiders and third-party employees may misuse their access to vital network function and cause high impact/large scale availability issues in the network itself. Such incidents may have

cascaded impact on interconnected industries/verticals. Given the fact that disgruntled/dissatisfied insiders are a primary target for high capability agents, they might be recruited to abuse their insider knowledge, e.g. through monetary rewards. Finally, given the current race for 5G patents/IPS matters, it is expected that this threat agent group will have an additional motive to increase their activities.

Nation States: This threat agent group is important due both to its ability to compromise future 5G Network and its potential motivation to do so. It is indisputable that vendors of 5G components – just like any other technology vendor– are in a better position to cause devastating attacks to the operation of self-developed components, especially when governments influence them. Given the importance of 5G to the sovereignty of nation-states, they will most probably be a target of state-sponsored attacks. Despite the numerous activities to setup vendor requirements, such as understanding the misuse vectors of various components and designing the corresponding security controls, it will not prevent a nation state from attacking another's country 5G Network. According to recent statistics, attacks motivated by espionage represent a significant number in the 2019 threat landscape.

Cyber warriors: Cyberwar, according to incident statistics, is the third most frequent motive and a trend that will inevitably keep up in the 5G ecosystem. The 5G infrastructure will be one of the most vital components to protect in the technology landscape. This is mainly due to the need to maintain dominance, independence and sovereignty of a country, especially the ones in which a vicinity between vendors and governments is being maintained (e.g. US, Europe, China). Moreover, there is evidence, that the military sector will be interested in using 5G, just as many security-related verticals (e.g. critical infrastructures). Such development will increase the protection requirements and the attractiveness of 5G as a target of cyberwar. Cyber warriors will maintain their presence in the cyberthreat landscape with a focus on 5G in both roles of defender and offender, depending on global geopolitical developments.

Hacktivists: Though this threat agent group has a presence in the cyberthreat landscape (fourth position by means of number of incidents), it is not clear how it is going to be engaged in 5G malicious activities. While it is most probable to see this group engaging in regional campaigns, it cannot be excluded that it could achieve high impact activities in national and even global 5G infrastructures. Just as the efficiency of attacks of all other threat agent groups, this will depend heavily on: a) the maturity of 5G rollouts for cybersecurity protection measures, b) the number of vulnerabilities of 5G components, c) the availability of 5G exploits/malicious tools and modus operandi and d) the skill set available to master 5G infrastructure complexity at the side of 5G stakeholders. Just as other threat agent groups, hacktivist will be able to gain legitimate access to 5G network, hence attacking from inside the network.

Corporations: Although this threat agent group has not enjoyed special attention in recent ENISA Threat Landscape, it is believed that its role will increase in future editions of the report. The main reason lays in the intention to increase competitiveness and becoming part of the 5G ecosystem. On the other hand, corporations will be interested in tracking the development of patents and IPRs that are related to 5G infrastructure: given the emergence of 5G technology, this area is going to attract the attention of this threat agent group mainly. Other reasons for increased engagement are to trace the involvement of competitors to 5G procurements, understand business opportunities related to 5G and strengthen their role in the market. Due to the overarching nature of 5G, corporations from several sectors/verticals will be potentially attracted by 5G developments, increasing thus the number of entries into this threat agent group.

Cyber-terrorists: There are multiple references to alleged interest from this threat group to produce harm to 5G infrastructures. The main concern about future actions from this group is the concentration of ‘values’ that will take place as a result of a 5G deployment. 5G is going to (inter-) connect vast amounts of services that are vital to the society, governments and business and this will thus attract the attention of cyber-terrorist groups. Through the integration of multiple verticals, 5G will provide a single attack surface that once targeted, may result in damages in the physical space

(e.g. hybrid threats). Although incident statistics do not provide evidence for significant activity of cyber-terrorists in the cyber-space, 5G stakeholders will need to take the protection of this infrastructure very seriously to avoid high impact events that would cause severe harm to society. This effort requires multifaceted/multilevel protection controls involving coordinated activities of numerous stakeholders at a scale that had never existed before 5G. This is a challenge that can be mastered, only if there is a concerted effort to protect 5G infrastructure and its importance goes beyond the threats posed by a single threat agent group.

