INSPIRE-5Gplus

Evolution of 5G Cyber Threats and Security Solutions

White Paper

March 2022

Table of Contents

List of Figures

Abbreviations

5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, Accounting
AAE	Adversarial Autoencoder
AI	Artificial Intelligence
ML	Machine Learning
NF	Network Function
SBA	Service Based Architecture
SSLA	Security Service Level Agreement
SDR	Software Defined Radio
SMD	Security Management Domain
E2E	end-to-end
ZSM	Zero touch network & Service Management
HSPL-OP	High-level Security Policy Language Orchestration Policy
MSPL-OP	Medium-level Security Policy Language Orchestration Policy
CTS	Cyber Threat Landscape
MANO	Management and Orchestration
ENISA	European Union Agency for Cybersecurity
VNF	Virtual Network Function
FL	Federated Learning
TEE	Trusted Execution Environment
SCA	Side Channel Attacks
EPC	Enclave Page Cache
TME	Total Memory Encryption
NDT	Digital Network Twin
GANs	Generative Adversarial Networks
CTI	Cyber Threat Intelligence
GPDR	General Data Protection Regulation
NIS	Network and Information Security
ISAC	Information Sharing and Analysis Centres
TLS	Transport-Layer Security
IMSI	International Mobile Subscriber Identity
EAP	Extensible Authentication Protocol
OSINT	Open-Source Intelligence
TAXII	Trusted Automated Exchange of Intelligence Information
CSV	Comma Separated Values
MTD	Moving Target Defense
MiTM	man-in-the-middle
DoS	Denial of Service

VIM	Virtual Infrastructure Manager
FeM	Further Enhanced Mobile Broadband
MOTDEC	MTD controller
UE	User Equipment
DLT	Distributed Ledger Technologies
p2p	peer-to-peer
RCA	Root Cause Analysis
ICS	Information and Communication Systems
SP	Service Providers
RT-SSLA	Real Time SSLA
SLO	Service Level Objectives
RL	Reinforcement Learning

List of Contributors

Editor In Chief

Rodrigo Asensio, University of Murcia, Spain

Section Contributors

Edgardo Montes de Oca, MONTIMAGE EURL, France

Huu Nghia Nguyen, MONTIMAGE EURL, France

Vinh Hoa La, MONTIMAGE EURL, France

Manh Dung Nguyen, MONTIMAGE EURL, France

Pol Alemany, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Ricard Vilalta, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Raul Muñoz, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Wissem Soussi, Zurich University of Applied Sciences, Switzerland

Gürkan Gür, Zurich University of Applied Sciences, Switzerland

Tarik Taleb, University of OULU, Finland

Vincent Lefebvre, TAGES, France

Gianni Santinelli, TAGES, France

Antonio Pastor, Telefonica I+D, Spain

Dhouha Ayed, Thales SIX GTS France SAS, France

Cyril Dangerville, Thales SIX GTS France SAS, France

Pawani Porambage, University of Oulu, Finland

Chafika Benzaid, University of Oulu, Finland

Maria Christopoulou, National Centre for Scientific Research Demokritos, Greece

Jordi Ortiz, University of Murcia, Spain

Alejandro M. Zarca, University of Murcia, Spain

Rodrigo Asensio, University of Murcia, Spain

Final editing

Uwe Herzog, Anja Köhler, Eurescom

Please cite:

R. Asensio, C. Benzaid, P. Alemany, D. Ayed, M. Christopoulou, C. Dangerville, G. Gür, V. Hoa La, V. Lefebvre, E. Montes de Oca, R. Muñoz, H. Nguyen, M. Nguyen, J. Ortiz, A. Pastor, P. Porambage, G. Santinelli, W. Soussi, T. Taleb, R. Vilalta, A. Zarca. **White Paper: Evolution of 5G Cyber Threats and Security Solutions**. INSPIRE-5Gplus, Mar. 2022.

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

Intended audience

This white paper targets individuals interested in cybersecurity in the context of 5G networks and beyond. Accordingly, it addresses the challenges and tendencies in state-of-the-art security solutions and exemplifies the use of these solutions to daily and understandable threats. It goes in depth into the selected solutions with special emphasis on Chief Information Security Officers (CISO) as well as Chief Technology Officers and other decision-making roles putting them into context thanks to the analysis of threat evolution and tendencies in security including the effects produced by COVID-19 pandemic.

Executive Summary

5G aims to change the way we offer services and how we interact with them, leaving as a legacy static services and configurations and offering adaptability not only depending on the type of application but according to the volatility of the environment conditions and the devices restrictions, UE subscriptions or Service Level Agreement (SLA). 5G implies a structural change, incorporating a service-based architecture (SBA) at the core of the network, allowing it to be modularized, distributed and scaled; having capabilities to incorporate new Network Functions (NFs) to the system, where the control plane and data plane are fully decoupled. It is also characterized by the inclusion of new forms of access, both 3GPP and non-3GPP compliant (Wi-Fi). All this forms a very heterogeneous set of technologies and devices that make management one of the main challenges, especially in terms of security, as 5G consider E2E services involving multiple and different domains (e.g., Edges, Centralized Clouds, RAN...).

The evolution of 4G towards 5G was a slow and laborious process. However, this panorama changed rapidly with the outbreak of COVID-19, where the surging demand for digital services by millions of consumers around the globe, led to unprecedented network traffic levels, accelerating the digital transformation of the telecommunications industry. Millions of companies expanded their business model portfolio by standardizing teleworking and remote office solutions, while people constrained in their homes, increased their online presence, through the use of streaming services, digital workplace solutions and online learning. These circumstances dictated that telecom providers must adopt their legacy business models and infrastructure in order to ensure continuous delivery of digital services through optimized backend practices, increased access coverage and efficient service orchestration. The flexibility and scalability that characterizes 5G when it comes to providing services became a key factor to be able to dynamically adapt services to the demands of the environment, driving a faster evolution towards 5G.

On the other hand, the evolution towards the Service-Based 5G architecture is also increasing the attack surface that the telco industry has to address. That is why it is necessary to be able to manage with flexibility, intelligence and speed the changing needs in a dynamic way, guaranteeing the robustness and security of the system constantly. This task, due to its high complexity and strict requirements to not compromise the system, must be automated, where AI and ML must acquire a major role to be able to solve these complex problems and adapt to the context. These AI and ML engines will need the system to be fully monitored continuously, in order to detect anomalies (e.g., possible attacks) and take reactive decisions, where in turn they need to be sure that the data collected are trustworthy and have not been tampered with. In addition, to perform these management operations, a language flexible enough is necessary, in order to model all the heterogeneous characteristics of the 5th generation of mobile networks and different domains, thus enabling the management of E2E services. In this sense, SLA and policies are presented as a solution with the level of abstraction required to model the system requirements into capabilities, allowing the system to be able to autonomously communicate with all its parts regardless of the underlying technology and to execute actions where necessary.

In this context of security management for 5G networks, INSPIRE5G-PLUS emerges as a 5G-PPP Phase 3 project, which presents a multi-tier and multi-domain architecture based on the ETSI Zero touch network & Service Management (ZSM) standardized architecture, which automates security policy-based orchestration through a closed loop, where an E2E Security Management E2E (E2E SMD) coordinates, directs and validates inter-domain security management, while supervising the actions taken intra-domain by each Security Management

Domain (SMD). INSPIRE5G-PLUS is able to take as an entry point a Security Service Level Agreement (SSLA) established with a customer and proactively trigger the enforcement of security policies to enforce the agreement. On the other hand, it has AI and ML engines capable of using data collected by monitoring systems to detect anomalies and possible attacks and establish intra- or inter-domain actions to be taken through security policies. These policies meet the condition of flexibility to model multiple security capabilities through languages with different levels of abstraction, High-level Security Policy Language Orchestration Policy (HSPL-OP) and Medium-level Security Policy Language Orchestration Policy (MSPL-OP), from higher to lower level respectively. This abstraction introduced by the different policy languages allows finally to be translated into specific configurations of concrete security assets (e.g., SDN controller, Monitoring Agent, IPsec tunnelling establishment).

This whitepaper studies the evolution of the cyber threat landscape from the beginning of the pandemic and how the network usage habits of millions of users have changed. Where demand for online services has reached levels never seen before and due to the great acceptance that it has had among companies and public agencies due to economic savings (among other reasons) is not expected to return to pre-pandemic levels. In order to solve the problems related to cybersecurity, we present the INSPIRE5G-PLUS security enabling technologies, the main challenges concerning each of these technologies and how they can be applied to improve cybersecurity in 5G networks.

1 Introduction

COVID-19 had a major impact on the network behaviour of corporate and non-corporate activities and introduced additional strain to operators. The pandemic affected the Cyber Threat Landscape (CTS) as well, producing challenging scenarios in terms of: *i)* network management, to ensure service continuity and user experience, and *ii)* system security management, considering that the attack surface has increased considerably by the use of heterogeneous devices and technologies using different type of access. During the different phases of the pandemic, operators and application service providers had to adapt their offered services to the ever-changing conditions and constraints. For this reason, it is important to monitor the CTS evolution, accumulate the main security and management challenges and consider solutions stemming from the 5G ecosystem, having propelled its research and development on multi-technology and multi-tenant environments.

These 5G solutions point to SDN, NFV and MEC as the enabling technologies of the flexibility and programmability needed to address security challenges. Cloud-RAN is a concrete example of these three technologies applied to cellular networks: they enable the virtualization of the base station operation on open hardware, decrease the computational burden of the RAN by moving all or some resource intensive operations to centralized servers and allows flexible service deployment at the Edge. We can also highlight the evolution of Management and Orchestration (MANO) and dynamic E2E Network Slicing solutions.

Considering the complex characteristics of such heterogeneous scenarios in cellular networks, it is necessary to enable the automation of management processes, using the advantages of SDN, NFV and MEC along with AI and ML, to unleash the full potential of 5G. These technologies can optimize all system procedures, adapt services and resources with a global vision of the system, with special emphasis on maintaining security. For 5G security management to be effective, it is necessary to deal with its complexity, which requires continuous learning of threats through AI and ML for detecting zero-day threats, as well as being able to share the learned information securely with other entities. This cooperation is of vital importance to mitigate the rapid expansion of exploitation of detected vulnerabilities. Likewise, the use of DLT technologies is of special relevance, since it will allow storing reliable distributed information between different nodes of the system, facilitating the detection of malicious components when they try to spoof the system. Assuming that a threat or attack is detected in the system, the system must be able to identify the root of the vulnerability in order to mitigate and correct it.

Considering the multi-tenant capabilities across network slices that 5G offers, a way to introduce the security requirements of these tenants into the system is needed. These requirements should act as a strictly enforceable contract between the system and the tenant. In turn, they must be modelable within the system and translatable for each of the endpoints in order to execute actions to ensure compliance.

In this regard, with this work we introduce the current situation of the Cyber Threat Landscape once the pandemic has passed to another stage with less restrictions, we will check if the effects of the pandemic on the previously mentioned behaviours have subsided or however, they seem to be maintained or even increased (Section 2). We will also relate how INSPIRE-5Gplus affects the autonomous management of both network and security through its various enablers, explaining their usefulness and the latest challenges encountered by the scientific community (Section 3) as well as use cases related with the use of INSPIRE-5Gplus enablers

inside and/or outside the project. Finally, we present conclusions and future work for the explained enablers (Section 4).

2 Evolvement of 5G Cyber Threat Landscape

The situation created by the pandemic has led to the digital impulse of all kinds of businesses and companies, which have been forced to adapt to recent technologies to offer uninterrupted service delivery. Even companies with elevated level of digitalization have changed their habits to face the pandemic, they had to rapidly introduce cloud computing to their services to adapt to the higher demand, developing a strong dependency on online facilities that currently has increased the usage of the network more than when we were inside the first or second wave of COVID-19.

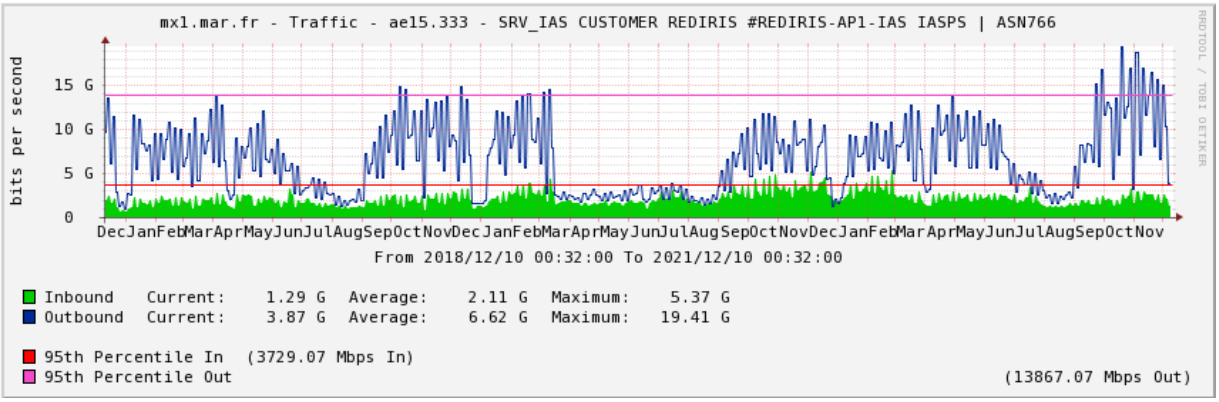

Figure 1: Srv_global customer rediris from 2018 to 2021 by GÉANT tools [1]

Figure 1 depicts the network traffic from the University ISP RedIRIS [1]] and we observe the highest network usage since 2018. This could be reasoned by considering that Universities have adapted their resources on cloud environments offering streaming video services among other online facilities, and although that attendance has returned to pre-COVID-19 levels, these facilities are still on demand from both students and professors. The same reasoning could be applied to other business sectors, where the cost saving and efficiency granted by online services made companies aware of the benefits of the use of these tools, so the impulse caused by the need for online tools has led to a proliferation of the paradigm shift in dealing with the structure of business.

