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

INSPIRE-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond

D3.1: 5G security assets baseline and advancements

Version: v0.7

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2021
Submission date	11/05/2021
Lead editor	Vincent Lefebvre (Tages)
Authors	Dhouha Ayed, Geoffroy Chollon, Nicolas Peiffer, Cyril Dangerville (TSG); Anastasios Kafchitsas, Sabina Sandia, Orestis Mavropoulos (CLS); Anastasios Kourtis, George Xilouris, Maria Christopoulou (NCSRD); Edgardo Montes de Oca, Huu Nghia Nguyen (MI); Antonio Pastor, Sonia Fernandez, Diego Lopez (TID); Vincent Lefebvre (TAGES); Chafika Benzaid, Tarik Taleb, Othmane Hireche, Yongchao Dang (AALTO); Pol Alemany, Charalampos Kalalas, Ricard Vilalta, Raul Muñoz (CTTC); Gürkan Gür, Bernhard Tellenbach (ZHAW); Jordi Ortiz, Rodrigo Asensio (UMU); Pawani Poranbage (OULU),
Reviewers	Maria Christopoulou (NCSRD), Jorge Bernal Bernabe (UMU)
Work package, Task	WP 3, T3.1
Keywords	Security enablers, smart and adaptive security

Abstract

This deliverable describes all enablers defined by the consortium that were either fully developed or advanced in the course of this project and which are relevant to the INSPIRE-5Gplus smart and adaptive security tenet. The enabler descriptions are ordered inside five main functional building blocks, hence regrouped by functional proximity. The enabler descriptions follow one unique and recurring template for the sake of easing the reading and coherence.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	06/11/2020	Initial document created with MS3 content	V. Lefebvre (TAGES)
v0.2	01/02/2021	Work on the introduction and enabler description	D. Ayeb (TSG), V. Lefebvre (TAGES), C. Benzaid (AALTO)
v0.3	16/03/2021	Finalization of the ToC with new chapters introducing each main functional blocks. Rewriting of the introduction based on last progress on the HLA definition. Merging, removal and add of enablers.	V. Lefebvre (TAGES); D. Ayed, G. Chollon, N. Peiffer, C. Dangerville (TSG); A. Kafchitsas, S. Sandia, O. Mavropoulos (CLS); A. Kourtis, G. Xilouris, M. Christopoulou (NCSRD); E. Montes de Oca, H. Nghia Nguyen (MI); A. Pastor, S. Fernandez, D. Lopez (TID); C. Benzaid, T. Taleb, O. Hireche, Y. Dang (AALTO); P. Alemany, C. Kalalas F. Mira, R. Vilalta, R. Muñoz (CTTC); G. Gür, B. Tellenbach (ZHAW); J. Ortiz, R. Asensio (UMU); P. Poranbage (OULU)
v0.4	16/04/2021	Reviewer version first edition	J. Bernal (UMU), V. Lefebvre (TAGES)
v0.5	27/04/2021	Reviewer final edition	M. Christopoulou (NCSRD), V. Lefebvre (TAGES)
v0.6	29/04/2021	Modifications resulting from the internal reviews	All above listed authors
v0.7	03/05/2021	Final editing	A. Köhler (EURES)

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1 Introduction	TAGES, TSG
Section 2 AI/ML for smart security	TAGES, TSG, ZHAW, MI, AALTO, CTTC, TSG
Section 3 E2E ZTM	TAGES, TSG, AALTO, TSG, CLS, CTTC, NCSRD,UOULU
Section 4 Security enforcement	TAGES, TSG, UMU, TID, CTTC, AALTO
Section 5 Security analytics	TAGES, TSG, NCSRD, MI,
Section 6 Security data collection	TAGES, TSG, TID
Section 7 Enabler to security gap	TAGES, TSG, AALTO, MI, CLS, UOULU, NCSRD, CTTC, MI, TID

Disclaimer

This report contains material which is the copyright of certain INSPIRE-5Gplus Consortium Parties and may not be reproduced or copied without permission.

All INSPIRE-5Gplus Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License[1].

Neither the INSPIRE-5Gplus Consortium Parties nor the European Commission warrant that the information contained in the Deliverable is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

Acknowledgment

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

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

Executive Summary

This deliverable describes all enablers in the context of delivering Smart/Adaptive/Flexible 5G security as sought by INSPIRE-5Gplus, owned by consortium members and either fully developed or upgraded in the course of the project. It has been constructed in the sake of delivering structured, coherent, well ordered descriptions as well as highlighting how these enablers interact and bring a progress with regards to the project identified security gaps (recalled in this document).

The enabler descriptions are grouped in five project advancement categories defined as AI-ML for smart security, E2E Zero Touch Security Management, Security Enforcement and Control, Security Analytics and Data Collection. These categories group enablers and their developers by technological proximity and cover altogether the security gaps identified as part of prior work in this project (and recalled in this document). Each category is in fact a section of this document.

We begin this document with a general introduction recalling the main tenet of our work, introducing the typical closed-loop mechanism that controls and propagate the context-adaptive and measured-controlled security. This introduction also recalls the main categories as stated above and their interactions inside the closed-loop. Each Section includes an introduction on the relative positioning and interactions between the enablers that fall under one category.

Inside a section, the enabler description follows one unique and recurring template for the sake of easing the reading and coherence. The template includes the enabler problem statement and challenges, the State of the Art, the enabler description and it’s positioning inside the INSPIRE-5Gplus High Level Architecture, the unique architectural reference for this project. Each section starts with an introduction which depicts the relative positioning of the covered enablers between them.

The document concludes by mapping each enabler with the previously identified security gaps and addressing how the enablers bring a progress in that direction.

Table of Contents

List of Figures

List of Tables

Terminology and Abbreviations

Terminology

For removing ambiguity on the meaning of these frequently used terms in this document, the following clarifications are given.

Security Asset	A security asset is any component that supports security related activities (protection, detection and/or mitigation). In this report it generally represents existing software or virtualized functions from research prior to INSPIRE-5Gplus.
Security enabler	INSPIRE-5Gplus Security Enablers are the major building blocks to achieve a fully automated End-to-End security management in multi-domain 5G environments. They are the security features, products or services developed within the project. These enablers can leverage on one or more security assets, their configuration and logic of operation to empower security as a service paradigm.

Abbreviations

5GC	5G Core
AMF	Access control and Mobility Management Function
AUSF	Authentication Server Function
BTB	Branch Target Buffer
CU	Central Unit
DU	Distributed Unit
DVB	Digital Video Broadcast
E2E	End-To-End
EC	European Commission
eCPRI	evolved Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
GDPR	General Data Privacy Regulation
gNB	Next Generation Node B
HOA	Higher Order Ambisonics
JSON	JavaScript Object Notation
L1	First level of Cache
LLC	Last Level of Cache
mMTC	massive Machine Type Communications
KVM	kernel-Virtual Machines

MANO	Management and Network Orchestration
MEC	Multi-Access Edge Cloud
mMTC	massive Machine Type Communications
NF	Network Function
NFV	Network Function Virtualisation
NR	New Radio
NRF	Network Function Repository Function
NS	Network Service
NSA	Non-stand Alone
NSSF	Network Slice Selection function
OS	Operating System
PCF	Policy Control Function
PNF	Physical Network Function
REST	Representational State Transfer
RRH	Remote Radio Head
RRU	Remote Radio Unit
SA	Stand Alone
SBA	Service-Based Architecture
SDN	Software Defined Networking
SGX	Software Guard Extension (Intel's TEE technology)
TLB	Translation Lookaside Buffer
UDM	Unified Data Management
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
VNF	Virtual Network Function
VSF	Virtual Security Function
ZSM	Zero-touch network and Service Management

Informative references

In this document, many references to the following documents issued by INSPIRE-5Gplus are made:

D2.1 Delivered at M6

This initial and collectively produced Deliverable defines the initial security landscape of 5G networks, as well as the evolution of requirements and trends in 5G security. Security threats, security requirements, standards and the collaborative research projects are analysed. The document concludes with deemed actual security limitations and gaps regrouped in paragraph its 5.7, always referred by the present document. This document can be accessed at [111].

D2.2 Delivered at M18 (concurrently with this Deliverable D3.1)

This Deliverable introduces the enablements that vertebrate current and future security assets and architectures in present 5G and beyond. Based on these technologies and the enablers introduced, a set of initial Use Cases at platform and vertical level contextualise and demonstrate the usage of the security enablements as well as of the trust and liability mechanisms.

1 Introduction

The 5G architectural landscape is based on the disruptive concepts and technologies of Softwarization, Virtualization, and Cloudification. While these innovative technologies introduce new risks to 5G networks, security management should align with these paradigms, exploiting their flexibility and scalability benefits while ensuring consistency with the deployed system's architecture. The introduced benefits of these technologies are summarized below:

- Virtualization of the security functions includes a large diversity of capabilities ranging from classical firewalls to early detection and response systems with potentially sophisticated intelligent protection and detection;
- the Softwarization of these functions allows their orchestration and chaining at various levels and consequently their dynamic composition;
- Cloudification allows security to follow the cloud “As a Service” paradigm in order to reach the required scalability of security applications and align to the best Threat Intelligence updates regarding emerging vulnerabilities and attacks.