Script kiddies: The emerging technology landscape has many components that are in the control of individual users. Examples are IoT devices, mobile phones, cloud and storage spaces, social media platforms, etc. These components are the perfect playground for technology-interested young individuals that have low motivation/low capabilities but are equipped with malicious tools. In the past, we have seen high impact attacks (e.g. DDoS) spreading from home devices and gadgets. With the availability of high-speed 5G networks and interconnected devices, activities of this threat agent group may cause significant impact though cascaded events affecting upstream components of 5G operators. Just as all other threat agent groups, script-kiddies may possess legitimate access to the network and be able to use network functions to manage their own devices, increasing thus the potential of misuse.

Appendix B. Survey of existing TEEs

TEE for X-86 platform, SGX, SEV and associated frameworks

When considering the SDN-NFV (and 5G core network and edge computing), Intel SGX [233] and AMD SME-SEV [234] are the two first TEE technology to consider. Both relates to X86 compatible processors where Intel and AMD capture the entirety (at the time of writing) of the cloud blade market.

In its view of comparison of SGX and SEV, The Wayne State University [235] and their presentation at HASP conference, June 2018, reflected the two diverging approaches which rely on two opposing architectural designs. Intel SGX is depicted a means to secure small payload which must be preferably be an extraction of a reduced part of a larger code, whereas SEV is a basic VM encryption with no code extraction-selection to be made. More Intel 's SGX interacts with user code (ring-3) while SEV operates on ring-0.

When SGX imposes code changes (typically to remove all system calls) and a new compilation worked out through Intel's SGX user SDK, SEV is totally transparent to the payload. In fact, it would be difficult to build more diverging techniques as they differ radically, technically and operationally. In all respects (required code changes, size of the Trusted Computing Basis from a security-sensitive function or a complete VM with its operating system, offered security guaranties), SGX and SEV differ. It is worth noting that these divergences are originated and defended in their respective patents. Patents are legal weapons in the no-mercy cloud server processor commercial war where Intel and AMD are engaged. As security is a key element to consider for present and future cloud operated systems, both companies invest massively and protect their research investment which results in these opposing approaches.

At the time of production of this analysis, Intel SGX 2.0 was already released (but not studied) and the authors omitted to consider code confidentiality and was not offered by SGX 1.0. As a matter of fact, the enclave code is in clear text in the application project. It is then transferred to the enclave (to be precise, its memory page allocation opts-in the secured mode) where it is protected by encryption in both confidentiality and integrity. In the sake of getting the code for analysis (typically look at vulnerabilities to exploit or reverse engineering), the attacker gets everything she wants on the project file. However, this is a description of how SGX was (failing to bring code confidentiality) until the recent past (2019). Since then, this highly critical SGX breach had been curated by Intel with its Protected Code Launcher (PCL) mode capable to digest encrypted enclave file. The enclave software is thus permanently encrypted and protected in both confidentiality and integrity. Conversely, as stressed in the cited publication [235], SEV does not bring any integrity guaranty. The code can be modified at any time. One can argue that modifying an encrypted code is not a straightforward operation.

Intel SGX	AMD Memory Encryption Technology (SME, SEV)
Provides Memory Integrity Protection	Does not provides Memory Integrity Protection
Vulnerable to Memory Side Channels	Vulnerable to Memory Side Channels
Vulnerable to Denial of Service Attacks (OS Handles System Calls)	Vulnerable to Denial of Service Attacks (Hypervisor Handles System Calls)
Small TCB (TCB is CPU package)	Large TCB (VM's OS is located inside TCB)
Vulnerable to Synchronization Attacks (TOCTTOU, Use-After-Free)	AMD Secure Processor Firmware Bug Discovered. (MASTERKEY and FALLOUT)

Table 5: SGX-SEV Comparison table (Abstract of Wayne University presentation at HASP, 2018)

As a reminder and as shown in the table above, vulnerabilities are not stopped by TEE. Wayne University technical survey went to use cases with real experiments with heavy process TEE inclusion for performance loss analysis, all along necessary steps to activate the two types of TEE. All these elements are pertaining when considering using a TEE for high performance legacy code and/or when considering a seamless setup for protecting any VNF at the lowest effort level on VNF vendors or operators. The study ends with a statement that "*SGX is suited for highly security-sensitive but small workloads. AMD SEV provides a greater amount of secure resources to applications, is faster and is far easier to use with a much higher ability to deal with legacy applications and services*."