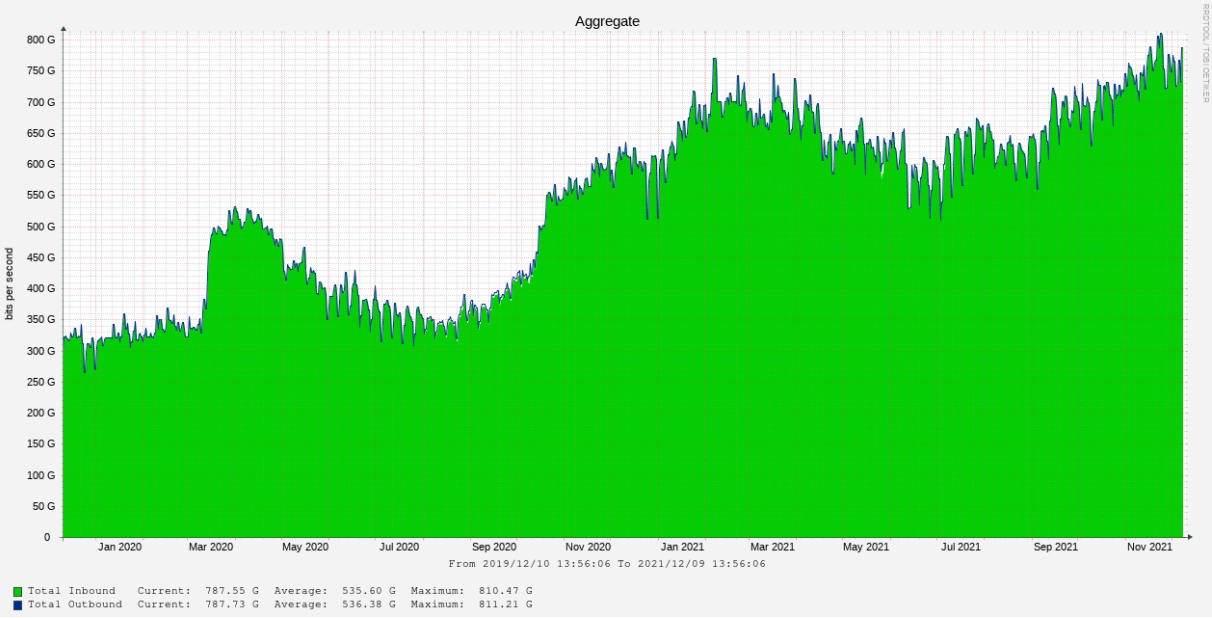

Figure 2: Aggregated network usage in Espanix neutral interconnection [2]].

Figure 2 represents the Spanish network traffic by Espanix [2]] neutral interconnection. It is clearly observed the network usage peak during the lockdown, and how the dependency on online services has increased to levels never seen before. In this context, 5G has been

introduced at the right moment, that as well as the advances made on edge and cloud computing and virtualization have allowed the decongestion of the network and the continuity of the online services.

Considering the current network traffic demands, it is apparent that there is no expectation to return to pre-pandemic network usage levels. Thus, there are on-going efforts for maintaining an updated Cyber Threat Landscape, incorporating new threats closely related with changes in the network habits.

In this regard, the European Union Agency for Cybersecurity (ENISA) [3]] is dedicated to achieving a high common level of cybersecurity among Europe. ENISA has been publishing for 9years the ENISA Threat Landscape (ETL) report [4]], identifying prime cyber threats, major trends observed with respect to threats, threat actors and attack techniques. The last report was made in October 2021, but ENISA has also published documents focusing on the cyber threat landscape of 5G networks (2019, 2020) [5]]. In the last 5G Threat Landscape report, the evolution in the standardization, migration and integration from 4G to 5G, and developments made in the architecture (Release 16) are also included, as well as improvement of information related to vulnerabilities and relationship with sensitive assets, but due to preliminary stages of 5G solutions thus also the 5G deployments in 2020, all threat agents are based on hypothetical attacks, as real attacks on 5G were not yet possible.

With the significant increase in network usage and the increased attack surface, achieving the intelligent automation of flexible, robust, and scalable security management is considered as one of the main challenges. In this consideration, there is a current trend to entrust 5G security management to AI systems, where ML engines acquire and analyze vast amounts of data; learning and instructing the system to react to threats and attacks, empowering the wireless networks to self-control, adapt and heal themselves with changing user, service, and traffic requirements. While ML is expected to play a major role in addressing the main security challenges of 5G, the usage of this technique itself symbolizes a novelty in the attack surface, arising a risk of structurally affecting the maintenance of security. Belonging to ML vulnerabilities, the main threats related to unfair use or resources, denial-of-services and denial-of-detection, and leakage of private and confidential information has been studied [6]]. Considering that ML will perform the core of maintaining the security of the system, the threats affect several ambits of 5G: Infrastructure Management, Network Operations, Service Orchestration, Assurance and Security Applications. There is also a novelty in the attack vectors that could potentially exploit these threats: Network Components such as base station, SDN switches, virtualized infrastructure and functions, or cloud and edge servers hosting ML functions. Also, open air interfaces and SDR-based frameworks could influence aspects such as measurements of the physical radio layer properties, for instance by tampering application layer UE data if it is not integrity protected. It is considered potential misbehaving UE introducing malicious data for ML functions that use UE component's Information. And the development and supply time threats for ML software products, as well as devices, which are running ML and collecting data.

Even with the implicit sensitivity of ML techniques, the promising solutions to 5G security challenges it offers make it a huge field of research that is ambitious for research teams. In particular, applying security to IoT is one of the main challenges. The resource constraints of these devices make them particularly vulnerable to DoS threats, intrusion and data leakage, with IoT devices representing a significant portion of the UEs that will be connected to 5G networks. With this regard, [7]] proposes a novel ML based security framework leveraging

SDN and NFV enablers for coping with the expanding security aspects related to IoT domain mitigating threads previously introduced.

Focusing now on 5G protocol stack, there are several efforts to gather and update the key elements of 5G networks security in addition to the standardization body 3GPP itself. In [8]], a study focusing on the proper configuration of the equipment and performing correct authentication and authorization of network elements is made, where also an in-deep analysis show how PFCP and HTTP2 protocols vulnerabilities could affect system security.

3 INSPIRE-5Gplus Enabling Technologies

3.1 Automation and Zero-Touch Management (ZSM)

3.1.1 Introduction

5G Networks have increased network complexity, rendering practically impossible and non-cost-effective for human operators to manage all the heterogeneous technologies and devices. Hence, automation is a key requirement to achieve the stringent performance and to cope with system complexity and security characteristics of 5G networks [52]]. Management automation will not be reduced to a single domain, but this self-management process capability will be realised E2E, crossing multiple domains and technologies, enabling massive savings, displaying capabilities such as self-healing and self-repairing, as well as offering flexibility and adaptability in the services requested. In this context, ETSI's Zero Touch network and Service Management Industry Specification Group is a prominent initiative behind achieving the full automation of network management. The main objective of the ETSI ZSM ISG is to specify an end-to-end reference architecture for network and service management [55]] that enables agile, efficient, quality-of-service management and automation of new and future networks and services. The ZSM framework reference architecture is designed to enable fully automated management of networks and services in multi-domain environments, spanning operations beyond legal operational boundaries.

3.1.2 Challenges in using Zero-Touch Management

Despite the advantages of the full (i.e., closed loop) automation of network and service management and operation intended by a ZSM system, this last can rises several security concerns. In INSPIRE-5Gplus, we comprehensively investigated the potential security threats that may impede the adoption of ZSM in 5G and beyond networks [52]]. The identified security threats have been classified into five categories, namely: (i) Open API's security threats, (2) Intent-based security threats, (3) security threats driven by closed-loop networked automation, (4) AI/ML-based attacks, and (5) attacks due to adoption of programmable network technologies (i.e., NFV and SDN). In addition to our previous findings, we consider that the emerging need of coordination between multiple management closed loops to ensure system-wide consistency and efficiency may raise serious concerns about privacy and security. Indeed, the closed loop coordination entails hierarchical and/or peer-to-peer interactions between multiple closed loops for either delegation and escalation of goal(s) or issues, or for coordination of actions and sharing of information, respectively [53]]. For instance, as illustrated in Figure 3, an E2E security closed loop can delegate to the security closed loops at the different management domains (MDs) the task of predicting a security event (e.g., a DDoS attack) against a slice X and automatically enforcing preventive and/or corrective actions to prevent the problem reaching the end user. Moreover, an energy optimization closed loop deployed to dynamically decide the optimal placement of the core network (CN) sub-slice's VNFs on the physical servers can coordinate and share its decision with the security closed loop in order to identify the optimal placement schema that ensures the desired security service level agreement (SSLA). Such interactions and exchange of information between closed loops require mechanisms that allow to establish trust between the communicating closed loops by guaranteeing the accuracy and integrity of the shared information. Furthermore, mechanisms to prevent potential privacy leakage from the

exchanged information are of upmost importance, especially when the interacting closed loops are under different administrative domains.

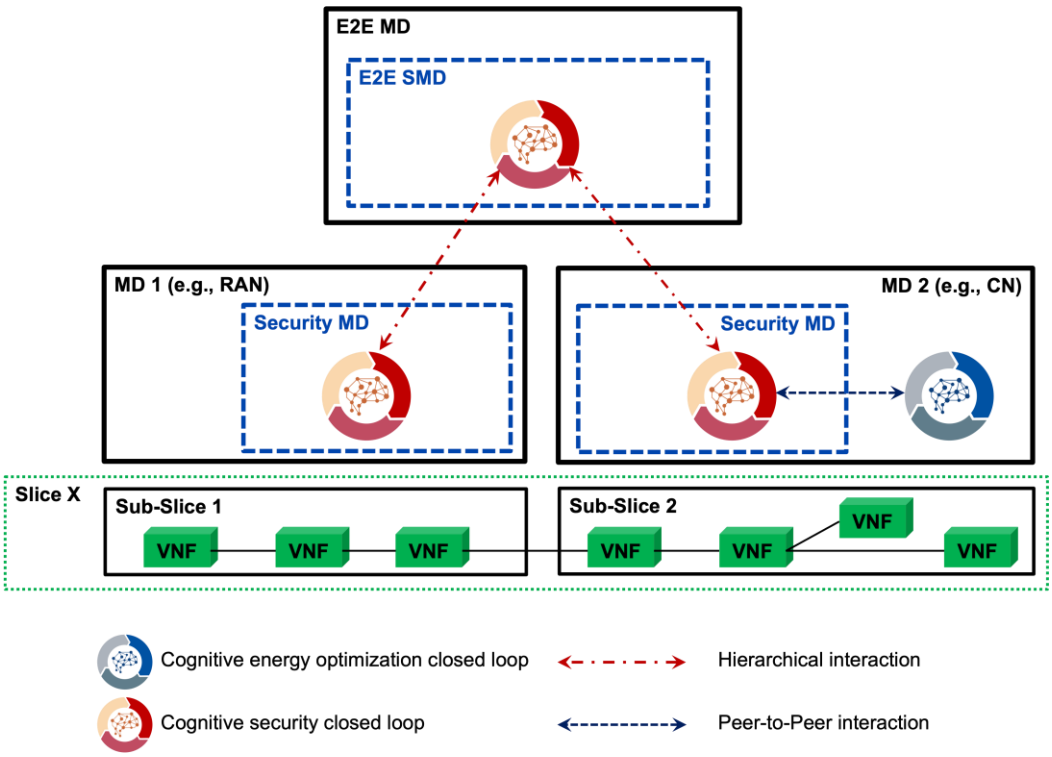

Figure 3: Closed loop coordination.

3.1.3 Use cases

3.1.3.1 Secure and Privacy-Preserving Closed Loop Coordination

The closed loop coordination topic has recently gained much attention from the standards developing organizations (e.g., 3GPP [54]] and ETSI ZSM [53]]). However, the ongoing efforts are mainly revolving around how the coordination between multiple closed loops can be enabled and governed. To embrace the security-by-design vision, it is important that the security and privacy concerns should be considered in the closed loop coordination specifications. One potential enabling technology that can address the privacy issue stemming from closed loop coordination is the Federated Learning (FL) technique. In fact, FL allows to knowledge sharing between closed loops without exchanging raw data. However, as we will elaborate in Section 3.3, FL unleashes new threat vectors that need to be tackled.

3.1.3.2 ZSM end-to-end network slicing

Network slicing is one of the main enablers of the next generation of services. They have been designed to support a vast number of use cases with very specific requirements for each slice deployed. But deploying thousands of individual slices where each can be created, configured, managed or reconfigured to meet the specified SLA is a challenge [56]].