Softwarization, virtualization, and cloudification allow the intelligent orchestration of security functions across various domains utilizing AI & ML in order to achieve zero-touch automation. This deliverable describes such implementations and provides State-of-the-Art information to support this approach by detailing the results of INSPIRE 5G+ WP3/T3.1 “Smart 5G security assets” related to the period from M4 to M18.

The objective of Work Package 3 is to leverage on 5G security achievements to date to progress most promising ones, such as the usage of Software Defined Security models and techniques to increase the level of automation, while making them smarter by advancing 5G drivers and the way they are used to render security. Investigating AI-based models and techniques is considered as the most significant advancement driver for 5G security in this WP.

The work done in Task 3.1 for the M4-18 period is focused on the analysis of 5G security assets, requirements, use cases, and evolutions identified in WP2, as well as the test cases of WP5 in order to select the useful and promising existing assets for WP3 and plan their advancements in each of the WP3 tasks: Task3.2 focusing on leveraging Software Defined Security, Task 3.3 focusing on advancements related to Artificial Intelligence and Machine Learning, and Task 3.4 related to ZSM Security Management. Planned advancements look for extending the existing selected assets or defining new enablers.

Based on this analysis, and more specifically the gap analysis that was delivered in D2.1 (see brief info on D2.1 on the previous page), five categories for 5G advancement were identified to be covered in WP3:

1. *AI & ML* explores Artificial Intelligence and Machine Learning techniques for advancing 5G security.
2. *ZSM (Zero touch network & Service Management)* focuses on the automation of E2E security management and slicing based on Software-Defined Security and SECaaS paradigms.
3. *Security enforcement & control* is related to the previous category; it leverages Software-Defined Security to enforce security policies and SSLAs (Security Service Level Agreements) that are needed to be managed in a flexible, optimal and autonomous way.
4. *Security Analytics* explores the usage of data analytics and efficient AI and ML driven mechanisms for detecting threats in 5G networks, based on data generated from network elements and heterogeneous probes distributed across the 5G infrastructure (RAN, CN, TN, Edge).
5. *Security data collection* is important to the *Security Analytics* category, as it also explores Machine Learning relevant techniques for data collection.

INSPIRE-5Gplus has formulated its High-Level Architecture (HLA) described in D2.1, based on identified requirements stemming from the Project's Use Cases and ETSI ZSM reference architecture. The HLA is composed of a set of functional blocks both at Domain level (i.e., RAN, CN, TN, Edge domains) and E2E level that ultimately form a closed-loop mechanism when enforcing policies.

Figure 1 depicts how the building blocks of the INSPIRE-5Gplus High-Level Architecture (HLA) falls into the five categories or functional blocks described above, marked in blue colour.

- The ***AI and ML* category** includes the E2E and Domain Decision Engine building blocks, as well as the various security intelligence enablers.
- The ***ZSM for security management*** category englobes security policies, orchestration, SSLAs, and secure slicing management (included in service management building block).
- The ***Enforcement and Control*** category represents the security enablers that can be dynamically deployed or configured by the Security Orchestrator to enforce security policies by supporting 5G infrastructure with Network Security Functions, designed using Network Function Virtualization (NFV) and Software Defined Networks (SDN) paradigms.
- The ***Security Analytics*** includes enablers that aggregate information from the data collection process and trigger decisions and alerts by analysing big amounts of collected data and detecting anomalies in order to reduce cyber resilience KPIs.
- The ***Security Data Collection*** category relates to data management (generation, processing, etc.) and security related information

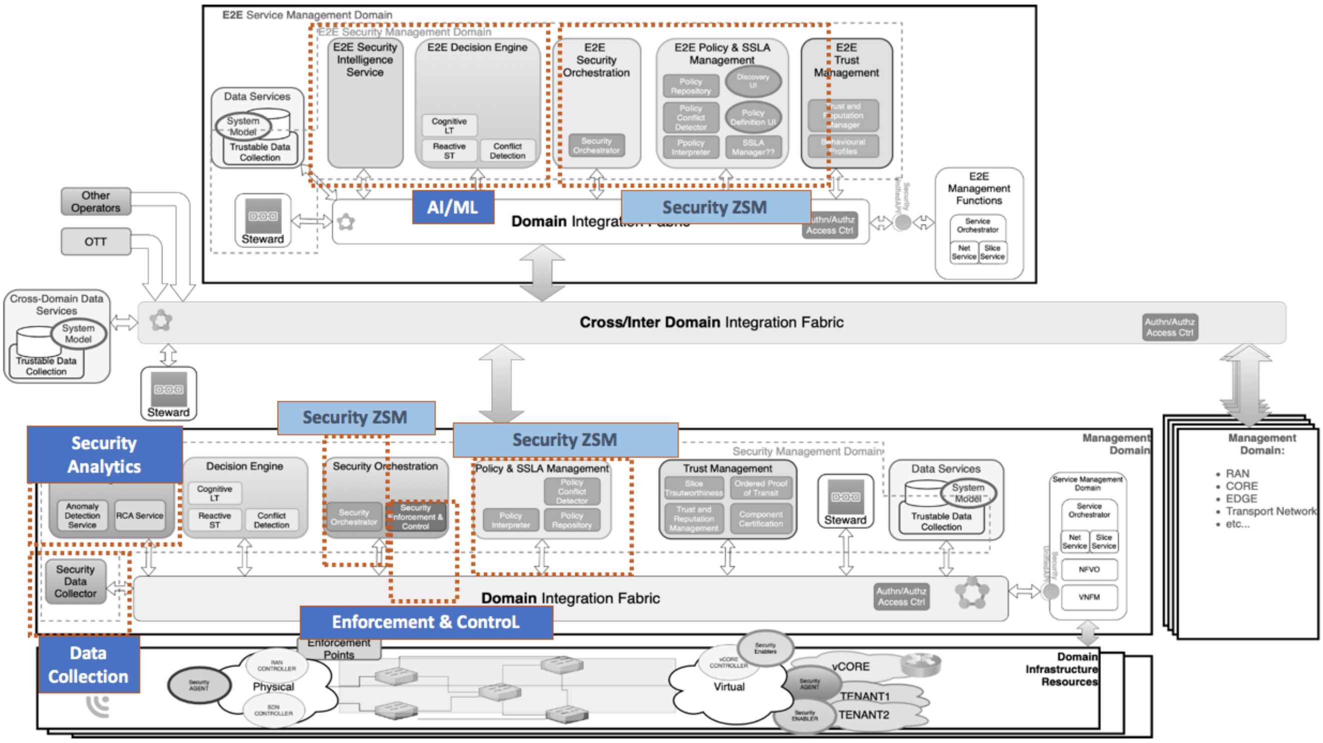


Figure 1: INSPIRE-5Gplus High-Level Architecture building blocks coverage

The ultimate objective behind the identification of these advancement categories is to devise how smart 5G security can be architected and orchestrated in order to cover a complete closed-loop of protection, detection, and response (see Figure 2), based on the typical INSPIRE5G-Plus closed loop defined in D2.1.

Such a closed-loop relies on a set of enablers for data acquisition that collect data and events from various distributed sources. It makes these elements available for analysis and usage to make decision for managing security based on flexible and adaptive end-to-end policy management and orchestration enablers. The latter act on security enforcement and control enablers to enforce security according to the contextual events (vulnerabilities, attacks, etc.) and security policies.

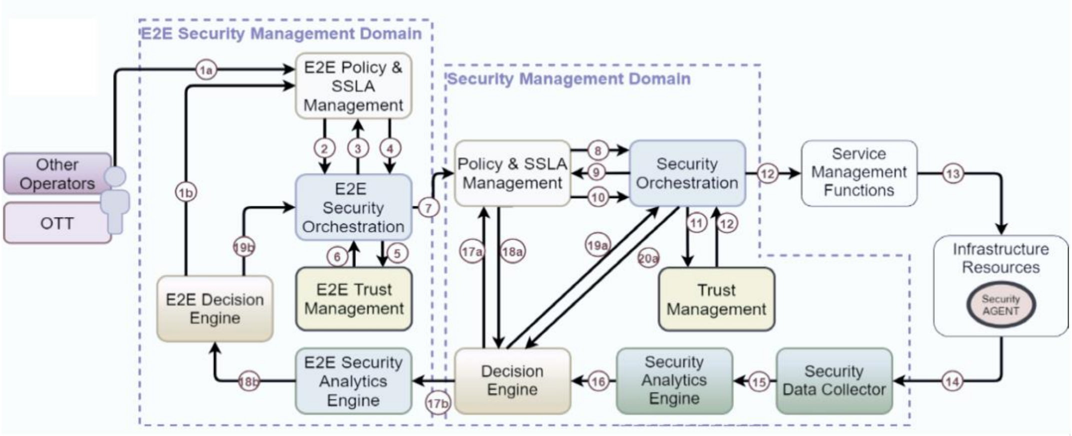


Figure 2: Typical INSPIRE-5Gplus closed loop covered by WP3 enablers

All enablers that relate to this project Smart 5G security, whether being progressed or reused as part of the project are grouped and described in sections related to one of the five above-cited categories.

For each enabler, a description of the problem statement and challenges is exposed, then the State-of-the-Art is detailed in order to analyse existing assets. A set of planned advancements are specified as well as the role of the enabler in the high-level architecture of INSPIRE5G-plus as defined in WP2. Finally, Section 7 concludes the report with a table showing the coverage of the security gaps that have been identified in Deliverable D2.1.