Intel SGX 2.0 enclave key features are given here:

- Hardware fused root keys at Intel's production chain
- Processor-controlled decryption of created (encrypted) memory space (enclave). Several concurrent and isolated spaces can be created
- Ephemeral and runtime initiated and terminated enclave life cycle.
- Concept: Limit the Trusted Computing Base (TCB) to the minimal. Extraction of the TCB is worked out by the developer using Intel SDK.
- Extra functionalities possibly leveraged: remote attestation and data sealing.
- Version 2.0 has brought a significant improvement: software (enclave) confidentiality at any stage of the life cycle.
- Operates at ring-3 which has some limitations in what memory access it can have)

Intel SGX 2.0 enclave	
TEE Key criteria	**Compliance and information**
Isolation.	Yes
Code confidentiality.	Yes (with PCL mode, available from 2.0)
Data confidentiality.	Yes
Code integrity.	Yes
Data integrity.	Yes
Remote attestation of TCB.	Yes
Secure provisioning.	Yes
Secure data sealing-storage.	Yes
TEE secondary criteria	Compliance and information
Performance loss.	Low (with a restricted TCB, performance overhead is low)
TCB size.	Yes (restricted and limited code section is advocated by Intel)
Easy setup.	No (the code portion cut & trim with syst calls removal is a security expert task.
Several domains.	Yes, several concurrent isolated enclaves

AMD SME-SEV key features are given below:

- SME enables several memory encryption modes (full, partial and transparent). It is based on a dedicated AMD-SP (secure processor), featuring an ARM-based 32-bit crypto-module. AMD-SP deals with memory page "C-bit"'s content (0 or 1) of their virtual address to decrypt the data and code before transfer to the CPU. Keys are not accessed by the host-OS or hypervisor.
- SEV works at a lower grain: a virtualized content (a VM or a container). Threat model is a malicious host OS or hypervisor against a guest OS and payload. Isolation of user mode against lower ring level is delivered. SEV relies on SME and the management (by the SEV firmware) for key management.
- Code and data integrity are not offered but one can state that it is not an easy task to modify encrypted content.

- It operates at ring-0 (but is itself protected against ring-0 originated attack)

AMD SME-SEV Secure Memory Encryption-Secure Encrypted Vitualisation	
TEE Key criteria	**Compliance and information**
Isolation.	Yes
Code confidentiality.	Yes
Data confidentiality.	Yes
Code integrity.	No
Data integrity.	No
Remote attestation of TCB.	Yes
Secure provisioning.	Yes
Secure data sealing-storage.	Yes
TEE secondary criteria	Compliance and information
Performance loss.	Low, since hardware-based decryption, at VM or container initiation phase only.
TCB size.	Big, TCB is a container or a virtual machine with its guest OS
Easy setup.	Yes, no change on code. SEV firmware to mount on guest OS
Several domains.	Yes, each virtualized content (VM or container) is isolated. Several domains inside the same VM or container are not protected one against the other one.

Developer frameworks bridging SGX and SEV technologies: Google's Asylo and Microsoft's Open Enclave

As one cannot foresee any technical convergence of SGX and SEV, only a software abstraction layer (exposing common APIs to exploit both technologies) can bridge them. Software vendors and academics, as well as industry working group (Trusted Computing Group) had developed frameworks. As such [236] or [237] abstract the TEE to remove dependency from the hardware. These frameworks are certainly to be considered as they break the two SGX-SEV separation, making it possible for a developer to reach a TEE execution in situation where she does not control which soldered processor is on the execution machine as it is the case for off-premises execution (cloud). As at the end of the day, the framework activates diverging technologies (offering different guaranties), a question remains if this valuable workflow facility is not engraved with either a security loss or a performance loss, as one can foresee with any abstraction extra layer looking for the best of several underlying (diverging) techniques.

Trans-TEE (SGX-SEV) frameworks: Asylo and Open Enclave	
TEE Key criteria	**Compliance and information**
Isolation.	For each criterion, one shall refer to the underneath hardware TEE available (SGX or SEV), as they will be used. The frameworks do not break or improve the criteria for both hardware TEE types.
Code confidentiality.	
Data confidentiality.	
Code integrity.	
Data integrity.	
Remote attestation of TCB.	
Secure provisioning.	
Secure data sealing-storage.	
TEE secondary criteria	Compliance and information
Performance loss.	For each criterion, one shall refer to the underneath hardware

TCB size.	TEE available (SGX or SEV), as they will be used. The frameworks do not break or improve the criteria for both hardware TEE types.
Easy setup.	
Several domains.	