To address this ZSM has released the GS ZSM 003 [57]] specification for a blueprint architecture (based on ZSM) with solutions for zero-touch management and orchestration of network slicing E2E and cross domain. This specification defines the processes of instantiation,

activation and operation of network slices. ZSM end-to-end network slicing specification supports a number of business models and scenarios through the introduction of network slicing and third-party tenants. Now the tenant goes from not being able to interact with the slices, to being a tool, becoming a "Network Slice as a Service" model, being able to manage and adapt it to the current needs through exposed interfaces.

3.2 Trusted Execution Environment (TEE)

3.2.1 Introduction

Trusted Execution Environment as AMD's SEV, ARM's Trustzone and Intel's SGX will play a key role in protecting core network, edge and AI/ML, delivering outstanding security properties to software and data in the context of untrusted execution locations. While we studied the main obstacles when employing these technologies with a higher focus on Intel's SGX as the most studied contender, we have also demonstrated the relatively low or insignificant impact of all past and probably future side channel attacks in a typical networking deployment where classical security provisions should be normally taken (e.g., platform-O.S. authentication, process white-listing).

Consequently, the main questions when considering TEE use in the upcoming future are the performance impact and the workflow complexities.

3.2.2 Challenges in the use of TEE and Intel's SGX

The challenges to use TEE in telecom industry have been listed in INSPIRE-5Gplus D2.2 [32] as follows:

The unrivalled security properties brought by TEE change the software security game. A paramount research effort from security responsible academics to stress and challenge these properties has been placed since the five last years, essentially targeting Intel's SGX. As depicted by D2.2 technical survey, four waves of Side Channel Attacks (SCA) from cache-timing first generation to micro architectural last generation, have emerged from a small group of reputed universities and smart researchers with deep X-86 architecture understanding. The good thing which can be drawn is that none of these highly sophisticate attacks can be worked out in secure SDN deployments where the platforms (OS and co-residing process) are checked. More, with our thorough technical survey on SGX's SCA we reached the conclusion that the common security threat to all of these attacks pertains to pre-known victim (e.g., cryptographic primitive). Conversely, proprietary code will stay safe in SGX and are not exposed or threatened to SCA.

For these reasons, security breaches of SGX from SCAs shall be highly relativised and actually be viewed as secondary against the performance impact and workflow implications. Limiting the performance impact demand some understanding on the two main causes: Page decryption before processing and execution context changes (from untrusted to trusted execution). Workflow implications varies with the processor vendor. A well-known issue for SGX is the exclusion for system calls produced from the enclave-inserted code, which imposes their extraction at source level prior to enclave compilation.

At deployment stage, as TEE technologies differ from one vendor to another (including inside the X86 world dominated by Intel and AMD), TEE-secured software shall be executed on specific TEE-enabled processors loaded with ad hoc BIOS and kernels. All attempts to brake the TEE silos do it at the cost of degraded security (by bridging diverging concepts) or

degraded performance (by adding an abstraction layer), as discussed in INSPIRE-5GPlus D2.1 [30]]

We believe the future will bring marginal security improvements but more significant progress on both performance and workflow sides. It is worth noting that in the recent months, the 128 Mb limitation of Intel's SGX has been broken to expand to 512 Mb for one of the two sockets and 1Tb for two of the two sockets of its third generation Xeon Scalable processors [30]]. For this, Intel's design has diverted from the Merkle tree layout to use "AES-XTS" technology. This reflects the strong commitment of Intel on SGX technology. Expanding the size of the SGX Enclave Page Cache (EPC) is aimed at breaking the limitations of SGX and make it compatible to new memory consuming usages such as AI/ML, while reducing the page swapping overall overhead.

In addition to that, it is also important to mention Intel Total Memory Encryption (TME) technology [30]], which brings an additional complementary security property for confidential computing, remediating to possible hardware-based attacks on DRAMs. Looking at the TME descriptive paper, one can consider the sharing of AES-TXT newly designed technology on both TEE and TME. Intel's press release on TME was issued in April 2021 the first Ice Lake (TME capable) processors were on the shelves on July 2021.

3.2.3 Use case - SGX Protection of virtual security function

At INSPIRE-5Gplus, we have been developing Systemic-SGX taking advantage of SGX strong shield while reducing both performance and workflow impact. In a demonstrated use case, Systemic-SGX is used to protect a virtual Security function from Montimage dubbed as MMT-Probe. Our design drastically diverts from the integral placement of MMT-Probe inside SGX.

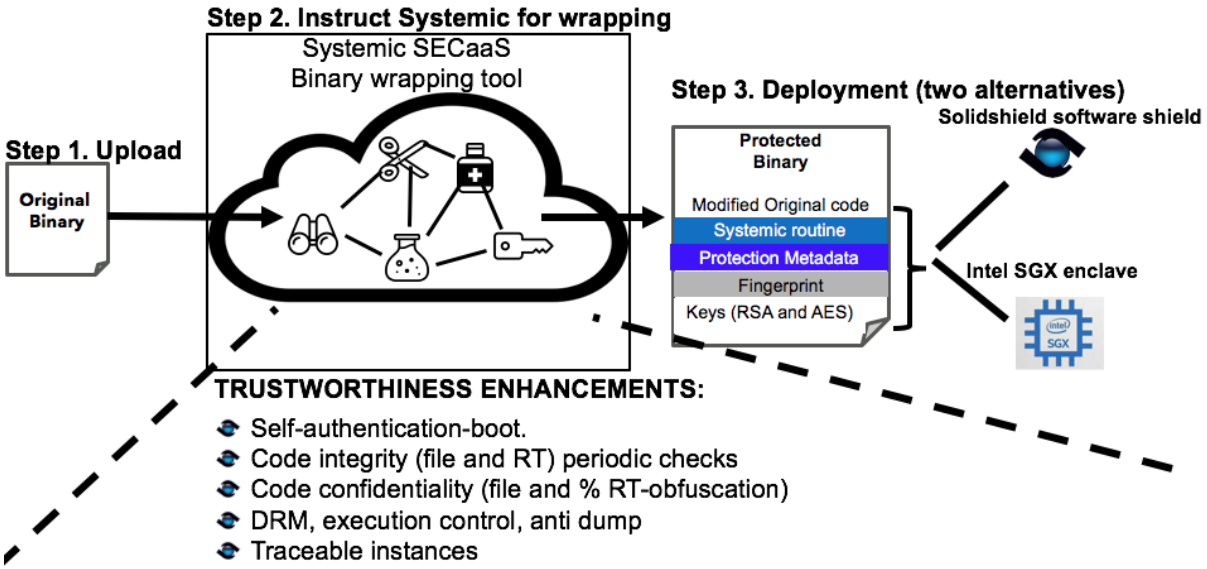

Figure 4: Systemic-SGX general view (workflow, security functions and deployment)

Systemic-SGX leverages SGX security, shielding our Systemic routine inside and which unrolls several security functions consecutively: (self-) authentication check, decryption of the code semantics, periodic runtime integrity checks, control flow obfuscation and fingerprinting. The security pattern is relevant to bring a solid initial security level with a progression margin. Systemic-SGX does not claim to deliver SGX's native security level (i.e., the highest level for

software security) for the code Systemic-SGX protects. Our setting brings the SGX-native security level to Systemic routine which confers security measures to the protected code which remains outside SGX. The solution is designed to confer high security measures through an automatic seamless setup, decreasing workflow constraints drastically. For instance, the periodic integrity checks on the protected code for instance cannot be broken and by-passed as they are operated from within SGX. More SGX is the place to hide the keys associated to the code decryption and authentication. Last, Systemic-SGX routine can transfer unforgeable execution monitoring elements (e.g., integrity, proof of execution) to a centralized orchestration position. From this centralized position, the protected software can be fully controlled. In the networking industry, inter-domain and cross-domain full traversal process or application controllability is a raising requirement fulfilled by Systemic-SGX. Our margin of progress resides on the confidentiality aspect and notably against memory introspection aspect. At the current stage, Systemic-SGX conceals the execution flow graph. The solution will evolve to create more semantic dependency between the protected code and systemic routine. The objective is to augment the dependency to what is inside SGX but keeping our same automatic set-up employing a unique and common to all protected program Systemic routine.

Regarding Systemic-SGX design, it is secondarily aimed at minimizing SGX EPC usage to limit the enclave page swap decryption costs as well as the context switches while no system calls cleansing is anymore required. This is obtained by quarantining our Systemic security routine inside SGX, which itself checks what is running outside (i.e., the code to protect). The performance optimization of the quarantined routine is done once for any code to protect without needs to be removed as the code lays outside SGX.

On the workflow consideration, we do not fix the processor market fragmentation, but at least, there are no special effort for one type of TEE when using Systemic-SGX solution. More, as far as Intel's SGX is concerned, it is worth stressing that our Systemic-SGX solution requires only one single license from Intel and usable for any protected software. In short, it deals with Intel's enclave (legally and technically) for our own code only and once. To augment our solution usability, Systemic-SGX automatic set-up (on binaries) can be ported or better extended to leverage AMD's SEV or ARM's Trustzone following the same pathway. Noticeably, Systemic-SGX already offers the means to protect code when no TEE is available and by use of our code virtualization technology. Another benefit of the solution is to be independent to the TEE (e.g., hardware-based, software based) which can be used, thus breaking the silos and frontiers erected by CPU vendors, a major cause of TEE concept market slow or low adoption.

3.3 Artificial Intelligence (AI) and Machine Learning (ML) Techniques

3.3.1 Introduction

The standard setting in ML considers centralized datasets which are tightly integrated into the system. However, in most of the real-world scenarios, data are usually distributed among multiple entities. More specifically, the centralized data collection is challenging due to the higher communication cost for sending data, when the devices create large volumes of data, serious privacy issues coming with the sharing of sensitive data, overfitting issues with the small datasets and the biased local datasets. Federated Learning (FL) is a distributed learning concept where end user devices or workers are participating for learning process. Central entity or parameter server shares the training model and aggregate the local model updates coming from workers. Workers train the shared model locally using their own data and send

the trained model back to the parameter server. Parameter server aggregates the received models and shares the aggregated model to workers. The final model needs to be as good as the centralized solution (ideally), or at least better than what each party can learn on its own. FL brings the advantages in terms of improving privacy awareness, low communication overhead, low latency and addressing the distributed networking scenarios in the more complex networks. These benefits have stimulated the recent growing interest in applying FL for 5G and beyond networks to meet their stringent isolation demands and data sharing regulations[41]]. It is worth mentioning that FL concept is officially introduced in 3GPP R17 standard as a key enabling technology to improve the performance and quality of 5G and beyond network management such as slice SLA guarantee, wireless network optimization, and enhanced security [42]].

An alternative commonly adopted today is to work with offline training and subsequent online inference deployments. As an advantage, offline training allows taking advantage of higher computational capacity (e.g., GPUs) and higher iterations to deliver more complex models that can also be optimised on systems with fewer resources in distributed inference engines, such as the IoT [49]]. Apart from the disadvantages of centralised ML mentioned above, the offline approach needs to periodically retrain the models with fresh data to update the models, which requires data from 5G production networks. To address these problems, a new paradigm has recently been proposed around the Digital Network Twin (NDT) concept [50]. As a solution that allows creating a virtual image of a physical network, the NDT is positioned as a potential solution to apply activities related to ML training, such as controlled data generation, capture and engineering activities (labelling, normalisation, feature extraction, optimisation, etc.), and finally validate ML inference models, prior to their deployment.

3.3.2 Challenges in using Federated Learning

The growing enthusiasm for FL adoption in managing future mobile networks should not overlook the security concerns stemming from the use of FL. Indeed, FL is vulnerable to several attacks that if exploited can undermine the performance and security of FL-based services. In addition to threats targeting centralized ML models [43]], FL introduces new security risks that we will highlight in what follows.

FL is vulnerable to model poisoning attacks by design. Parameter server can be poisoned using minimum of one adversarial worker. This will affect the learning process of the entire network. The problem is that the parameter server cannot guarantee that the workers provide accurate local models and have no control over the level of security at each worker. Another issue is that it is possible to encounter single point of failure at the parameter server. Therefore, it is necessary to implement defence mechanisms at the parameter server to distinguish poisonous and honest users.

Despite the merit of FL in preserving the privacy by sharing only the local model parameters instead of the data, the privacy leakage risk is still possible. In fact, a malicious adversary, including an honest-but-curious aggregator (i.e., parameter server) or an honest-but-curious local worker can perform membership inference attacks against other local workers. A membership inference attack consists in exploiting the shared model parameters, particularly the gradient information, to infer the private local training data [44]]. Recently, the emerging Generative Adversarial Networks (GANs) have demonstrated their effectiveness in conducting inference attacks against FL [45][46]], ushering in a new era of pitting AI against AI.