2 Artificial Intelligence and Machine Learning for Smart Security

2.1 Introduction

The anticipated complexity and diversity of 5G and Beyond 5G (B5G) networks, accompanied with the stringent performance and service requirements of newly introduced Use Cases, have called for smart, adaptive and efficient network management and control schemes. This is also reflected in the overall security management and provisioning in these systems. Accordingly, in the INSPIRE-5Gplus project, novel AI/ML based security enablers will be investigated and integrated to the overall proposed INSPIRE-5Gplus security architecture.

The goal of having advanced security enablers driven by AI/ML requires a multi-pronged approach. INSPIRE-5Gplus will focus on different aspects to serve that goal.

The INSPIRE-5Gplus enabler **MOTDEC** will be a totally new enabler designed and developed in the course of INSPIRE-5Gplus. It will provide the capability to adaptively control Moving Target Defense (MTD) in a softwarized network environment, as envisaged in 5G and B5G networks. It will closely cooperate with the OptSFC enabler to facilitate MTD. Any AI/ML scheme is also heavily reliant on data and situation awareness.

In that regard, the **Cyber Threat Intelligence (CTI)** service is being adapted for 5G to provide awareness of ongoing attack campaigns and improve the prevention and mitigation of attacks. An online service is being set up with an Open API, so that different cyber security enablers can obtain information that will improve their detection capabilities. This service integrates Machine Learning techniques to identify anomalies in different types of captured information (e.g., BGP announcements, traceroute logs, honeypot and darknet traffic).

As a key technique, an important utility of AI/ML is the attack detection and mitigation in 5G networks. The **DDoS Detection & Mitigation enabler** is a new enabler that will be devised and developed in the framework of INSPIRE-5Gplus. The enabler will leverage ML techniques to tackle stealthy DDoS attacks in two 5G system settings, namely: (i) network slicing environment and (ii) multi-domain/multi-tenancy environment.

The **Decision Engine** will drive the ZSM closed-loop to create mitigations for security threats detected by enablers, such as the DDoS Detection enabler. The mitigation will take the form of new policies forwarded to the INSPIRE-5Gplus security framework to trigger the security assets. This generation may use advance AI/ML techniques if the context is applied.

In the following subsections, we describe these enablers in terms of addressed challenges, relevant state of the art and solution description. Moreover, we depict their integration into the INSPIRE-5Gplus HLA.

2.2 Moving Target Defence Controller

2.2.1 Problem statement and challenges

Software Defined Networking (SDN) and Network Function Virtualization (NFV) characterize the advent of 5G networks and will allow a significant manoeuvrability of large-scale networks. Paired with the increased bandwidth in 5G infrastructure, this opens a range of new use cases, especially for large-scale environments like IoT applications, autonomous cars networks, drones, and Edge Computing. However, the increased complexity of the ecosystem results in a greater attack surface and a considerably extensive action space for attackers. A malicious user can perform various attacks such as jamming, DoS, spoofing, man-in-the-middle, and can attack from within the network as the risk of compromising a single device from the thousands of IoT devices belonging to a single slice increases.

A great challenge is to prevent and mitigate attacks toward large-scale 5G systems in a proactive manner. It becomes imperative to have an automated system that monitors, detects and adaptively mitigates the anomalies by minimizing the attack surface, performing optimal and dynamic decisions, considering the multitude of factors in the current state of a protected network.

Therefore, the Moving Target Defence (MTD) enabler aims at serving these requirements related to the Security Gaps defined as “MTD and Cyber Mimic Defence Techniques” and “Artificial Intelligence and Machine Learning” listed in D2.1 Chapter 5.7 table. (Security Gaps)

2.2.2 State of the art analysis

Moving Target Defence (MTD) is the technique of changing properties and configuration of an ICT environment, such as the topology and the address space layout, by potentially modifying instruction sets, IP addresses, port numbers, proxies, virtual machines, operating systems, software programs, protocols and packet headers resident in a network [1]. This paradigm cancels the advantage of data intelligence that attackers gain by the targeted ICT environment (i.e., fingerprinting) proactively, and reactively mitigates detected attacks and anomalies if needed. It complements classic security approaches, such as firewall, security protocols, authentication and encryption, increasing the hardening of the system. Such moving parts could be the network itself (e.g., its topology to make eavesdropping on specific traffic difficult), technology stack (e.g., the network equipment that processes a packet to make it hard for an attacker to execute precision strikes on specific vulnerabilities), execution environment (e.g., randomize the underlying VM technology on which a certain service runs when an instance is started) or the software (e.g., use different implementations of the same functionality).

Previous research has proposed various approaches using shuffle, diversity and redundancy operations [2], such as network and memory address space randomization, instruction set randomization, and software diversification, to increase the difficulty and time required to discover a target system’s configuration by expanding the exploration surface or proactively moving the attack surface. Cyber deception and mimicking techniques are also used as a cyber-defence approach. How those deception resources will be selected, deployed and managed are crucial research questions. As an example, an intelligent deployment policy used to dynamically adjust the locations of deception resources according to the network security state is developed in [3].

Although various MTD based solutions have been explored in the literature[131 to 137], the slice-oriented protection in 5G networks and how to integrate MTD is an open question. MTD implementation is also challenging in fragmented and multi-domain networks, since such proactive schemes may require distributed and wide-range of changes in the overall network. Moreover, the optimization and automation of MTD in such context, using AI/ML techniques, needs further investigation. MOTDEC (together with OptSFC enabler) will address this research gap and facilitate MTD in 5G security context.

2.2.3 Solution description and achievements

The MOTDEC module will be interacting with different 5G components such as Slice Manager, the network management system, and INSPIRE-5Gplus framework elements, like the security decision engine and the security agents in order to implement the security policy and perform the mitigation actions in conformity. The specific use case is planned to be network slice protection as shown in Figure 3, even though that can be extended to other security scenarios. It will need a cognitive system that dynamically determines what to move, where to move and how to move, based on the received input and on the action costs, in order to perform an optimal mitigation action.

To this end, Machine Learning (ML) will enable MTD intelligence on evaluating the cost of the different actions, based on the actual state of the network and on the gravity of the threat. To orient MTD towards the optimal policy, we consider the usage of a Deep Reinforcement Learning algorithm, which will allow the system to continuously optimize its actions and adapt to changes of the attacker's strategies and the network's advancement. This will be realized in the OptSFC separate enabler described in paragraph 4.2 of this document with simple and open APIs for a modular and extensible design.

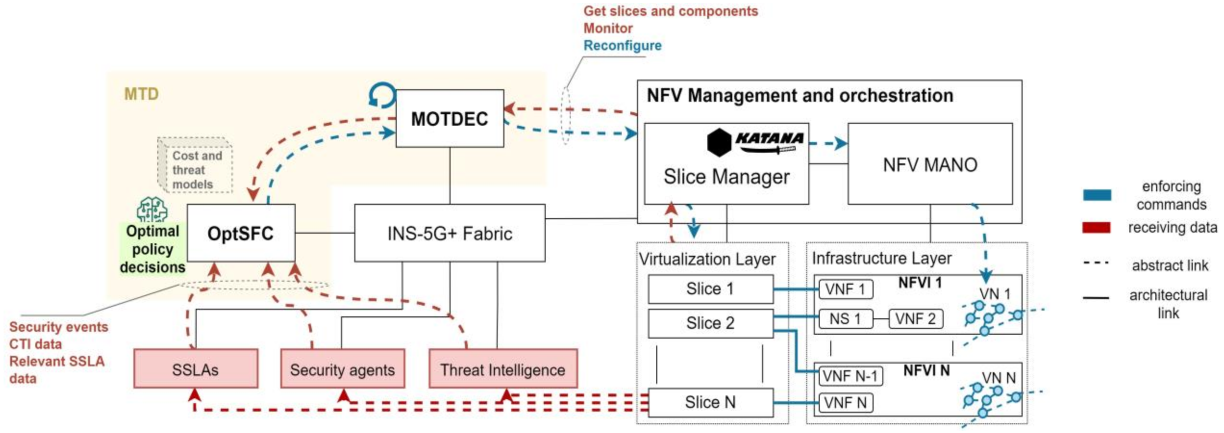


Figure 3. MTD instantiation for network slice protection

Apart from the mitigation actions of MTD (reaction mode), we also plan to have a prevention policy which periodically changes the network each period *p,* independently from the detection of threats; *p* will be randomly defined at runtime, limited by a defined average period to obtain the optimal cost-effectiveness ratio of the MTD operations (proactive mode). The MTD can also be used to deceive attackers by giving them incorrect information. For instance, one can implement a "Smart Moving Honeypots" mechanism to replace important strategic nodes with a honeypot. We can also use honeypots to train the MTD against occasional attackers without risks and maximizing the learning experience by removing limits on learning exploration that we would have in the real network. Again, these actions will be optimized using cognitive techniques mostly realized in OptSFC module.