Developer frameworks democratizing Intel SGX

Intel SGX TEE is reputed to be complex to use and usually viewed as a good tool for academic research explanatory work. This obstacle to adoption gave birth to several initiatives aimed at making its implementation a much simpler thing. SGX-LKL [239] and SCONE [240] simplify the workflow, all sharing the same design idea of placing a micro kernel inside the SGX enclave to limit and control all interactions with the external world. For the users, these tools remove the burden of selecting a sensitive code section (which can only be done by a security architect, not always available) by absorbing complete applications. This is done at the cost of interfacing (proxying) all exchanges with the host which has an average performance cost of at least 30%. Some security sensitive applications deserve this overhead but cost burden on the machine may be too high in the general use case, especially in the telecom industry. More, these frameworks all deviate with Intel's recommendation for the smallest TCB, as they not only insert a complete un-touched application, paired with an external micro-kernel.

Easier SGX frameworks Panoply, SGX-LKL and Scone	
TEE Key criteria	**Compliance and information**
Isolation.	Yes
Code confidentiality.	Yes
Data confidentiality.	Yes
Code integrity.	No
Data integrity.	No
Remote attestation of TCB.	Yes
Secure provisioning.	Yes
Secure data sealing-storage.	Yes
TEE secondary criteria	Compliance and information
Performance loss.	High (in the range of 30% +) and in corresponds to the big TCB size.
TCB size.	Big, TCB is the complete binary level application extended with a micro-kernel (filtering syst calls)
Easy setup.	Yes, no change on code, the key objective of these frameworks
Several domains.	Yes

TEE for ARM and RISC-V platforms

TrustZone [241] creates two different "Worlds" (Secure and Non-Secure) using the same CPU. Isolation results from a complex inter-world switch and a well-guarded trustzone data access control, which radically differs from X-86 TEE memory page encryption mechanism.

Each world is allocated to its own resources (a different CPU can even be assigned to the Secure world) which cover the full range of functional elements of the device (CPU, memory, I/0). The concept splits the system into a Rich Execution Environment, controlled by a rich OS (feature-rich OS with possible user-defined relaxed controls and full openness) and a Trusted Execution Environment with a reduced and trusted OS. Switching from one world to the other is a complex and costly operation (which therefore shall be limited). By necessity and design, each world work on their own. Both worlds can communicate with the secure channel, orchestrated by AMBA bus (general SoC ARM architecture) acting as a diode for memory access. Secure world applications can get access to the memory of the Non-Secure World, but the reverse is not possible.

Trustzone fully complies with the specifications produced by Global Platform and it integrates its developer APIs.

ARM TrustZone and associated Global Platform APIs	
TEE Key criteria	**Compliance and information**
Isolation.	Yes
Code confidentiality.	Yes
Data confidentiality.	Yes
Code integrity.	Yes
Data integrity.	Yes
Remote attestation of TCB.	Yes (Secure boot from Global Platform)
Secure provisioning.	Yes
Secure data sealing-storage.	Yes
TEE secondary criteria	Compliance and information
Performance loss.	Depends on the number of interactions between both Worlds
TCB size.	Global platform advocates for restricting the TCB to the lowest. This demands to split code into two partitions (worlds) to reduce the TCB. However, the TCB includes a safe and limited OS, supposedly vulnerability-free
Easy setup.	No, the code split (cut and trim) into two worlds is a security expert task
Several domains.	No, there is only one secured world per platform: If you are in, you are sharing the same Secure World user space with all other security sensitive applications.

RISC-V Multizone

MultiZone [242] (license open source de Hex-Five Security) can be viewed as an extension of Trustzone. It creates not two but x security worlds, allocated with hardware resource and exchanging on a secure inter zone communication channel. The technology brings flexibility to security architect to define the Read and Write policy of the memory of each zone. These policies and the memory allocations are frozen in a signed Target Firmware image (HEX).