3.3.3 Use case - Robust and Privacy-Preserving Federated Learning

To build a robust FL, we need not only to safeguard the local workers against adversarial attacks targeting local models, but also to counteract the aforementioned new adversarial threats targeting the FL process. In INSPIRE-5Gplus, we recommended several defence measures that can be leveraged to increase the resilience of local models, including input validation, adversarial training, ensemble methods and moving target defense approach [43]]. In what follows, we extend the list of defences by advocating emerging technologies and approaches that can play a key role in improving the local models robustness as well as defeating the poisoning and privacy leakage risks against FL:

- **Blockchain:** The intrinsic features of decentralization and immutability characterising the Blockchain technology makes it a promising solution to overcome poisoning attacks against FL models [41]]. Indeed, blockchain can be leveraged to ensure the integrity of the local and global model updates to prevent their alteration during their exchange. Moreover, the smart contracts can be used to identify malicious workers by automatically evaluating the quality of local model updates against a validation dataset; only local models with high performance are considered in the aggregation process. Figure 5 illustrates the application of the smart contracts as proposed in [41]] to enable fully decentralized (i.e., without requiring a central parameter server) FL-based anomaly detection service which can withstand poisoning attacks. The smart contracts allow to assess the quality of model updates uploaded to the blockchain and automatically identify malicious workers involved in the learning process. It is worth mentioning that a key challenge facing the applicability of this approach is how to create and update the validation dataset.

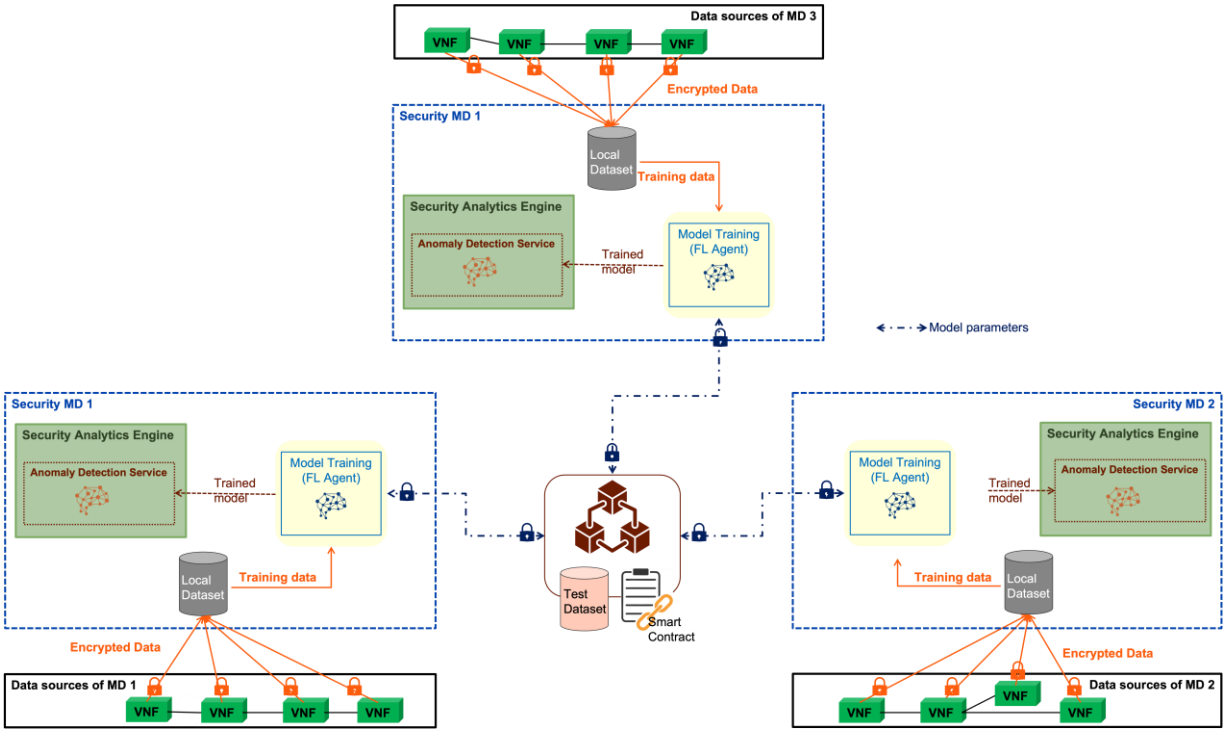

Figure 5: Blockchain-empowered Decentralized FL-based Anomaly Detection Service in INSPIRE-5Gplus Security Management Framework.

- **Trusted Execution Environments (TEEs)**: The confidentiality and integrity properties endowed with applications run and data saved inside TEEs make those environments

a potential enabler for empowering privacy-preserving ML models. Recent contributions have demonstrated the feasibility of using TEEs to guarantee the integrity of ML code and the privacy of the processed data by allowing the ML algorithm to execute over encrypted data. TEEs are also applicable to address the privacy leakage risk in FL, where the local and global models' codes and updates (i.e., model parameters) as well as the aggregation algorithm are saved and run inside the TEE [47]. Figure 6 illustrates an example of how TEE can be leveraged in INSPIRE-5Gplus framework to enable secure and privacy-preserving training of an ML-based anomaly detection service integrated in the security analytics engine. However, realizing TEE-empowered FL to protect against privacy attacks while taking into account the limited memory of TEEs and the additional computation overhead induced by encryption/decryption operations is an open challenge to solve.

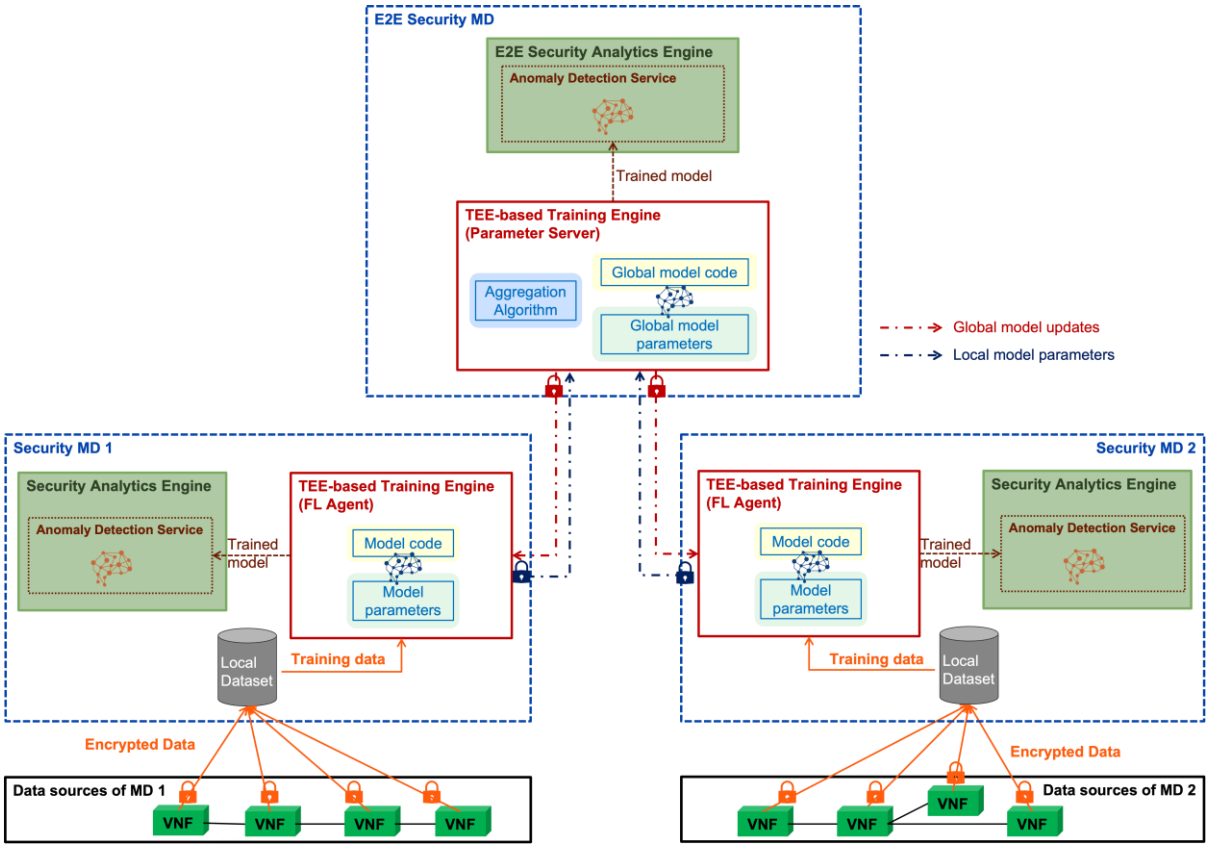

Figure 6: TEE-empowered FL-based Anomaly Detection Service in INSPIRE-5Gplus Security Management Framework.

3.4 Cyber Threat Intelligence (CTI)

3.4.1 Introduction

Cyber Threat Intelligence (CTI) is important in 5G mobile network security in two main areas: i) the sharing of cyber threat information between the different operational stakeholders; and ii) the use of open-source or commercial CTI to improve the detection, prevention and mitigation of cyberattacks. These are presented in the following subsections.

3.4.2 Challenges in CTI

3.4.2.1 Challenges in the sharing of CTI

The introduction of more software oriented and virtualised environments in 5G introduces new cyber threats that can impact the security of the network by allowing, for instance, tracking of users, deploying false base stations, compromising IoT devices to create botnets and perform DDoS attacks that disrupt the network services. On the other hand, 5G has introduced new security enablers to monitor and protect users and network communications. The protection mechanisms include more widespread use of encryption at both the user and control plane, AI/ML-assisted network security functions used to detect and prevent advanced threats, etc. Nevertheless, detecting zero-day attacks and reducing false positives continue to be challenging. This makes it necessary to continuously improve the security techniques used.

In a multi-tenant multi-operator environment, the situation becomes even more complex and introduces new challenges and requirements, in particular, to achieve end-to-end security across the different domains and equipment (e.g., UE, RAN, edge, IoT, core, verticals) and involving different operators. In this context, the sharing of threat intelligence is potentially of great value to improve the threat and risk awareness and help in the prevention of attacks. The sharing of CTI brings advantages along two main dimensions in such distributed and large-scale systems: 1) greater visibility in terms of security events going beyond the domain of a operator or tenant alone ("improved awareness"); and 2) better accuracy and efficiency for detection and protection due to richer and larger amounts of data for decision making ("improved intelligence"). Moreover, CTI sharing is essential for better security solutions since the relevance of any CTI data is not confined to a single system due to hyperconnectivity among 5G subsystems and elements.

One of the mayor bottlenecks that prevent the sharing of information are the privacy requirements and regulations (e.g., GDPR). Thus, filtering and anonymizing the shared information, in such a way that it remains actionable, remains a big challenge.

As defined by General Data Protection Regulation (GDPR), personal data is any information that allows identifying a data subject, i.e., that directly or indirectly allows identifying a person. In Article 4 of GDPR, a personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." GDPR also requires that data controllers and processors have robust data breach detection, investigation, and internal reporting procedures. Furthermore, data subjects need to be informed on any data breaches with the exception when the proper measures to protect the data are in place (e.g., using encryption, backups). But can operators share information with other organisations?

The authors of [10] stipulate that "There are several contexts in which CTI can be shared. It can be from a government to another government or to private entities; private entities sharing CTI with each other; or when private entities share CTI in their possession with the government". A cybersecurity framework has been defined in Europe to protect organisations against any liability that may result from CTI sharing intended for the protection of network and systems [10]] but certain rules need to be followed.

The EU Cybersecurity Act empowers ENISA to support information sharing in and between sectors, in particular concerning operators of essential services, by providing "best practices

and guidance on available tools and procedures, as well as on how to address regulatory issues related to information-sharing" [11]].

Furthermore, as indicated in ENISA's report [12]] "legislation such as the Network and Information Security (NIS) Directive and its national implementations require that critical infrastructure operators report cybersecurity incidents to the authorities and inform their peers through Information Sharing and Analysis Centres (ISACs)". It also recognises the need for CTI sharing, SIEM and SOAR platforms. Here, the certification program being implemented by ENISA [13]] will play an important role.

3.4.2.2 Challenges in CTI for detection, prevention and mitigation of cyberattacks

Threat intelligence involves awareness and information that can be used by organisations to protect their systems. In 5G, the organisations include all the stakeholders and particularly network operators, vertical application operators, and service providers. These organisations need to protect their networks, services and applications from attacks that impact their correct functioning or threaten the privacy and well-being of their customers.

Threat intelligence involves obtaining and analysing large amounts of data from many different sources that contain information on evolving threats that occur inside or outside of the organisations' networks to obtain alerts that can be acted on. As explained previously, the data and alerts can be shared among the stakeholders to better prevent the propagation of attacks.

5G mobile networks and beyond rely more than ever on the Internet. IP-based networks act as the common bearer for all 5G services. 5G has introduced many new security features that include: base station spoofing protection, capture and tracking of International Mobile Subscriber Identity (IMSI), advanced identity and access management, Transport-Layer Security (TLS), Extensible Authentication Protocol (EAP) supporting certificates and public key encryption, dedicated secure slices, etc.

However, the reliance on the Internet for the services and management actually increases the vulnerability and attack surface in 5G-based networks. This is also due to: the widespread deployment of not always secure IoT networks; the programmability of devices and components that can be more easily compromised; the complexity of a multi-provider multi-tenant ecosystem and supply chain; the promised high-throughput, high-density and low-latency; and, the interconnexion with and between clouds, IoT networks, databases and MEC. Already exploited threats include: DDoS attacks based on IoT networks; suspicions of backdoors in software components and connected devices; hacked endpoints such as autonomous cars; or, those carried out during the 5G Cyber Security Hack organised by Cisco, Ericsson, Nokia, PwC Finland and Aalto University [17]]: interception of a data session and extraction of sensitive data; network fuzzing to attack 5G components (using, for instance, 5Greplay [18]]), remote intrusion into an edge cloud data centre, deploying malicious network function.