2.2.4 Integration-interaction with the HLA enablers

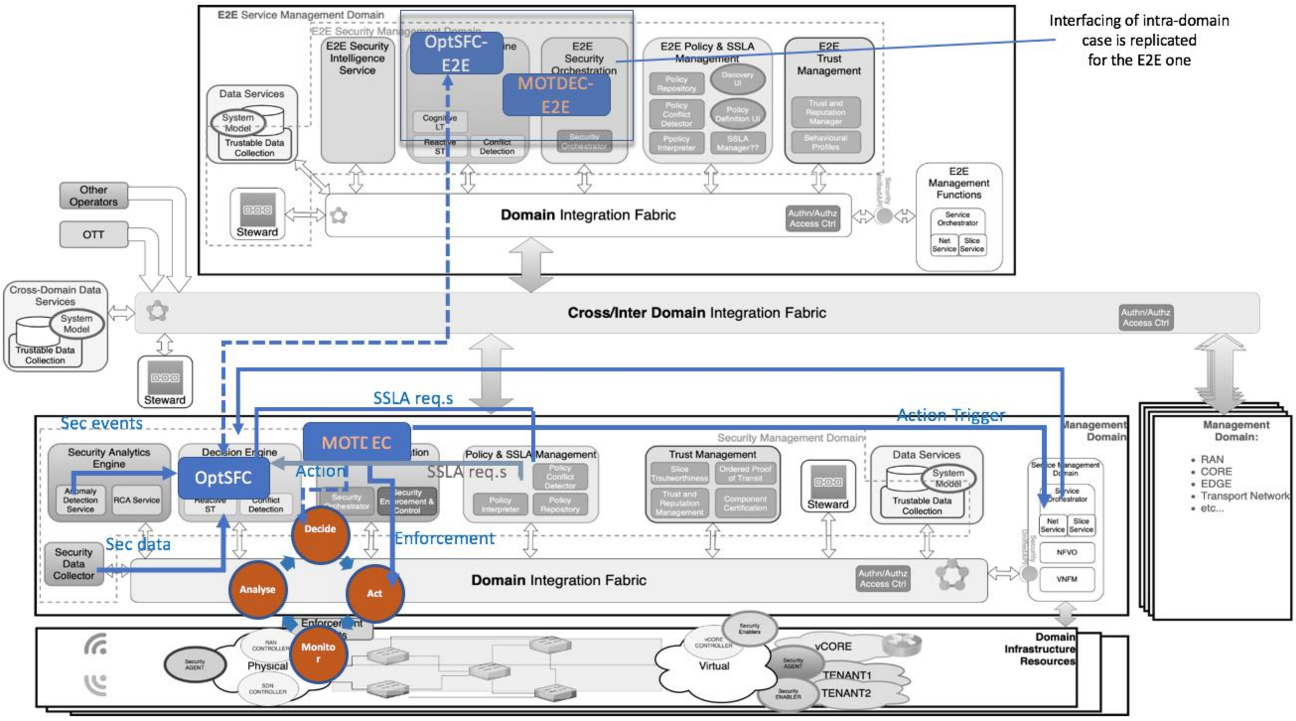


Figure 4: MOTDEC (and OptSFC) embedded in the INSPIRE-5Gplus security architecture

MOTDEC collaborates with OptSFC to realize the smart MTD schemes in the network environment. It relies on OptSFC for optimized security actions and smart action planning. Please note that although the interactions between different INSPIRE-5Gplus functional blocks and MOTDEC are shown as direct arrows, the actual information exchange occurs over the integration fabric.

2.3 Cyber Threat Intelligence service

2.3.1 Problem statement and challenges

Stakeholders (e.g. operators, verticals, CERTs, CSIRTs) require streamlined and efficient threat intelligence that allows them automate self-protection and/or position their threat operations teams to understand and quickly act upon the highest priority threats they face. Threat intelligence improves the effectiveness of the security functions and can even help prevent attacks from occurring.

Many sources of CTI exist today but unfortunately, they suffer from many drawbacks that have been identified by the end-users. The main complaints are that the information is not timely (i.e., rapidly becomes obsolete), too complicated to use (e.g., not well-categorised according to threat type or attacker), and it is often not possible to automate its use. Furthermore, there is much to be done to obtain CTI tailored for 5G mobile communications and infrastructure.

The solution addresses the challenge described in the Table 4 found in Sec. 5.7 of the deliverable D2.1: Cyber threat intelligence and data sharing. (Security Gaps)

2.3.2 State of the art analysis

A lot of work has been done to produce CTI and many open and commercial services exist. Nevertheless, there are many gaps that need to be filled as previously indicated. When looking at the cybersecurity and cyberterrorism landscape, one can easily recognize a strong and continuous evolution at every level, from the vulnerabilities to the attack surface, to attack techniques and tools and moreover the attackers and their motivations. These turbulences increase the need for solutions able to adapt in the shortest possible time frame and recognize cyber-threats and cyber-actors, a scenario which emphasized the strategic role of CTI and led to the creation of a variety of CTI platforms.

Such solutions vary in their scope. On one end of the spectrum are threat exchange specifications that enable CTI to be shared among interested parties. At the other end are complete CTI platforms including data collection, correlation, analysis and visualisation (often involving hardware installation, typically labelled as a SIEM solution). Some of the most popular CTI solutions are as follows, in increasing order of scale:

- OpenTAXII: Open-source implementation of TAXII, a specification for CTI message exchange.
- Collective intelligence frameworks (CIF): Platform for integrating and collating CTI feeds for multiple sources.
- OpenTPX: Specification and tools for sharing CTI data.
- YETI: Platform for integrating CTI indicators and events into a single database.
- GOSINT: Framework for integrating and collating CTI indicators.
- MISP: Full-featured CTI platform for collecting, correlating, storing and sharing indicators, feeds, binaries and more.
- AlienVault OSSIM: Full-featured CTI & SIEM platform for attack detection, vulnerability correlation, monitoring, and extensive visualisation features.

All of these specifications and platforms are designed to be open and generic in order to ease the integration with other third-party feeds and services. The solution that is being built, on the other hand, is an end-to-end platform, from data collection to visualisation and incident response. Its detection and analysis capabilities will be backed by different types of data (coming from BGP, traceroute, honeypots, darknet), hundreds of detection sensors around the world, giving a broad base of data, and with specific support for protecting 5G networks and functions.

Concerning the detection of anomalies in the Internet routing and topology, INSPIRE-5Gplus has started building its advanced CTI service in the H2020 SISSDEN [4] project that experimented the use of a worldwide sensor network, deployed and operated by the partners of the consortium. The results of this project provide a highly configurable probe for the detection of anomalous behaviour in the European wide network of honeypots and darknets. The H2020 SAINT [5] project analysed and identified the effectiveness of collaboration and regulations to counter cyber security issues and studied the economics of cyber defence techniques and cybercriminal activity. It contributed to the studies and developed tools for improving the awareness of users of the risks and costs related to security breaches and the best practices and costs related to the protection of assets. The results of both of these projects serve as baseline for defining and building the CTI service for better preventing and countering security breaches in 5G mobile networks that will be extended and tested in the context of INSPIRE-5Gplus.

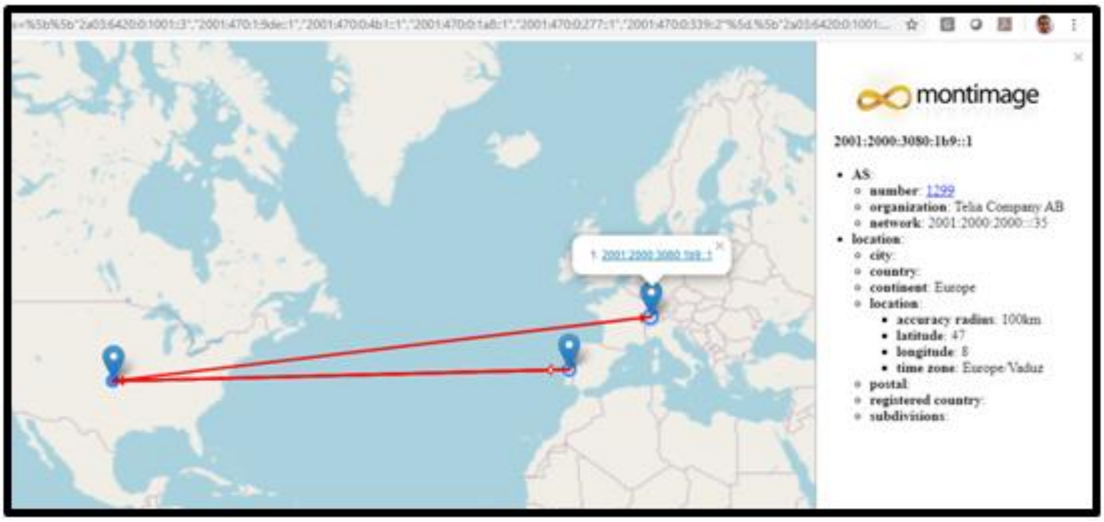
2.3.3 Solution description and advancements

A CTI framework started to be developed in the H2020-SISSDEN, H2020-SAINT and CARTIMIA projects. The framework serves for collecting and aggregating data from different sources (Honeypots, Darknets, OSINT, commercial data), and analysing it to obtain threat intelligence that can be used for preventing attacks on one's network. Its main components are (some more evolved than others):

- Network of honeypots and darknets
- Monitoring probes
- Analytics platform
- Aggregator of data from different sources
- Data repository
- Visualiser of physical and logical Internet routes
- Detector of anomalies in Internet topology

The CARTMIA project was carried out in response to a Challenge called SYNAPSE [6]organised by the French Cap Digital cluster. In this challenge, the recuperation of data was from different sources (e.g., BGP and traceroute datasets, own probes) was automated to map the physical and logical topology of global Internet, with the goal of detecting anomalies such as: hijacking, AS-path changes, failures/outages, Bot and Command & Control activity, DDoS and scan activity. This work is being extended in the INSPIRE-5Gplus project by introducing Machine Learning techniques to aggregate information on malicious activity captured by a honeynet; detect the anomalies in the network; and, later, include data from darknet (i.e., network telescope) and specialised honeypots deployed in the different network domains and verticals.