RISC-V Multizone	
TEE Key criteria	**Compliance and information**
Isolation.	Yes
Code confidentiality.	Yes
Data confidentiality.	Yes

Code integrity.	Yes
Data integrity.	Yes
Remote attestation of TCB.	Yes (Secure boot from Global Platform)
Secure provisioning.	Yes
Secure data sealing-storage.	Yes
TEE secondary criteria	**Compliance and information**
Performance loss.	Low
TCB size.	Big, as each zone is supposedly embarking its own OS
Easy setup.	Yes, apart the multizone configuration presenting, no change on binaries or OS required
Several domains.	Yes

Appendix C. Questionnaire

Dear Participant,

We kindly seek your response to this survey. The purpose of this survey is to define the user, stakeholder, security and privacy requirements from the business perspective for the ongoing H2020 project. INSPIRE-5Gplus aims at providing and demonstrating a smart, trustworthy and liability-aware 5G security platform for future connected systems. Briefly, the project is built around the following objectives:

- A **conceptual architecture** for supporting zero-touch end-to-end smart network and service security management in 5G and beyond networks. The architecture will leverage on flexibility of softwarization technologies (e.g., SDN/NFV) and smartness of AI/ML techniques;
- **Software-defined security (SD-SEC) orchestration** and management that enforces and controls security policies in real-time and adapt to dynamic changes in threats landscape and security requirements in 5G and beyond networks;
- **Novel AI-driven security models**, including AI-empowered Moving Target Defence (MTD) mechanisms and AI-driven Cyber Threat Intelligence (CTI) framework to empower smart security management with proactive defensive posture. The use of distributed and cooperative AI/ML models will be fostered to improve the prediction and detection accuracy as well as latency of AI-driven security models;
- Advanced mechanisms to foster trustworthiness of smart SD-SEC solutions in a multi-tenant/multi- domain setting by empowering trust in software components (e.g., VNFs) and AI/ML techniques. **Trust in software components will be based on Trusted Execution Environments (TEEs), new Digital Rights Management (DRM) approaches**, novel AI-powered validation tools, and a new labelling scheme. Trust in AI/ML models will rely on interpretability, adversarial machine learning, and blockchain;
- New mechanisms to enforce liability of involved parties when security breaches occur and/or system fail, including smart contracts and potentially VNF package Manifest to define Trust Level Agreement (TLA), mechanisms to enable AI liability, and new Root Cause Analysis (RCA) techniques.

Therefore, the questions asked in this survey aim to assist the project in collecting business, security and privacy requirements of the stakeholders in 5G infrastructure and services with respect to fulfilling these objectives. Analysis of the answers you provide will be used for the system specification and architectural design of the project's foreground. We would appreciate it if you could kindly answer the following questions to the best of your knowledge. Please note that in the course of analysing your response, your identity or that of your organisation will not be revealed and no publication will include any personal data of the respondents.

Business and organisational

1. What are the major threats you would like 5G services and applications to be protected?

2. What critical features in terms of security of 5G infrastructure would you require to be improved?

3. What key security design improvements would you consider as a plus compared to your business activities? How would you like your personnel to be assisted in this regard?

4. What would be the business impact of a security incident for your organization?

5. What type of technologies of INSPIRE-5Gplus you consider are more likely to improve your security? Explain briefly why?

6. What key processes, policies, best practices on privacy and security in your organisation do you consider key for the use of the proposed INSPIRE-5Gplus?

Regulatory compliance and reputation

7. What are the key standards and regulations your infrastructure has to comply with for security and privacy? How do you see INSPIRE-5Gplus can help to achieve this compliance?

8. What feature would increase your trust in relation to exchanging anonymous information about incidents within a closed group of 5G operators and providers?

9. Please describe possible usability requirements regarding the utilisation and deployment of INSPIRE-5Gplus which will be developed during the project (e.g., the tutorial of each components/processes should be available in different languages).

10. What availability tests do you consider necessary for testing the availability/efficiency of INSPIRE-5Gplus technologies you are waiting? Could you please specify what type of security KPIs are you expecting?

11. What are your availability concerns or issues? How do you think INSPIRE-5Gplus technology may assist you?

Other aspects

12. What kind of other improvements and/or technologies would like INSPIRE-5Gplus to implement and what are the expected value you would hope to derive from them?

SN	Additional improvements/requirements	Impact expected	Other remarks