CTI on ongoing attacks can greatly contribute in: identifying the compromised device's IP addresses; determine the paths of communication packets going from one IP to another or from one Autonomous System to another; and, identify initial stages of an attack (e.g., systematic or targeted scanning). Some examples of the type of data that can be used and the possible type of attacks that can be identified are: BGP announcements and Traceroute data to detect Internet routing attacks and provoked failures; Honeypots and Network

Telescopes (Darknets) to capture malicious activity such as malicious scans and botnet activity; and Open-Source Intelligence (OSINT) and commercial datasets to identify malicious hosts and determine the reputation of IPs and ASs.

Understanding and sharing information on the threat landscape is a big challenge and an important aspect for improved resiliency and response to cyber threats. Even though it is not always possible to detect Zero-day attacks, CTI can help prevent new attacks from propagating. The information needed includes: knowledge of motivations and activity of criminal/government groups, understanding cascading effects due to attacks, information on misbehaving roaming devices and bad hosts.

3.4.3 Use cases

3.4.3.1 Sharing of CTI

A typical example that shows the need for sharing of CTI concerns the roaming of IoT devices that are misbehaving. The home operator, that eventually has more knowledge for better detecting anomalies in the IoT network could inform the visited operator to take measures to mitigate any risks. Also, coordinated actions between the home and visited networks could be deemed necessary, and this requires sharing of information.

A popular platform that is being used for sharing CTI is the open-source MISP platform [14]] that allows sharing information and advice on the actions to be performed. To interoperate between operators or services, the STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated Exchange of Intelligence Information) standards [15]][16]] can be used to transmit information that includes the context of the attack or vulnerability, the indicators or features to detect the attack, the procedure to follow to prevent or mitigate the attack or vulnerability, the level of risk involved and the possible consequences, the profile of attackers, device and subscription identifiers, IP addresses, geolocation data, attack timestamps, attack duration, attack type, attack sources, and even code or network samples for further analysis. Thus, CTI sharing enables 5G systems that collect threat intelligence to structure and transmit this information in a standardized way to other operators (of networks or verticals) so that they can effectively take the appropriate actions.

3.4.3.2 Actionable CTI gathering and use

In the INSPIRE-5Gplus project, several techniques are being studied to obtain reliable CTI. First, Open-Source (OSINT, e.g., MITRE ATT&CK[2]) and commercial datasets (e.g., IBM X-Force Exchange[3], Cisco Talos[4]) are being used to provide information of malicious or compromised hosts and devices. A network of generic Open-Source honeypots is used to further provide more real-time up-to-date information on ongoing attacks, spams and illegitimate scans. Several different types of dedicated honeypots would complement this information, particularly to capture malicious IoT activity, 5G traffic and fake base stations. So called Network Telescopes or Darknets corresponding to un-allocated IP space can also be used to capture malicious activity related to machine-generated network activity called Internet

[2] https://attack.mitre.org/

[3] https://exchange.xforce.ibmcloud.com/

[4] https://talosintelligence.com/

background noise that can be generated by spamming, scans, worm activity, but sometimes corresponds to network control messages sent by error. To prevent exfiltration of data, and botnet command and control activity, the analysis of encrypted traffic is also needed and is being improved. This is based on behaviour analysis using machine learning techniques that allow differentiating normal and abnormal network traffic. Since the data obtained is from different sources and of heterogeneous nature, it is also necessary to aggregate and correlate this data to extract actionable information, giving rise to what can be called a Security Information Event Management (SIEM) system for 5G that considers communications from the OSI physical to the application layers. Due to the complexity and dynamicity of 5G infrastructures and services, this SIEM cannot rely on human based interventions to spot or remediate attacks as is the case of existing SIEM systems. It requires being able to automate practically all prevention and response activity.

Another aspect that is being considered is the routing of packets in the Web. Cyber-attacks also occur at this level. Cyber-attacks here disrupt the Internet routing (e.g., BGP poisoning, hijacking), attacks on naming system of the Internet (i.e., DNS attacks), as well as man-in-the-middle attacks that try to intercept TLS encrypted traffic utilizing attacks on X.509 certificates. Some of the datasets that can be used for detecting these have been mentioned before (e.g., BGP, traceroute).

Concerning the sharing of CTI, in the INSPIRE-5Gplus project we adopt different formalisms. First of all, the STIX standard allows a more standard exchange format that can be used by different stakeholders. On the other hand, more proprietary formats, based on Comma Separated Values (CSV) and JSON, offer better performance for the exchange of information between enablers deployed in 5G systems (e.g., Decision Engines, Security Analytics Engines, Intrusion Prevention Systems). These enablers can profit from the CTI to automate the protection of the network.

3.5 Moving Target Defense (MTD)

3.5.1 Introduction

Moving Target Defense is a defensive strategy that exploits the heterogeneity of the network by shifting the virtual resources in time and space, resulting in a proactive security tool that increases the difficulty for an attacker to perform reconnaissance and attack planning, as the intelligence gathered quickly becomes incorrect. MTD also provides a reactive security tool that can use the network changes to neutralize attacks or restore infected resources.

The automated network management system, integrating MTD [37]], has also to consider the security aspect in its strategic placement of network resources, including the prevention and the mitigation of network attacks at the various levels of the infrastructure:

1. at the networking level: this concerns network traffic and protocols, and includes attacks such as reconnaissance, man-in-the-middle (MitM), or denial of service (DoS);
2. at the virtualization level: this concerns the hypervisor's vulnerabilities and the isolation of VM-based or container-based network functions;
3. at the application level: this concerns software vulnerabilities and exploits.

MTD operations are mainly executed at the first two levels of the infrastructure: the networking and the virtualization level. The security of the third level, namely the application level, is under the responsibility of the VNF owner, i.e., the application vulnerabilities are

checked and patched by the developer (eventually using MTD) but out of the scope of CSP's network management systems. At the networking layer, MTD can change the traffic routes using SDN control, change virtual switches for diversity shuffles (e.g., change a Cisco virtual switch with an OpenvSwitch), and modify the network topology using NFV and proxy nodes. At the virtualization layer, virtual resources can be migrated to different cloud platforms (e.g., move a VNF from an Openstack Virtual Infrastructure Manager (VIM) to a VMWare or an Azure VIM), changing the virtualization stack on which network functions are running.

3.5.2 Challenges in the use of MTD

The strategic placement of network resources targets both performance optimization, efficiency, and security. Nevertheless, they do not always overlap, and conflicts might arise when performing such placements, favouring one objective to the detriment of the other. For instance, moving a resource to a closer node for latency optimization may be a poor choice security-wise, as an attacker can predict this. On the other hand, a purely random move for improved security can compromise the network performance. Hence, a critical research question is how to balance the three targets or favour one target over the other in particular circumstances based on the network state or predictions made. This problem requires advanced decision-making that can be achieved using AI and machine learning (ML).

The MTD techniques studied in the literature commonly focus on a singular aspect of the MTD and related security requirements. The integration and use of full-stack, full-spatiotemporal action space (e.g., VM live migration, OS diversification, hybrid diversity, shuffle, and redundancy actions) in virtualized infrastructure (multiple layers of the software stack) for inherent entropy maximization goal of MTD is still scarcely explored. Learning-based optimization of autonomous and proactive security is architecturally challenging due to the heterogeneity of services, infrastructure, and operational requirements. One major question is how to integrate MTD and AI/ML for protection of various strata in 6G as we formulate that new generation of wireless networks [39]].

The envisaged beyond 5G applications and thus requirements will pose formidable QoS and service level challenges. In that regard, Further Enhanced Mobile Broadband (*FeMBB)* expects extreme high data rates to serve beyond 5G verticals. However, such Tbps bitrates are incredibly challenging for traffic processing in security functions in the network. This complexity issue will challenge MTD solutions as well since they will incur additional overhead in terms of monitoring, event processing, and countermeasure enforcement. Therefore, how to design and implement distributed MTD solutions is an important research topic since traffic should be processed locally and on-the-fly at different points in the network. In the following Table 1 we summarize some of the important research questions and challenges that MTD poses:

Research Challenges	**Key Points**
Full-stack and full-spatiotemporal MTD action space	Exploit different virtualization layers to maximize MTD entropy
Security versus QoS Trade-off: Efficient MTD strategies	Strategic and minimalistic MTD combining proactive and reactive schemes, under the KPI formulation for Beyond 5G use cases

Extreme massive connectivity (e.g., umMTC)	Scalability
Secure and Robust AI	AI ethics and liability, AI unfairness, privacy, trustworthy data support and careful Reinforcement Learning (RL) modelling
Fundamental limits	Identification of security management capabilities attainable with MTD

Table 1: Research challenges of MTD

3.5.3 Use cases

3.5.3.1 Protection of NFVs and Slices

The protection of network slices, one of the fundamental building blocks of 5G, can be delivered by performing MTD operations on the NFV network resources, changing their setup in space and time. To this end, a proposed solution, the MTD controller (MOTDEC), is interfaced with the management system of the 5G network, such as the network slice manager and the NFV management and orchestration (NFV MANO) module, for the enforcement of MTD actions on network slices and their sub-components (network services and network virtualization functions, whether running as VMs or lightweight containers). MOTDEC receives MTD operations provided at runtime by a cognitive decision-making system, fitting in a closed-loop system that follows the ETSI ZSM specification. This results in an automated security management employing *monitoring, analysis, decision-making,* and *action-enforcement.*

MOTDEC is responsible for the execution of the various MTD actions that the framework will be providing. The MTD actions are grouped in 2 distinct categories:

- Soft MTD actions: these are SDN-based shuffle operations performed on network interfaces, traffic flow, and network topology on both the internal and the external/public views of the network. In the former view, MOTDEC could prevent an attacker inside the network slice from easily exploring and further penetrating it. In the latter view, the resource is meant to be always accessible by external devices with a public interface, and it provides a different public IP address to suspicious end-users or User Equipments (UEs), allowing further targeted analysis of their traffic and adding a second layer of security through proxy VNFs. To this scope MOTDEC integrates an SDN controller (i.e., ONOS) and creates a middle virtual network, called Topology Fuzzer, used to change the node links and network data flow, increasing the difficulty of identifying the network topology. Similar to the work presented by Islam et. al [40], MOTDEC assigns dynamic ephemeral IP addresses to the virtual nodes and redirects the packets to the protected resources with a softwarized address translation (NAT).
- Hard MTD actions: these are operations directly performed on the NFV assets used in the 5G infrastructure, for both assets allocated by the operator's clients and assets deployed by the operator to provide and manage their services. The MTD actions are: *1) MTD restart action*: here MOTDEC restarts the NSs or NFs by re-instantiating the resource starting from verified images. This mitigates security scenarios of attackers introducing themselves in the virtual units to eavesdrop and acquire sensitive data, to block the application running on the unit and resulting in a DoS attack, to encrypt the unit with ransomware, or to create a C&C bot and exploit it as a vector for other

chained attacks. The new instance of the service replaces the old one, expelling the intruder from the logic (and physical) resource.

- *2) MTD cloud diversity action:* in this case, MOTDEC moves the protected resource from a virtual infrastructure manager (VIM) to another one with a different cloud execution environment, e.g., from an OpenStack one to a VMware one. This changes the environment of the running resource and reduces the threats due to new specific system's vulnerabilities. In practice, this action is similar to the MTD restart action, but it creates a new instance of the resource in a different VIM than the old one, thus, it also solves the same threats addressed by the MTD restart action.

3.6 Distributed Ledger Technologies (DLT)

3.6.1 Introduction

DLTs are geographically (i.e., non-centralised) distributed databases in which all the nodes involved compose a peer-to-peer (p2p) network. Due to its non-centralization, any incoming data must pass a procedure called consensus mechanism in which the majority of the nodes must agree. The most common DLT is Blockchain. As its own name indicates, the data is saved in blocks and each block is linked (chain) to the previous one through the use of hash values. Among other parameters, each block is a composition of Blockchain transactions (i.e., an exchange of information between two peers). The data in a Blockchain can be trusted and considered as tamper-proof due to the fact that all the data are distributed (i.e., each peer has a copy of it) and so, it is almost impossible to modify anything without the majority of the p2p network nodes detecting it. Moreover, as the blocks are linked one to another, to modify a bock it becomes necessary to modify its linked blocks too, which is a very difficult and expensive processing action.

3.6.2 Challenges in the use of DLT

The main challenges that DLT is facing are due to the complexity and the greater resource utilization for the computation and storage purposes. The efficient integration of AI/ML with DLT have challenges in many types. Although, permissioned Blockchain ledgers can ensure data privacy by enabling encryption and allowing controlled access of the ledgers, it may limit the access and exposure of the large amount of data that can be necessary for AI to process and preform accurate and correct decision making and analytics. Having deterministic and static smart contracts may also cause challenges to incorporate AI/ML based decision makings with random outcomes. Current Blockchain relies on digital signatures which use public key encryption. It is envisaged that future quantum computing will have the ability to break public key encryption in which private keys can be determined. To solve this, it is envisioned that quantum-resistant mechanisms may render the underlying security of Blockchain breakable in future. Lack of standards may limit the interoperability and the adherence of DLT deployment in local and global level applications. For instance, in the context of AI applications and especially for public ledger transactions, policies should be carefully defined to assure the ethical rights of the communities.