Figure 5 shows the path of the network packets going from one Autonomous System (AN) to another obtained by analysing BGP announcements. The obtained topology needs to be periodically analysed to detect changes that could represent attacks (e.g., hijacking) or network outages. CARTIMIA goes beyond this classical way of doing things [7] (which essentially relies on BGP) by aggregating this data with data from different sources (in particular, traceroute probes, honeypot, darknet data and Open Source Intelligence), and implementing different ML algorithms. Work being done in collaboration with the University of Strasbourg[8] involves implementing and testing different algorithms. For instance, extracting features, using eigenvector centrality and other techniques that locate the most important elements in a graph; then the features are analysed using different Machines Learning algorithms, such as Support Vector Machines and Multi-Layer Perceptron to identify BGP path leaks.


=%5b%5b"2a03:6420:0:1001:3","2001:470:1:9de::1","2001:470:0:4b1::1","2001:470:0:1a8::1","2001:470:0:277::1","2001:470:0:339::2"%5d,%5b"2a03:6420:0:1001...
↑ 2001:2000:3080:1b9::1
montimage

2001:2000:3080:1b9::1

- **AS**:
  - **number**: 1299
  - **organization**: Telia Company AB
  - **network**: 2001:2000:2000::/35
- **location**:
  - **city**:
  - **country**:
  - **continent**: Europe
  - **location**:
    - **accuracy radius**: 100km
    - **latitude**: 47
    - **longitude**: 8
    - **time zone**: Europe/Vaduz
  - **postal**:
  - **registered country**:
  - **subdivisions**:

Figure 5. Path between two ASs represented on the map

2.3.4 Integration-interaction with the HLA enablers

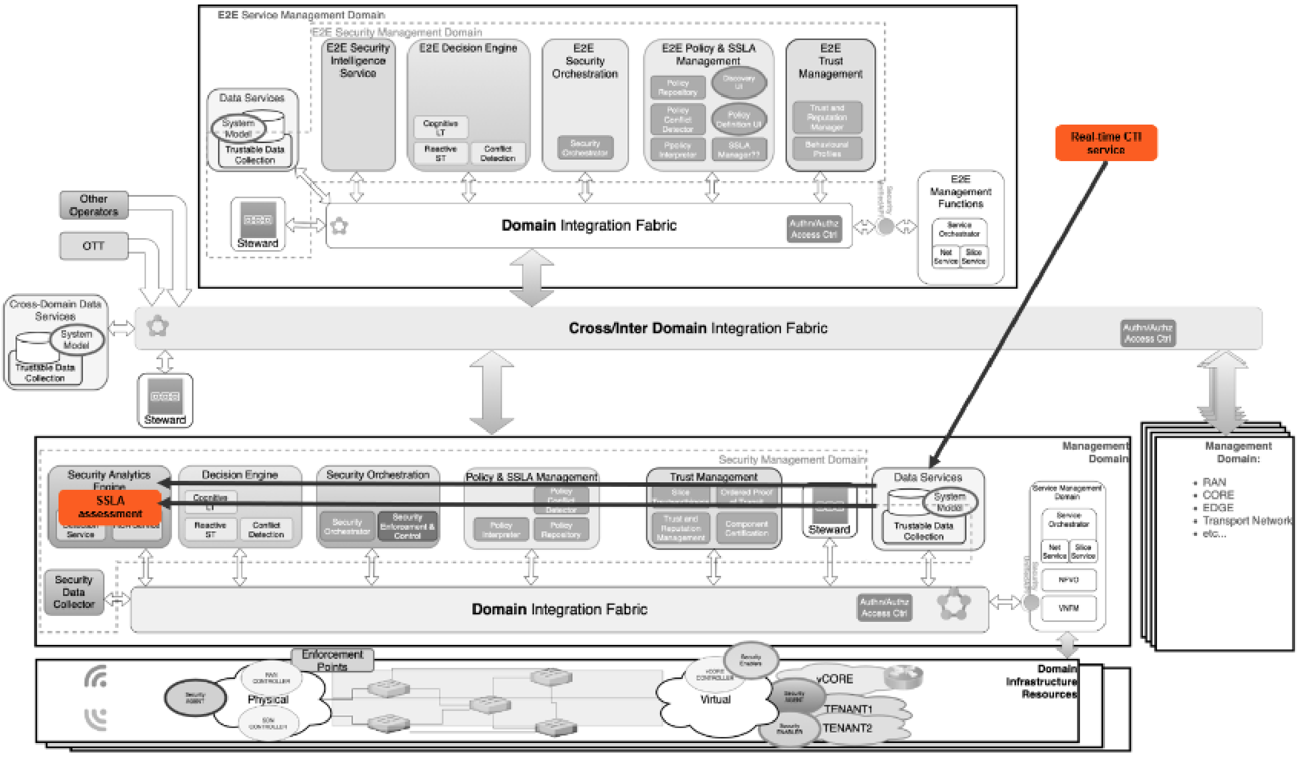


Figure 6. Integration-interaction of CTI enabler with HLA

The CTI service is an external service that aggregates information from many different sources and this information can be made available to the Security Analytics Engine or the SSLA assessment module to identify IPs, ASNs, and domains/hostnames/URLs involved in security breaches and malicious activity. It will also provide intelligence on different types of ongoing threat campaigns or even information on the reputation of the different countries, service providers and operators. This information can improve the detection (eliminate false negatives) or make them more precise (eliminate false positives).

2.4 Stealthy DDoS Detection & Mitigation

DDoS attacks can be broadly classified into two types, namely[9]: (i) network-layer DDoS attacks, aiming at saturating the network bandwidth by generating volumetric traffic or high-rated packets, and (ii) application-layer DDoS attacks, focusing on exhausting the server's computational and memory resources. Application-layer DDoS attacks are usually stealthy in nature trying to mimic genuine behaviour with low-bandwidth usage, making their detection and mitigation harder. The complexity of handling application-layer attacks is a key driver of the significant growth in their number these last years. Despite the research efforts devoted to tackle the DDoS attacks [21] [11], very few contributions have aimed at addressing the issue of stealthy DDoS attacks considering the peculiarities of a 5G system, such as network slicing and multi-domain/multi-tenancy.

This enabler aims to fill the aforementioned gap by tackling stealthy DDoS attacks in two 5G system settings, namely: (i) network slicing environment and (ii) multi-domain/multi-tenancy environment. The enabler will leverage AI techniques for efficient and effective detection and mitigation of DDoS attacks.

This enabler security motivation and engineering relates to the identified (security) limitation and gap of Chapter 5.7 of WP2 deliverable D2.1, defined as “Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats”. (Security Gaps)

2.4.1 DDoS Detection and Mitigation in network slicing

2.4.1.1 Problem statement and challenges

Network slicing is a key technology in 5G, boosted by SDN and NFV. It is based on soft or hard isolation of physical resources. While the latter ensures complete isolation, the former allows the sharing of the same physical resources and makes a virtual allocation of them to each slice. Used for SDN, software-based isolation is a pillar of network virtualization. Improper isolation between the network slices can lead to highly insecure situations. In fact, the sharing of virtual and physical resources between slices raises DDoS threat, where a DDoS attack against one slice may affect the availability and performance of services provided by other slices sharing the same visualized infrastructure. Moreover, unlike traditional DDoS attacks, the new breed of DDoS attacks is getting stealthier with the aim to mimic genuine behaviour with low-bandwidth usage, which makes their detection and mitigation harder [10]. Although extensive work has been engaged and several solutions have been proposed to tackle DDoS attacks, addressing the stealthy DDoS issue is far from being completely resolved, and even less in 5G network slicing environment [11].

2.4.1.2 State of the art analysis

DDoS attacks are recognized as a critical security concern targeting 5G network slicing during the run-time phase[15], [16]. Despite the research efforts devoted to tackle the DDoS attacks [21] [11], very few contributions have aimed at addressing the issue in 5G network slicing environment. The authors in[19] discussed the use of resource isolation as a mean to mitigate DDoS attack in 5G network slicing. They investigated potential methods to achieve host resource isolation and network communication isolation. Similarly, the work in Sattar [7] leverages inter-slice and intra-slice isolation for proactively mitigating DDoS attacks in 5G core network slicing. The complete isolation between slices enabled by inter-slice isolation allows the mitigation of DDoS attacks. Nevertheless, its use may lead to inefficient resource usage. Moreover, adopting containers for deploying VNFs makes the complete isolation hard to achieve due to the lack of strong hardware isolation [18], [19]. Thus, solutions to mitigate DDoS attacks while considering the resource sharing and the imperfect resource isolation are necessary. A special attention should be paid to the new breed of DDoS attacks, namely the slow-and-low application-layer DDoS attacks. These variant of DDoS attacks aim at exhausting the server’s resources (e.g., CPU, memory, I/O) through an attack flow that looks legitimate. Although application-layer DDoS attacks has recently attracted much research attention [20], [21], they are still an ongoing concern not yet resolved. Without proper mechanisms to defeat application-layer DDoS attacks in network slicing, their effect may be devastating to the whole system [22].

2.4.1.3 Solution description and advancements

AI usage is identified as a requirement to recognize abnormal traffic patterns that can lead to service unavailability or security threats in future networks [13] [22]. Indeed, AI has the potential of uncovering hidden patterns from a large set of time-varying multi-dimensional data and delivering faster and accurate decisions. Combining the capabilities of AI with the flexibility of virtualization (NFV) and softwarization (SDN) technologies, the envisioned enabler aims to automatically detect and mitigate stealthy DDoS attacks in 5G and beyond network slices. Furthermore, P4 (Programming Protocol-Independent Packet Processors) [14]can play a crucial role in achieving this goal by flexibly implementing a suitable DDoS solution at the Data Plane level or by using its Inbound network telemetry as a strategy to collect data from the network to be analyzed by the AI entity.

2.4.1.4 Stealthy DDoS Integration-interaction with HLA

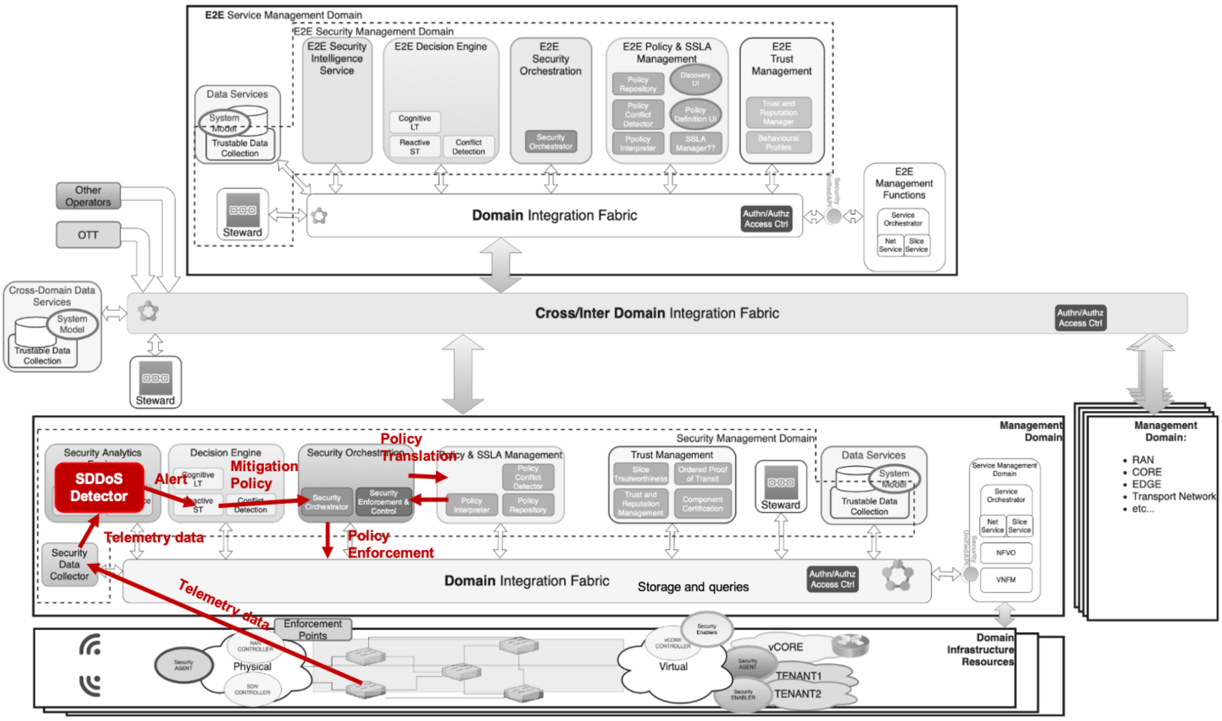


Figure 7. Integration-interaction of stealthy DDoS with HLA

The network is continuously monitored, and the collected monitoring data is captured by the “Security Data Collector” which forwards this data to the AI-based DDoS detector to perform anomaly analysis and detect any potential pattern of DDoS attack. In this last case, an alert is submitted to the “Decision Engine” to generate the mitigation policy which will be enforced by the “Security Orchestrator” after being translated by the “Policy & SSLA Management” module.

2.4.2 Multi-domain, multi-tenant AI-based DoS Detection

2.4.2.1 Problem statement and challenges

The arrival of 5G and its inherent proliferation of IoT devices has made the attacks that cybersecurity experts deal with every day more complex and difficult to counteract. The most representative example of this situation is distributed denial of service attacks, commonly referred to by their acronym: DDoS. This type of attack, despite its very limited complexity, has benefited greatly from the numerous advances brought in by new mobile network technology: greater bandwidth (around 10 Gbps), lower communication latency (1-2 milliseconds), the capacity of hosting more devices in less space, among other features. The most effective solutions currently available to mitigate this type of attack are Network Intrusion Detection Systems (NIDS), which monitor the activity of the network segment in which they are deployed in real time, in order to identify any anomalous pattern in the traffic corresponding to an attack that is taking place at a given time. This type of detection systems is generally deployed in small-medium sized networks, such as internal networks that belong to specific organizations, and there are hardly any use cases in larger, multi-domain networks, such as a 5G network.

This type of network incorporates multi-tenancy concept, which involves creating several virtualized network layers (slices) that emulate the physical infrastructure on which they have been deployed. In this way, a different virtual operator can be hosted in each of the slices, being able to make concurrent use of physical resources along with services deployed in other layers. This creates a problem in terms of monitoring the traffic needed for analysis, since specific protocols are used to implement multi-tenancy, and since the structure of the packets changes substantially as they go through the different segments of the network. Also, it is way more difficult to identify the attacker (traffic emitter) because of this.

What is proposed is a system that deals with the problems that we have already enumerated, capable of detecting denial of service attacks on 5G/IoT networks in an efficient and effective way using AI techniques. In addition, it allows early detection of the attack since it is deployed between the edge and the core of a 5G network.

2.4.2.2 State of the art analysis

There is a significant amount of research and surveys belonging to different universities and departments that focus on the detection of anomalies using Deep Learning techniques [23], others that apply statistical techniques, in addition to AI techniques, focusing on the detection of distributed denial of service attacks (DDoS) [24].

Ana Serrano Marmolar, Zeeshan Pervez et al. [25], focusing also on DDoS attacks, emphasize the limitations of current NIDS to work with 5G traffic, such as the lack of information to trace back the origin of the attack for proper mitigation, and present a proof-of-concept system that pursues a goal very similar to ours. Sabah Alzahrani & Liang Hong [26] proposed a hybrid signature-based and anomaly-based NIDS system that, also based on artificial intelligence techniques and deployed over a cloud computing scenario, was capable of detecting DDoS attacks with a high accuracy. One of the most interesting papers in this area is written by R. Doriguzzi-Corin, S. Millar et al [27]. It proposes a system for detecting DDoS attacks using quite powerful AI techniques such as Convolutional Neural Networks (CNN). The proposed system obtains an accuracy of 99.67% and has been tested with realistic and large-scale DDoS attacks datasets. It offers an excellent performance, processing up to 55000 samples per second. In addition, it is designed to be deployed at the edge of the network, which is very interesting for its later deployment in a real 5G network and can be executed without a problem on resource-constrained devices.

2.4.2.3 Solution description and advancements

The system we propose consists of three main modules, which are: real-time network monitoring (1), conversation processing (2) and AI model for cyber-attacks detection (3).

The first one is in charge of capturing in real time all the traffic that arrives to the interface on which it is listening, extracting a set of relevant packet fields from each of the captured packets, and making them available to the conversation processing layer. It is in this part of the system that we have to deal with the problem of the structure of the packets, which are doubly encapsulated since they are 5G multi-tenant packets. In this solution, the GTP and VXLAN protocols are being considered for the implementation of multi-tenancy, so this first module, which should be written in raw C, should be capable of extracting the needed information from each of the GTP and VXLAN headers and from the rest of the headers that compose the package. This parsing has to be done at a very low level by handling manually defined data structures and offsets, in order to obtain quite competent performance in execution times, which is necessary for the rest of the system since where more time must be spent is in the modules described below. Solutions based on P4 are also being considered for traffic processing and analysis.

The second module will be responsible of grouping all the packets it receives from the first module into conversations. Two packets will belong to the same conversation if the source and destination IP addresses are the same, and if the port number is also identical. From each conversation it has to be able to calculate a set of features such as: number of new connections to the same destination host as the current connection in the last seconds, percentage of active connections from the current host which have the same destination service, among many others (ideally, about 50-60).

The last module of the system receives a message for each conversation identified by the previous module, composed of all the features belonging to that conversation. This module is the most important part of the system, as it is responsible for obtaining the conclusion of whether the traffic captured for a conversation (based on the metrics obtained) is a denial-of-service attack or not. To do this, it will perform a clustering-based process and then, if no firm conclusion has been reached, a second processing phase is performed using an Autoencoder (AE). Before processing the actual conversations, the system has to pass through a training process with genuine traffic. This will train both the models with traffic that does not represent an attack, so that they can later identify the attack traffic as anomalous.