Blockchain is currently being studied in multiple aspects around the communications networks management. For example, on optical networks, Blockchain is being studied as the element in charge to have a fair optical spectrum between Elastic Virtual Optical networks either in the edge and core domains. Other works, as similarly done in INSPIRE-5Gplus, aim to join Blockchain with Software Defined Networks (SDN) technologies by improving the security and

trustworthiness around the exchange of information between SDN controllers, the identification of evil nodes in the network or the enforcement of SLAs.

3.6.3 Use cases

3.6.3.1 Blockchain-based slice resource provision

DLT is a technology that brings a lot of opportunities in the control and management of network communications and their safety. Two examples in which the INSPIRE-5Gplus project is working are:

The **SFSBroker** enabler is a novel security enabler designed and developed for INSPIRE-5Gplus project. The "SFSBroker" leverages Smart Contracts of Blockchain technology to automatically provision slice resources in compliance with the SSLAs. It is an extension of the 5G network slice broker which is introduced as a new business model to allow dynamic interoperability and resource trading requirements of infrastructure providers, consumers, and mobile network operators in trading the network and computational resources. The network slice broker is running as a stand-alone third party blockchain service and communicates with the network slice/SSLA managers.

The **management of Network Slices** in the scope of INSPIRE-5Gplus is done through the WP4 enabler called "Trusted Blockchain-based Network Slices". This enabler aims to allow a set of Network Slice Managers (Slicers) to share their local domain resources with the other Slicers in order to create End-to-End Network Slices in a multi-domain scenario. By doing so, hierarchical architectures in multi-domain scenarios are avoided as no E2E manager is on top and so, there is no centralised point of failure blocking that could block E2E deployments. More information and experimental results can be found in [25]

3.7 Root-Cause Analysis (RCA)

3.7.1 Introduction

Root Cause Analysis (RCA) is a general term used in different domains, namely IT operations, telecommunications, manufacturing industry, medical diagnosis, and healthcare industry. RCA is defined as "a systematic process for identifying root causes of problems or events and for responding to them"[28]]. RCA plays a vital role in the Risk Management process which principally includes Vulnerability Scanning, Anomaly Detection, Root Cause Analysis, and Remediation. System administrators, and DevOps engineers use RCA not only for detecting the problems but also for understanding their causes to prevent their recurrence and/or mitigate their impact.

In the context of INSPIRE-5Gplus, we focus the analysis on Information and Communication Systems (ICS) to infer the root causes of problems by analysing the causal chains governing the system under monitoring using machine learning techniques.

3.7.2 Challenges in the use of RCA

In ICT-based systems, failures are recurrent. The system administrators, with experience in dealing with failures, can react more quickly and efficiently against their recurrence. The mitigation actions (e.g., reset a particular server every night) can be thus taken promptly. However, this human-based troubleshooting task becomes a lot more challenging, time consuming or even impossible in complex systems (e.g., virtualised multi-domain and multi-

provider 5G mobile networks). This is especially due to the fact that failures usually propagate in complex systems through causal chains and produce evolving fingerprints of noisy symptoms. This leads to the need of an automated tool helping humans to troubleshoot a system, regroup events that are causally connected, and keep unrelated events separated. Achieving this is often not straightforward, since components of a system can exhibit similar symptoms in two unrelated failures. Thus, the main challenge here is providing a tool for automating the RCA as much as possible. This can be done by using machine learning techniques that allow learning from identified past failures to determine if they are similar to new detected failures.

An RCA tool based on Machine Learning techniques needs to address several important issues. First of all, one must consider that the statistics and monitoring data that can be collected from the system has important impact on any tool's efficiency. This data consists of the learning dataset during the off-line knowledge acquisition phase and the data recuperated in real-time during the monitoring phase. RCA requires enough relevant monitoring data attributes and significant domain/system knowledge that can reflect the changes in the monitored system. For example, a system can exhibit similar symptoms in two unrelated failures. We need, thus, a higher level of granularity in the monitoring indicators and a deeper analysis to distinguish the two. Besides, in some specific systems, the data collection may not have the same frequency as other information used for the diagnosis (e.g., IoT battery-powered devices may have a low-activity mode to extend their operation autonomy, resulting that, in this mode, sensed data may not be synchronized). Therefore, RCA must be able to deal with out-of-order data and changed samplings.

Second, attribute selection (also known as feature selection [30]]) is one of the core concepts in Machine Learning that highly impacts model performance. For complex systems, it is common that the data collected is too complicated or redundant. In other words, there might be some irrelevant or less important attributes (i.e., noise) contributing less to the target variable. Removing the noise helps not only to improve the accuracy but also to reduce the training time. It is the first and most essential step that should be performed automatically using feature selection techniques, or manually by system experts.

Third, the data used as the input of RCA is normally heterogeneous. Data normalization step is needed for eliminating any disparities in units of measure and making the attributes comparable despite different value ranges. The way RCA normalizes data input is also an important efficiency factor.

Last but not least, a machine learning-based RCA approach relies on similarity learning to identify the most probable cause(s) of detected anomalies based on the knowledge of similar observed ones. The accuracy of the results depends on the algorithm used for calculating the similarity score. Thus, computing the similarity score based on more than one similarity and distance measure will help improve the confidence and precision of the results. During the training phase one needs to determine the measures that are used to compare the past states and new occurrences to find the highest similarity score. Besides, to avoid false positives, the similarity between a normal proper state and each known state involving anomalies or malicious activity should be as low as possible.

3.7.3 Use cases

3.7.3.1 Monitoring of 5G IoT Campus

Security monitoring of 5G IoT networks requires not only the detection of failures or degraded performance but also determining but also identifying the causes (e.g., intrusions, denial of services, compromised devices, etc. or just normal wear-and-tear) as a prerequisite for triggering corrective actions. For addressing this need, the use cases here involve meaning from experience to determine the most probable cause of any detected malfunctioning. The RCA machine learning approach developed in INSPIRE-5Gplus considers highly granular monitoring indicators (e.g., statistics and data extracted from the logs, metrics, network traffic, and any data that could identify the system state) and performs deep analysis to assess the similarity of a newly observed event reflecting the current system status and each past experience recorded in the historical database. This RCA enables systematizing the experience in dealing with incidents to build a historical database and verify whether a newly detected incident is similar enough to an observed one with known causes. Thanks to the suggestions provided by the RCA, remediation actions could be timely and wisely taken to prevent or mitigate the damage of reoccurring similar problems.

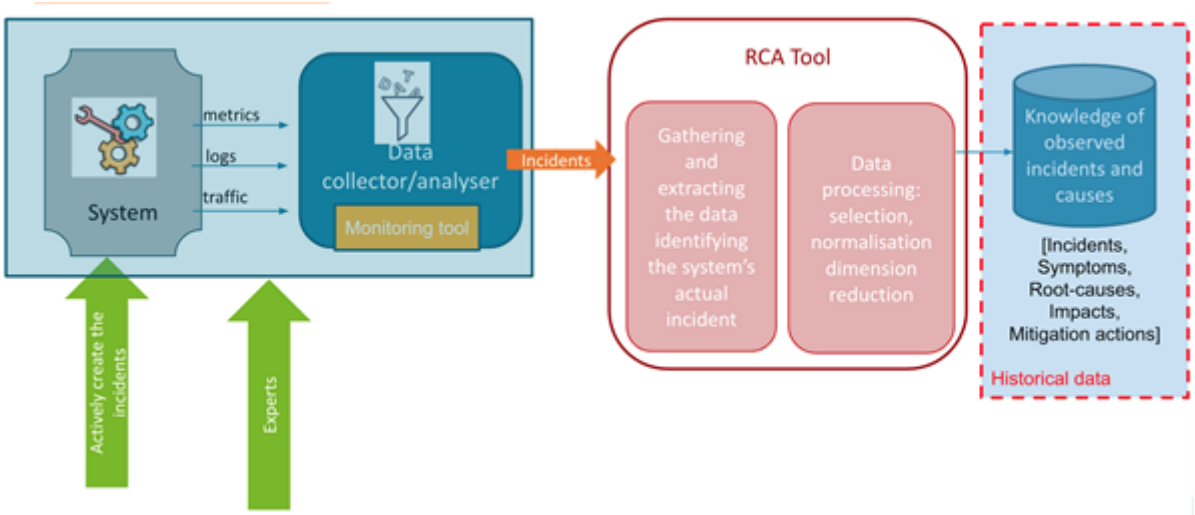

Figure 7: RCA - Knowledge acquisition phase

The RCA Enabler works following two phases: the knowledge acquisition phase (Figure 7) and the monitoring phase (Figure 8). The former is for building a historical database of known problems and incidents. The latter consists of monitoring the system in real-time, analyze the upcoming incident by querying the historical data, and suggesting possible root causes.

In the knowledge acquisition phase, the historical data is a set of data used for learning purposes. It consists of labelled records collected over time. These records describe the original cause of several incidents (e.g., a sensor is no longer permitted to send data to the central gateway) and the relative attribute values (e.g., downstream data bitrate measured in the central gateway decreased). The historical data is constructed by two means:

- Active learning: By actively performing different tests including the injection of known failures and attacks. In this case the collected data can be easily labelled since we deal with a controlled system.
- Passive learning: Once an incident is detected without knowing its origin, and thanks to the aid of system experts, classical RCA is performed by debugging different logs

and correlating various events to determine the corresponding root causes. The result of this task can be stored in the database with its relevant attributes values.

The historical data is derived from these two sources. The idea is to determine when the system reaches a known undesirable state with a known cause. It involves using the concept of Similarity Learning [29]], i.e., Ranking Similarity Learning. The RCA tool calculates the similarity of the new state with the known ones. It presents the most similar states in the relative similarity order. The final goal is to recognize the incident's root origin by using historical data. In this way, the tool can recommend to the operator which countermeasures to perform based on known mitigation strategies.

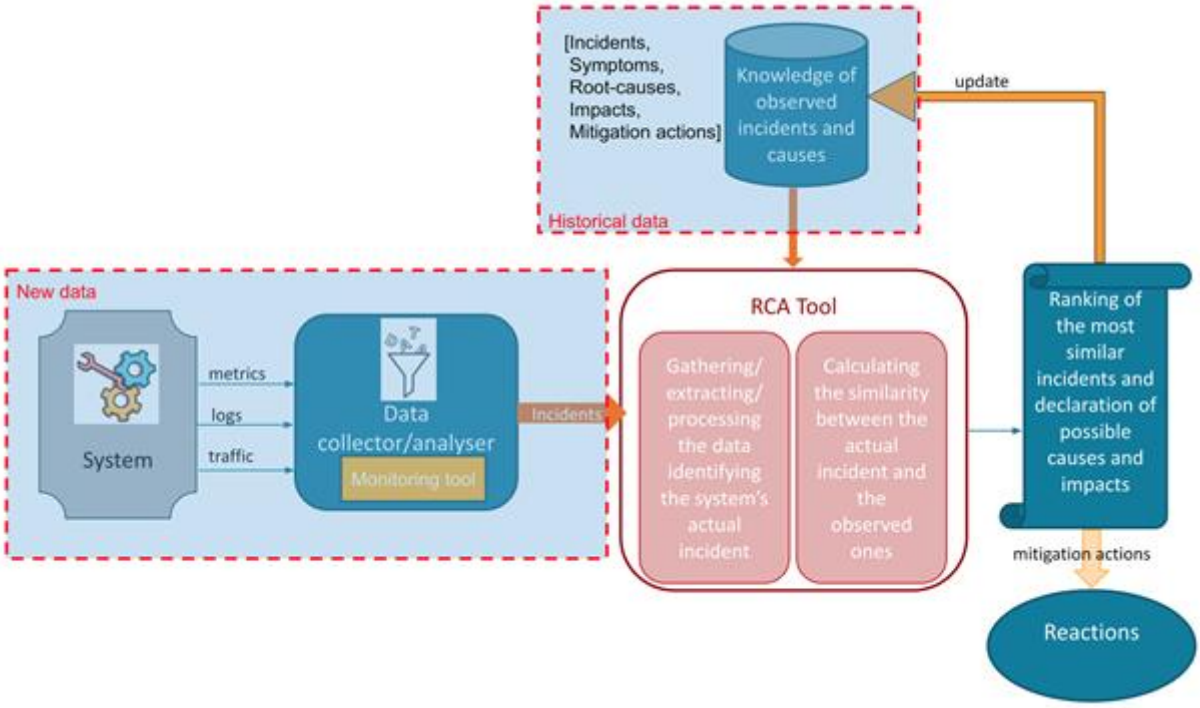

Figure 8: RCA - Monitoring phase

In the monitoring phase (Figure 8), the data is collected and transmitted to the RCA enabler in real-time. In theory, there is no restriction on the type of data to be gathered. On the contrary, a maximum of data for identifying the system functionalities is desirable. Some data could be redundant, so data processing steps are performed to extract the most pertinent data. It is worth noting that passive learning in the knowledge acquisition phase can be continuously run during the monitoring phase.