To make possible the communication between the modules, we need to use a publisher-subscriber service like Apache Kafka. For the communication between the first and the second module of the system a topic has to be created, while for the communication between the second and the third one a different topic has to be used. In the first topic, the real-time network monitoring module will publish one message per captured packet, while in the second topic a message will be published by the conversation processing layer for each identified conversation, composed of all the features obtained from each one of them. Finally, a third topic can be created so that, once the third module detects whether a conversation is an attack or not, it will publish a message with the result, in order to subsequently implement a mitigation mechanism based on SDN techniques.

2.4.2.4 DoS detection enabler Integration-Interaction with HLA

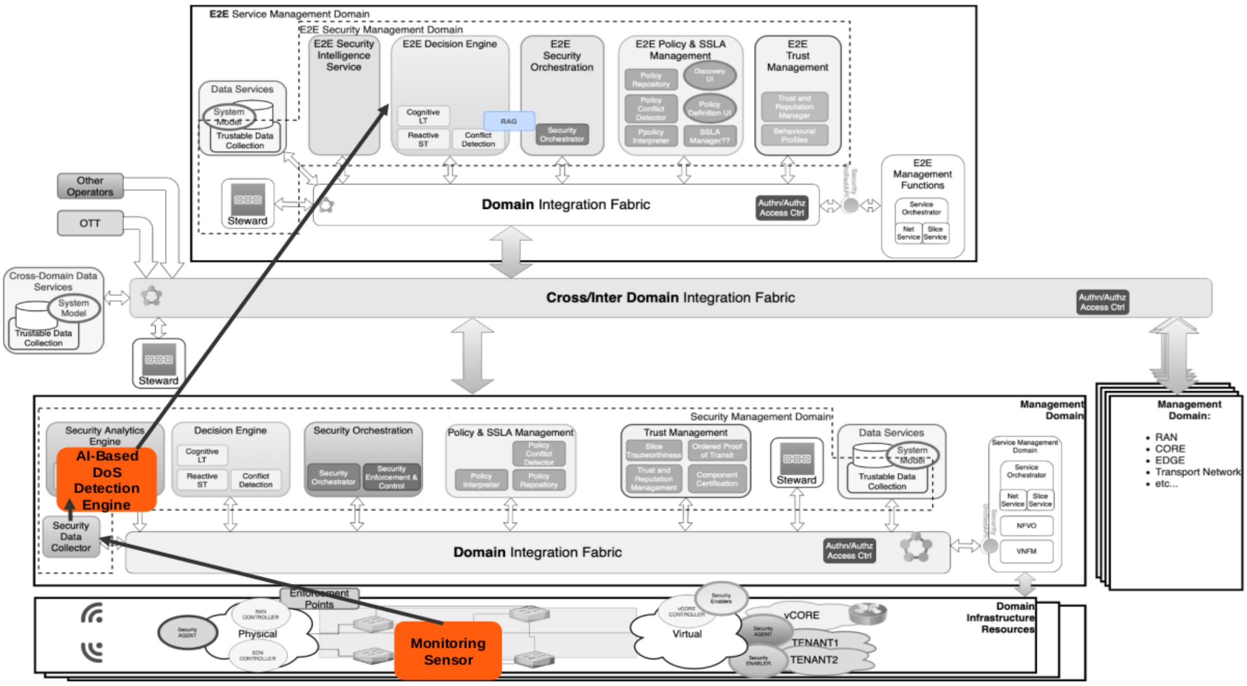


Figure 8. Interaction of DoS detection with the HLA

Deployed sensor infrastructure that is constantly monitoring the network and send collected data to the Security Data Collector which will forward to the AI-Based engine capable of detecting DoS attacks, this engine when an attack is detected will communicate to the E2E Decision Engine for further mitigation actions.

2.5 Decision Engine

2.5.1 Problem statement and challenges

In today's security platforms, multiple advanced assets (generally based on AI techniques) process events to build high level notifications on detected threats. In the ZSM loop, theses detections need to be translated into mitigation plans intelligible by the underlying security actuators, mainly the Security Orchestrator. The problem is to transform threats notifications into meaningful mitigations.

In this context, the encountered challenges are:

- The ability to create powerful mitigations within a short delay.
- Building mitigations that span across multiple domains and utilize them as an extended poll of insight to thwart distributed attacks.
- Being able to extract the semantic of a threat notification to handle generic, open events.

The previous Deliverable D2.1 describes various Security Gaps in its section 5 (Security Gaps) The Decision Engine is related to:

- Automation and Zero-touch Service Management: The Decision Engine fills the gap between the detected threat and the creation of their corresponding mitigations. The use of Reactive assets to deploy simple and bare-bone mitigation will keep the Decision Engine to fall into a over-arching solution. It is also a sandbox to understand and adapt the ZSM standards as seen by the ETSI specifications.
- Artificial Intelligence and Machine Learning: The Decision Engine will also encompass complex AI assets as "plugins". Thus, it will inject AI and ML techniques into the ZSM loop.

Moreover, the INSPIRE-5Gplus project targets a multi-domain context. A local domain could take a decision / mitigation and then propagates it toward the E2E domain. This mitigation can be replicated inside others separated domains if the security changes make sense: for example, a device banned in the Cloud domain can be isolated in every managed domains.

Finally, the use of multiple security assets, each having its own area of expertise, could be an opportunity for the Decision Engine to create "enhanced" decisions that combine multiple mitigations: for example, triggering an encryption key refresh with a MTD update.

2.5.2 State of the art analysis

The ETSI ZSM reference architecture [28]describes a Zero-touch network and Service Management (ZSM). It details the Domain intelligence services, which are responsible for driving intelligent closed-loop automation in a domain. They support variable degrees of automated decision-making and human oversight with fully autonomous management being the final target. Some of the key principles are:

- That the closed-loop management automation is a feedback-driven process. It drives the system towards a set of objectives without any intervention while controlling the impact of the chosen actions on the system.
- The management functions should be stateless and decoupled from the storage.
- The exposed interfaces should be intent based and hide the underlying complexity.

The intelligence services can be categorized as Decision support, Decision making and Action planning, via technologies such as AI, ML and knowledge management. Therefore, the system should deploy AI models and manage them through an AI model assessment service. The derived assessments are used to decide on the most appropriate actions to perform on the running AI model (e.g., to reconfigure, to replace, ...). This management loop also includes the training of the AI, the evaluation of the resulting outputs and the eventual retraining on recent data.

In that regard, Maelstrom (Mitigating Data center-level Disasters by Draining Interdependent Traffic Safely and Efficiently) [29] is a production tool created by Facebook to mitigate and recover from data center-level disasters and outages. It manages data centers' traffic to drain interdependent services from affected regions to healthy ones. To do so, Maelstrom encodes the constraints of services and their dependencies. It also watches the well-being of services to check that these constraints are fulfilled. Maelstrom implements a feedback control loop to estimate the impact of its mitigation deployment. This tool is used in production and also during tests to evaluate the complexity of a system and its ease of recovery and discover silent dependencies between services. Maelstrom is designed around some key principles, two of them are:

- Embracing human intervention: a human operator is needed during the recovery to validate the mitigation plan proposed by Maelstrom. This tool automates the tedious tasks but leaves the critical decision to a human. This aspect is in conflict with the ZSM vision encompassed by the INSPIRE-5Gplus project. Perhaps, a good middle-ground would be to grade generated mitigations in term of impact to fully automate the low ones in a ZSM loop and provide a notification system to a human operator for the most serious ones.
- Separation of policy and mechanism: policies that define how traffic should be shifted is separated from the mechanisms executing those shifts.

These policies are described inside runbooks that specifies the procedure for mitigating the specific scenario. They contain a composition of tasks. A task being a concrete operation (such as restarting a container or moving traffic). When a runbook is run, the Maelstrom's scheduler will execute these tasks in the correct order and verify after each step the correctness of the system. Moreover, the scheduler starts with a small-scale drain tests and gradually enlarge the radius.

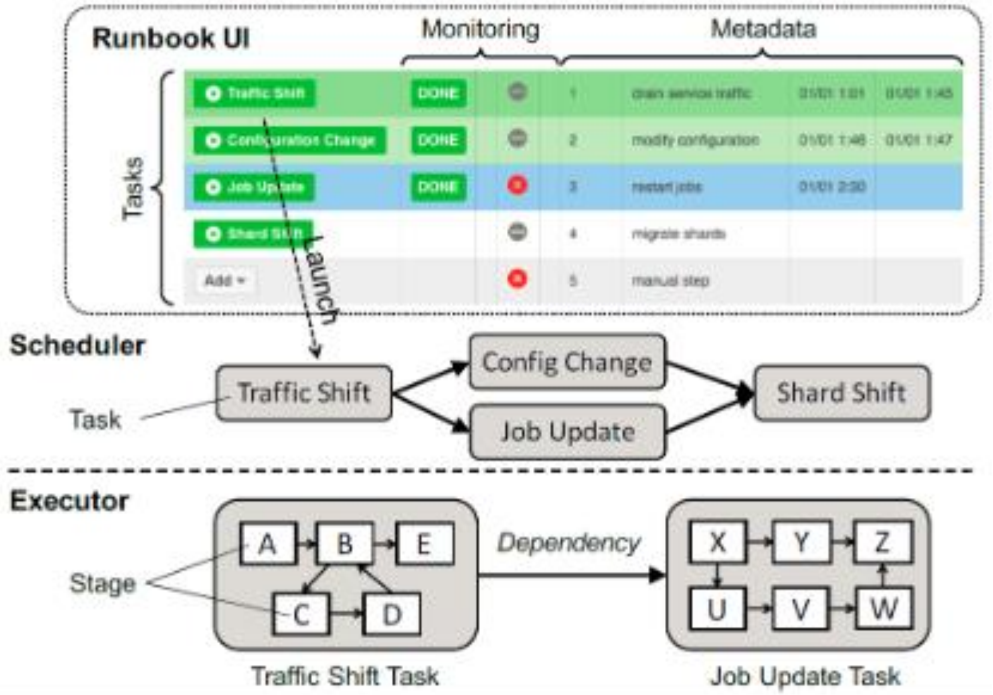


Figure 9. A runbook example containing 4 tasks

2.5.3 Solution description and advancements

The Decision Engine (DE) oversees the different actions emitted by the security assets and the security analytics engine to select the best decisions to apply for securing a running targeted application. This centric component acts as an arbitrator between security assets and the platform within a domain.