As 5G will allow IoT devices to communicate and share data faster than ever, the widespread adoption of IoT networks will rapidly grow with the deployment of 5G and beyond. In the context of INSPIRE-5Gplus, we are developing and testing RCA in a 5G-IoT use case. RCA will analyse the monitoring data collected from an IoT Industrial Campus connected to a Cloud via the 5G infrastructure and divine the potential root-causes of one or several incidents. RCA will notify the Orchestrator about detected anomalies and the sources possibly triggering them so that the correct reactions can be promptly triggered. RCA will assess all the challenges mentioned in the previous subsection, as well as apply advanced AI/ML techniques to improve the performance (e.g., accuracy, low latency, reliability).

3.8 Security Service Level Agreements (SSLA)

3.8.1 Introduction

Security has a non-negligible cost and various providers (operators or platform providers) have to differentiate security features on a vertical basis. Slice providers need to offer "tailored" security features, offered on-demand and as-a-service.

Security Service Level Agreements (SSLAs) possess a key role for slice security assessment, as they allow to declare clearly the security level granted by providers to verticals, as well as the constraints posed to both parties (slice providers and verticals).

A framework that allows a slice provider who acts as a broker relying on several Service Providers providing various network services to deliver slices controlled by Security SLAs to the verticals/end-users is needed. Each provided slice has to be covered by a Security SLA that specifies the security grants offered.

3.8.2 Challenges in the use of SSLA

The challenge is to provide an end-to-end management of the security requirements specified in SSLAs, during the full life-cycle of a Slice by: *a)* gathering the verticals/end-users security requirements; *b)* deploying the necessary security controls to enforce the agreed SSLA by enriching or configuring the services of the Service Providers (SPs) services; *c)* real-time assessment of RT-SSLAs using monitoring techniques to detect that the security functions are working as expected and that there are no security breaches; *d)* detecting violations in security provisioning level based on an analytic engine and notifying both end-users and SPs; and *e)* enabling the automation of reaction strategies in real-time to adapt the provided level of security or to trigger proper countermeasures. The most difficult stages are the dynamic selection of security controls that match the end-to-end SSLAs and the service providers platform and security constraints, and the continuous assessment to determine if the SSLAs are effectively respected so that the appropriate actions can be taken when they are violated. There is also a need to combine the SSLA with the security policies, establishing the hierarchy between them.

Most of the SSLA frameworks focus on the operation and negotiation phases of the lifecycle of SLAs, thus do not get into the specifics of what metrics need to be monitored and how it can be done. Complex systems like 5G or IoT, operate on data that are processed and stored in a distributed manner at multiple computing nodes. Therefore, addressing data availability or integrity in those systems by specifying certain techniques (for instance, the cryptographic techniques that should be used), as made possible by existing SSLA frameworks, is not enough. The main drawback is that they do not continuously monitor the preservation of specific properties in order to support the satisfaction of the specified SLAs at all times.

One of the biggest challenges of SSLA monitoring is the association of the high-level specification of the terms that need to be guaranteed into low level instructions that can facilitate the monitoring and assessment of the terms. For example, considering an SSLA whose SLOs are to guarantee the data availability, data privacy and data integrity of a system, it is crucial to deploy an enabler whose security capability is to monitor applications or network traffic in real-time. Indeed, there are different enablers that are capable of

performing security monitoring, such as MMT's Probe[5] or other Intrusion Detection Systems. As SSLAs and even HSPL/MSPL (high and medium level policy descriptions presented in Section 3.9 only provide what to monitor in general (e.g., protocol, port, IP address), they do not contain any specific technical details on how to detect any anomalies. Thus, we need to produce monitoring rules and algorithms corresponding to the specified SSLAs that allow specific monitoring tools to assess them in real-time. Here we refer to these rules and algorithms as RT-SSLAs.

3.8.3 Use cases

3.8.3.1 Dynamic selection based on SSLAs

Dynamic selection based on SSLAs provides a high-level of abstraction layer by using SSLAs which are independent to the underlying infrastructure, decoupling the security requirements of the specific implementations to deal with problems like heterogeneity and vendor-locking. This is especially useful in slicing environments where services including security must be adapted to available resources and constraints

In this regard, for each capability described in the SSLA file, it is calculated a list of enablers from the catalogue supporting all the metrics marked with a "HIGH" priority. Indeed, since the metrics can be associated with three different priority levels ("HIGH", "MEDIUM" or "LOW"), it seems logical to select only the enablers supporting all the metrics with the highest priority level. Nevertheless, we have chosen to classify the enablers according to the other supported metrics, favouring the greatest number of metrics with "MEDIUM" priority implemented, then the greatest number of metrics with "LOW" priority. The Figure shows the result of the selection before the enablers are sorted.

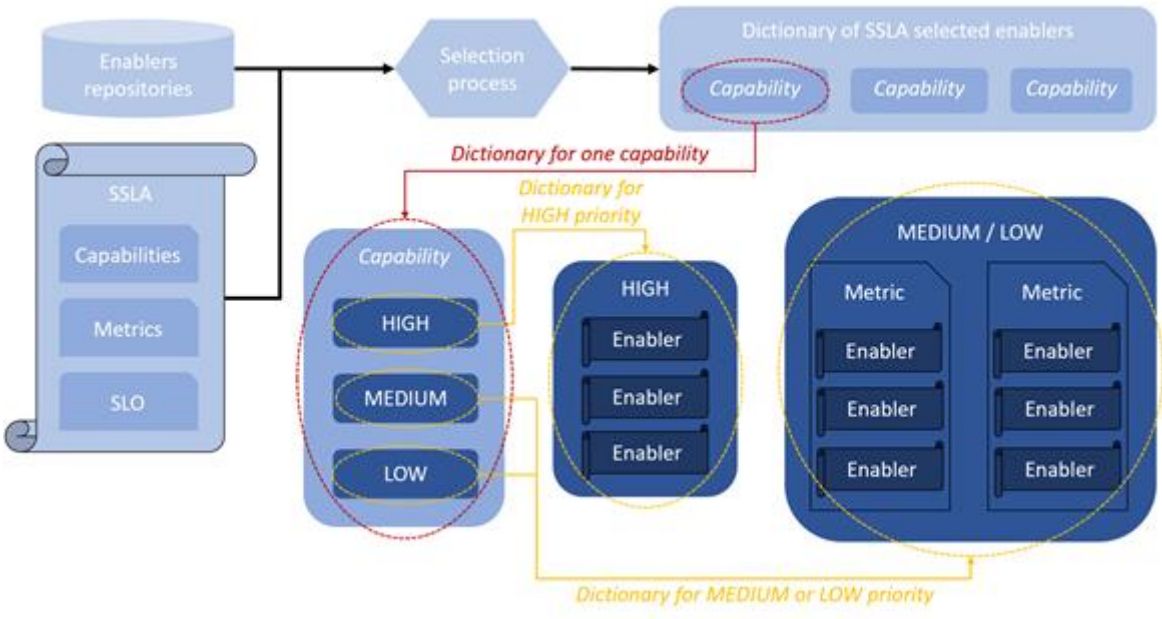

Figure 9: SSLA-based enabler selection process

[5] https://www.montimage.com/products that will be made available in open source: https://github.com/Montimage . Currently available: 5Greplay to modify and generate 5G network traffic, and MMT's GUI to visualize statistics and alarms.

Thus, this first selection remains effective, in the sense that only the enablers that comply correctly with the critical points are chosen without becoming too drastic and filtering only the enablers which implement all the metrics correctly, in which case it would not be obvious to always find it. Indeed, we want to avoid cases where the result of the selection would be an empty set of enablers.

In addition, we can notice here that only the capabilities (as defined by NIST) are considered. A more exhaustive work taking into account the security controls (as also defined by NIST) will have to be developed at the future using a new model.

3.8.3.2 Real-time SSLA assessment

Real-time monitoring of SSLAs (RT-SSLAs) and their continued assessment is of great added value for both end-users and service providers since it improves the trustworthiness of the services. RT-SSLAs can facilitate the ability to gain more insight concerning which system modules are responsible for any detected faults and problems, or the poor performance of a running component, as discussed previously in Root Cause Analysis (RCA) Section 3.7.

The aim is providing an automated SSLA-based monitoring framework that requires a minimum amount of input from the users. For this, in INSPIRE-5Gplus we have improved the security monitoring framework to focus on the runtime monitoring of security properties and continuously monitor dynamic complex services at runtime. Firstly, we automate the generation of the monitoring security rules on our framework from the specified set of high-level security specifications, such as SSLAs, or from different levels of security policies, such as HSPL/MSPL (presented in the following Section). Secondly, we automate the deployment of our framework to detect anomalies or attacks in real-time and consequently produce security reports that will be used by other enablers (e.g., Decision Engine) to perform the necessary actions. Finally, we modify our monitoring framework so that it can dynamically adapt to the runtime changes in the execution environment by enforcing, as quickly as possible, the configurations generated for the enforcement of new or modified network topologies and security policies.

We predefine RT-SSLA rule templates regarding the type of security policies (e.g., related to filtering, anomaly detection, IoT network behaviour). Then, we automatically generate rules by using key information extracted from HSPL/MSPL.

3.9 Policy Based Security

3.9.1 Introduction

The INSPIRE-5Gplus framework needs a language to automate the management of the resources and the security related to them. This language must be comprehensive by the Orchestrator of the system, and it must have a specification precise enough to not generate ambiguity. HSPL-OP [35]] and MSPL-OP [36]] are the languages that fulfil these requirements, they follow a concrete format covering all required aspects to interpret and configure all the security mechanisms offered by components, this format followed is called Security Policy. HSPL-OP and MSPL-OP are then Security Policy Languages, that specifies two levels of abstraction for defining security requirements that must be accomplished by specific assets for ensuring continuous system security. These policies will be transformed by a refinement process from HSPL-OP to MSPL-OP and this later by a translation process to specific configurations to be performed by arbitrary security assets. Security policies can be generated

in a proactive manner by the interpretation of the SSLAs, or in a reactive manner by system monitoring actions. During these processes conflict detection will be conducted in order to avoid system inconsistencies.

MSPL and HSPL Policy Languages, take advantage of several other standardized policy languages like Interface to Network Security Functions (I2NSF) [34]], but adding capabilities for representing specific security aspects on several security domains (e.g., filtering, traffic inspection, authorization or channel protection). MSPL and HSPL were extended, adding new models and capabilities, in addition to extending existing one to enhance the security policy languages with new features like IoT security capabilities or Network Slicing. MSPL and HSPL are also extended into HSPL-OP and MSPL-OP due to the need of using policy chains with priorities and dependencies.

3.9.2 Challenges in the use of Policy Based Security

Getting a conflict detection system smart enough to ensure the robustness of the system in real time, where monitoring the system to be able to extract the necessary data to detect conflicts is also a major challenge. Also, the security system must be flexible enough to be able to offer multiple and different alternatives to suit the current context or prediction. This needs to have multiple alternatives per capacity exponentially increases the complexity of both conflict detection and policy selection to deploy. In addition to all this, the use of the ZSM architecture with multiple domains proposes the challenge of coordinating, directing and validating actions of this abysmal complexity between different logical and/or physical spaces. Having to realise the aforementioned challenges in this scenario increases the possibilities of conflict and the need for flexibility in terms of options, thus making it more difficult to maintain the consistency and robustness of security operations.

The adoption of the ZSM approach makes the enforcement of security policies another of its main challenges, since there is now a delegation of security policies to other domains. The policy models collected from the state of the art must be extended to be able to manage multiple domains through the E2E Security Management Domain, the emergence of this higher domain makes new conflicts appear involving multiple domains where the decision to resolve them must be intelligent enough to know whether they should be resolved in the specific Security Management Domain or at the E2E level.

It should also be noted that until now, the security models developed were not fully oriented to security in 5G networks. Therefore, through this project, these models will evolve to cover the peculiarities of 5G networks and also propose flexibility mechanisms to ensure their extensibility to next generation networks.

3.9.3 Use cases

3.9.3.1 Flexible and scalable network management

SSLA & Policy Management will play an important role in the context of beyond 5G. As the 5G and its descendants will infuse industries and consumers, the overall connectivity fabric will evolve in a fuzzier agglomeration of domains and resources. For example, the next 3GPP release 17 oversee the adoption of a common core infrastructure supporting wireless and fixed access: Fixed Network Residential Gateway (FN-RG). It will allow ISPs to converge assets into a common pool of resources and allow for sharing common management functions (for example policy and subscriber databases). This convergence will be guaranteed that standard

SLAs are applied onto shared users and heterogeneous resources while using different access point from the conventional 5G RAN. In this future, the traditional ISP home fibre box could be replaced by a shared programmable box, controlled by a 5G core and enabling the users to seamlessly connect to various networks and also to provide a new pool of resources beyond the MEC frontier. The SSLAs and Policy Management enablement will set a common standard applied across all the domains while ensuring that the policy will ensure the correct integration of resources into the system.

To this aim, Policy Management will be aligned with the multi-level ZSM approach by using different abstraction policy levels, High-level Security Policy Language Orchestration Policies (HSPL-OP) for E2E Domain, and Medium-level Security Language Orchestration Policies (MSPL-OP) for end Management Domains. A conflict detection procedure is performed at each level. Assets in the scenario will be identified by its capabilities thus will be used for offering multiples alternatives to detected conflicts. A monitoring system will allow real-time transmission of information to E2E/end Management Domains to keep updated information of the current system status, thus maintaining the system information updated and enabling correct execution to solve dependencies. Policy Management decouples the complexity of hardware from management, allowing independent implementation of security assets, thus enabling the integration of current and further technologies into the system.

3.9.3.2 Secured Network Slice

Communications in 5G networks are designed to belong to different network slices tailored precisely to the service required. A clear example of this is vehicular communications, which is also expected to generate a significant amount of traffic and with critical needs to ensure both passenger safety and car cybersecurity. V2X communications will be hosted in a specific slice, where communication security is critical and given that the car components are likely to be quite restricted in terms of computing capacity, it is necessary to delegate the securing of the slice to the outside. It is therefore a key requirement to maintain the adaptability of the infrastructure to those of the vehicle that constrains them.

In this context, security policies play a fundamental role, as they ensure the necessary abstraction to be able to represent the security capabilities of the car and to coordinate, validate and adapt the infrastructure to be able to secure communications accordingly. Taking into account that each type of vehicle will have associated computational restrictions of different nature (eg. bicycles, motorcycles, cars...) the security based on policies allows to guarantee the most adequate option depending on these restrictions and guaranteeing the highest security for each type of communication and that the infrastructure can also offer it.

4 Conclusions and Future Trends

ZSM is with no doubt a key requisite to deal with the complexity of 5G and beyond networks and achieve full automation. However, as identified in this white paper, different privacy and security concerns need to be addressed to take full benefits of zero-touch management. While we identified Federated Learning as a potential solution to tackle the privacy issue stemming from collaboration between multiple management closed loops, we highlighted the new threat vectors introduced by federated learning and suggested a set of emerging technologies that can be leveraged to empower robust and privacy-preserving collaborative zero-touch management. In the regard of managing 5G ecosystem involving multiple actors, domains and slices, Security Service Level Agreements (SSLAs) play a key role for establishing negotiated security specifications that allow end-to-end management and enforcement of the security requirements. These can define what security services need to be deployed, how they need to be configured, and how they can be assessed during operation to be able to act when they are violated. For this SSLAs to be deployed in the system, policy-based orchestration is a key enabler for grating autonomous and flexible reaction on the system, as policies add the required abstraction to communicate with different enablers and devices and allowing to express large number of capabilities to be deployed with different level of granularity as required. Policies can be evolved easily in a modularized way, but this evolution is closely related with its integration with final assets and devices in which the capability will be granted. Not only the policies must be flexible, but defence methods too, the Moving Target Defense (MTD) is a promising method to enhance the security of future telecommunication networks leveraging their virtualization, service-based architecture and software-defined properties. Efficient MTD strategies can be learned using deep Reinforcement Learning, finding optimized trade-offs between agreed security levels and service performance needs. This paper presents MTD in an NFV network, the identified challenges in its deployment and usage, and, in particular the work done in the scope of the INSPIRE-5Gplus project. Once a malicious activity is detected, understanding the causes and effects is of primordial importance to operators for the effective and automated mitigation to attacks. In this regard, Root Cause Analysis (RCA) is vital for the Risk Management process. In INSPIRE-5Gplus, RCA is considered an integral part of the Trust and Liability management framework that offers the possibility of identifying responsibilities when a problem occurs, but also making it possible to react to maintain the required security and trust of the provided services.

The reliance of 5G on the Internet introduces all the vulnerabilities of the Web but also new ones, such as fake base stations and mobile tracking. Cyber Threat Information (CTI) can help improve the awareness and understanding of the threat landscape and automate the protection of networks from ongoing attack campaigns. As explained in Section 3.4, the main challenges that need to be addressed, and that are being addressed by the INSPIRE-5Gplus project, are: the sharing of CTI among stakeholders that can be facilitated by the adoption of standard exchange formats (e.g., STIX); the aggregation and analysis of CTI data from many different sources that requires the use of Machine Learning techniques; and the automation of the use of CTI to stop or prevent cyber-attacks that requires optimized exchange of information between different security enablers deployed in the 5G systems. Regarding trustworthiness of data, DLT seems to be one of the more interesting technologies to be use on both the management and security of network resources. This paper illustrated two examples being designed within the scope of the INSPIRE-5Gplus project, but many other utilities and use cases are being planned and will be planned in order to make networking as transparent and trustworthy as possible.

References

[1] GEANT. “https://tools.geant.org/”.

[2] Espanix. “https://www.espanix.net/es/index.html”.

[3] ENISA. “https://www.enisa.europa.eu/”.

[4] ENISA, 2021. ENISA Threat Landscape Report 2021: April 2020 to mid-July 2021. ENISA.

[5] ENISA, 2020. ENISA Threat Landscape for 5G Networks Report. ENISA.

[6] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä and I. Ahmad, "Machine Learning Threatens 5G Security," in IEEE Access, vol. 8, pp. 190822-190842, 2020, doi: 10.1109/ACCESS.2020.3031966.

[7] M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," in IEEE Access, vol. 8, pp. 114066-114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[8] Positive Technologies, December 2020. 5G Standalone core security research. Positive Technologies.

[9] L. O. Nweke and S. Wolthusen, "Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection," 2020 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 63-78, doi: 10.23919/CyCon49761.2020.9131721.

[10] Nolan, A.: Cybersecurity and information sharing: Legal challenges and solutions. Tech. rep., Congressional Research Service - Informing the legislative debate since 1914 (2015)

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union: http://data.europa.eu/eli/dir/2016/1148/oj

[12] https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

[13] https://www.enisa.europa.eu/topics/standards/certification

[14] https://www.misp-project.org/

[15] https://stixproject.github.io/ and https://taxiiproject.github.io/

[16] https://github.com/MISP/MISP-Taxii-Server

[17] https://app.hackjunction.com/events/5g-cyberhack

[18] https://5Greplay.org

[19] B. Al-Musawi, P. Branch and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 377-396, Firstquarter 2017, doi: 10.1109/COMST.2016.2622240.

[20] Fontugne, Romain & Aben, Emile & Pelsser, Cristel & Bush, Randy. Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements. May 2016, arXiv:1605.04784

[21] Nawrocki, M., Wahlisch, M., Schmidt, T.C., et al. 2016, arXiv:1608.06249

[22] E. Bou-Harb, "A probabilistic model to preprocess darknet data for cyber threat intelligence generation," *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1-6, doi: 10.1109/ICC.2016.7510881.

[23] https://github.com/hslatman/awesome-threat-intelligence

[24] Odnan Ref Sanchez, Simone Ferlin, Cristel Pelsser, Randy Bush: Comparing Machine Learning

Algorithms for BGP Anomaly Detection using Graph Features. Big-DAMA@CoNEXT 2019: 35-41

[25] P.Alemany, R.Vilalta, R.Muñoz, R.Casellas, R.Martínez, Peer-to-Peer Blockchain-based NFV Service Platform for End-to-End NetworkSlice Orchestration Across Multiple NFVI Domains , in Proceeding sof the 2020 IEEE 3rd 5G World Forum (5GWF'20), 10-12 September2020, virtual event.

[26] P.Alemany, R.Vilalta, R.Muñoz, R.Martínez, R.Casellas, Managing Network Slicing Resources Using Blockchain in a Multi-Domain Soft-ware Defined Optical Network Scenario , in Proceedings of European Conference on Optical Communications (ECOC 2020), 6-10 December2020, virtual event.

[27] P.Alemany, R.Vilalta, R.Muñoz, R.Casellas, R.Martínez, End-to-End Network Slice Stitching using Blockchain-based Peer-to-Peer Net-work Slice Managers and Transport SDN Controllers , in Proceedings of The Optical Networking and Communication Conference & Exhibition(OFC), 6-11 June 2021, virtual event.

[28] M. A. Latino, R. J. Latino, and K. C. Latino, Root cause analysis: improving performance for bottom-line results. CRC press, 2019.

[29] Marcello Pelillo, Similarity-Based Pattern Analysis and Recognition, Springer, 2013, isbn: 978-1-4471-5628-4.

[30] Richard Lowry, Concepts and Applications of Inferential Statistics, Vassar College, 2008

[31] https://www.inspire-5gplus.eu/public-deliverables/

[32] Intel Total Memory Encryption: https://www.intel.com/content/www/us/en/architecture-and-technology/total-memory-encryption-security-paper.html

[33] SGX extended EPC size: Intel Total Memory Encryption: https://www.intel.com/content/www/us/en/architecture-and-technology/total-memory-encryption-security-paper.htmlHit enter here to create a further reference

[34] L. Xia, J. Strassner, C. Basile, and D. Lopez, "Information Model of NSFs Capabilities," IETF, Internet-Draft draft-ietf-i2nsf-capability-00, 2017, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-i2nsf-capability-0

[35] F. Valenza, T. Su, S. Spinoso, A. Lioy, R. Sisto, and M. Vallini, "A formal approach for network security policy validation," JoWUA, vol. 8, pp. 79–100, 2017.

[36] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "Security policy enforcement for networked smart objects," Computer Networks, vol. 108, pp. 133 – 147, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128616302663

[37] W. Soussi, M. Christopoulou, G. Xilouris, and G. Gür, "Moving target defense as a proactive defense element for beyond 5G,"IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 72–79, 2021.

[38] Cho Jin-Hee et al, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense." ArXiv abs/1909.08092, 2019.

[39] Christopoulou, M., Soussi, W., Xilouris, G., Gür, G., Montes de Oca, E., Koumaras, H., & Stiller, B. (2021). AI-enabled slice protection exploiting moving target defense in 6G networks. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), virtual, 8-11 June 2021*.

[40] M. Islam and E. Al-Shaer, "Active deception framework: An extensible development environment for adaptive cyber deception," in 2020 IEEE Secure Development (SecDev), 2020, pp. 41–48.

[41] O. Hireche, C. Benzaid, and T. Taleb. Deep Data Plane Programming and AI for Zero Trust Self-Driven Networking in Beyond 5G. In Computer Networks, Vol. 203, Feb. 2022.

[42] 3GPP TR 23.700-91 v17.0.0. Study on Enablers for Network Automation for the 5G System (5GS);

Phase 2 (Release 17). Dec. 2020.

[43] C. Benzaid and T. Taleb. AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" in IEEE Network Magazine, Vol. 34, No. 6, pp. 140 – 147, Nov. 2020.

[44] J. Zhang, Z. Qu, C. Chen, H. Wang, Y. Zhan, B. Ye, S. Guo. Edge Learning: The Enabling Technology for Distributed Big Data Analytics in the Edge. ACM Computing Surveys, Vol. 54, No 7, Article 151, June 2021.

[45] Z. Wang et al. Beyond Inferring Class Representatives: User-level Privacy Leakage from Federated Learning. In Proc. of IEEE Conference on Computer Communications (INFOCOM), Apr./May 2019.

[46] B. Hitaj, G. Ateniese, F. Perez-Cruz. Deep Models under the GAN: Information Leakage from Collaborative Deep Learning. In Proc. of the 2017 ACM SIGSAC Conference on Computer and Communication Security, pp. 603 – 618, Oct. 2017.

[47] Y. Chen, F. Luo, T. Li, T. Xiang, Z. Liu, and J. Li. A Training-Integrity Privacy-Preserving Federated Learning Scheme with Trusted Execution Environment. Information Sciences, Vol. 522, pp. 69 – 79, June 2020.

[48] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis. PPFL: Privacy-Preserving Federated Learning with Trusted Execution Environments. In Proc. of the 19th Annual International Conference on Mobile Systems, Applications, and Services, pp. 94 – 108, June 2021.

[49] Dutta, L., & Bharali, S. (2021). TinyML Meets IoT: A Comprehensive Survey. Internet of Things, 16, 100461.

[50] H. X. Nguyen, R. Trestian, D. To and M. Tatipamula, "Digital Twin for 5G and Beyond," in IEEE Communications Magazine, vol. 59, no. 2, pp. 10-15, February 2021, doi: 10.1109/MCOM.001.2000343.

[51] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor,Q. Wu, M. Boucadair, and C. Jacquenet, "DigitalTwin Network: Concepts and Reference Architecture,"IETF, Internet-Draftdraft-zhou-nmrg-digitaltwin-network-concepts-05, Oct. 2021, (Accessed on Nov. 22,2021). [Online]. Available: https://datatracker.ietf.org/doc/html/draft-zhou-nmrg-digitaltwin-network-concepts-05

[52] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," in IEEE Network Magazine, Vol. 34, No. 3, Jun. 2020, pp. 124 - 133.

[53] ETSI GS ZSM 009-1 V1.1.1. Closed-Loop Automation; Part 1: Enablers. June, 2021

[54] 3GPP TS 28.535 V17.4.0. Management and Orchestration; Management Services for Communication Service Assurance; Requirements (Release 17). Dec. 2021.

[55] ETSI GS ZSM 002, "Zero-touch network and Service Management (ZSM); Reference Architecture," Aug. 2019

[56] Nurit Sprecher, "Major stride in enabling a broad variety of new premium services at scale and innovative business models", "https://www.etsi.org/newsroom/blogs", July 2021

[57] ETSI GS ZSM 003, "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing", July 2021.

[58] FP7 Project: https://cordis.europa.eu/project/id/610795

[59] https://www.nist.gov/cyberframework