The Decision Engine is going to delegate to assets the complex task of creating mitigations.

- First, the Cognitive asset (for example an advanced DDoS mitigation asset) will contain advanced and complex algorithms, based on AI/ML techniques, to create forecast or intricate mitigations. These assets can be difficult to implement or train and may increase decision latency due to their complexities.
- Second, the Reactive assets will contain static reactions templates. Those templates will output simple / swallow mitigation with limited scope. They will be quick to run and easy to create.

This separation allows the Decision Engine to quickly react to threats with Reactive asset, but it can also emit complex mitigation from a Cognitive asset. And viewing these assets as plugins liberates the Decision Engine from containing a all-in-one hard-coded intelligence that must fit every possible use-cases.

To simplify the architecture, the Decision Engine will only be compatible with a specific set of events. This Figure 10 removes the step of learning the intent behind a received generic event. The Decision Engine will mainly manipulate rules (or reactions) books. They will describe a set of actions to perform inside the INSPIRE-5Gplus platform. An action could be a new network slice policy, or a change in a SLA or blocking an IP globally. They will be done by the underlying platform component such as the Security Orchestrator, or The SSLA Manager.

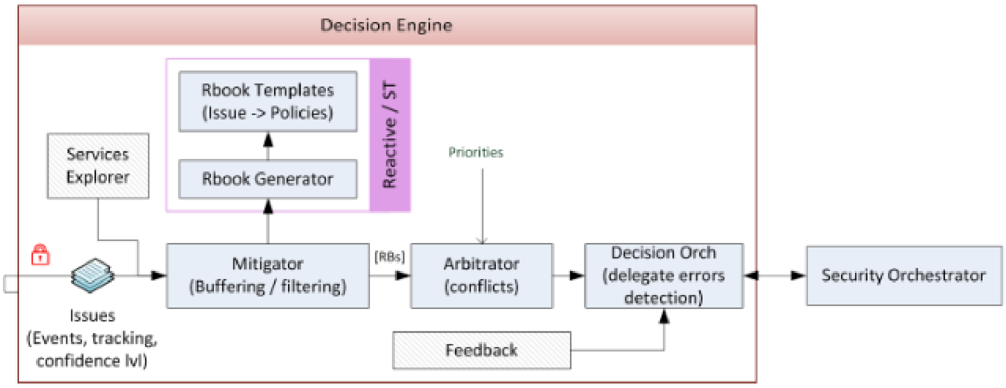

Decision Engine
Rbook Templates (Issue -> Policies)
Rbook Generator
Reactive / ST
Services Explorer
Priorities
Mitigator (Buffering / filtering)
[RBs]
Arbitrator (conflicts)
Decision Orch (delegate errors detection)
Security Orchestrator
Issues (Events, tracking, confidence lvl)
Feedback

Figure 10: Decision Engine. One implementation example of the DE based on Maelstrom design

2.5.4 Integration-interaction with HLA enablers

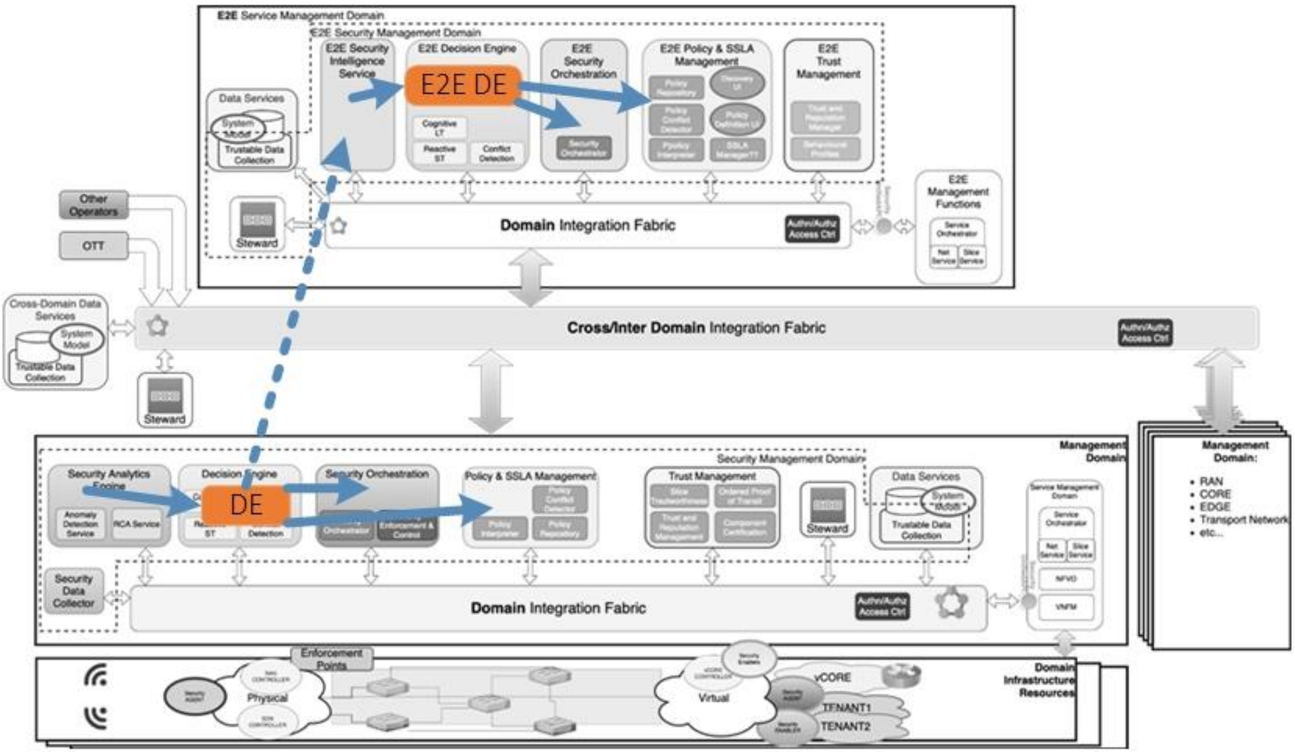


Figure 11. Integration-interaction of the decision engine inside the HLA

As specified in the D2.2 deliverable (Project Documents), the Decision Engine (DE) initiates the security mitigation. First, inside a domain, the Security Analytics Engine notifies the domain DE of ongoing security breaches or anomalies. With this notification, the domain DE generates an adequate decision to resolve the issue. The domain DE can also decide to ignore such notification. Then the DE adapts the decision in term of SSLAs and policies and submits them to the Policies & SSLA Manager for validation. After that, the result is sent to the Security Orchestrator to apply the mitigation. Those exchanges are made through the Domain Integration Fabric. The Domain DE notifies the E2E DE of the actions it takes. The E2E DE works similarly but at a higher level. The key difference is that the E2E DE can leverage its hierarchical view of the various domains to enhance the mitigation. It can also overrule the local decision taken by a domain DE. The Cross/Inter Integration Fabric facilitate this synchronization.

2.6 Baseline assets used in the project

The following assets will be used by partners as baseline assets in the development of their enablers:

- **PunchPlatform** (TSG), developed in SPIDER project: An Elastic, Logstash, Kibana (ELK) based Cyber Security Analytic Platform for quick prototyping with ML techniques. [31]
- **DDoS-dbScan** (TSG), developed in SPIDER project: A DDoS detector using the machine learning DBSCAN clustering algorithm.[30]

3 Zero-touch Security Management

3.1 Introduction

The anticipated complexity in orchestrating and managing security in 5G and beyond networks has driven the move towards zero-touch security management. A sufficient level of automation is required to empower zero-touch security management. In this vein, INSPIRE-5Gplus is designing and developing a set of key enablers that enable automation of security management operations at domain and E2E levels to ensure that the provided security fulfils the expected Security Service Level Agreement (SSLA).

The "Security Orchestrator" enabler is responsible of proactively or reactively enforcing security policies through automatic allocation, chaining and configuration of relevant virtual network functions. To achieve its goal, the security orchestrator interacts with different controllers (e.g., SDN controllers) and management/orchestration services (e.g., NFV MANO, Slice Manager). As the security management needs to be governed by policies and the agreed SSLAs, services to manage security policies and SSLA is essential. To this end, two enablers will be developed in the frame of INSPIRE-5Gplus, namely "SSLA Manager" and "Policy Framework". The "SSLA Manager" provides the whole SSLA lifecycle in a slice, providing necessary services to define SSLAs in machine-readable format, deploy required security policies to enforce the agreed SSLAs, and monitor their fulfilment. Meanwhile, the "Policy Framework" aims at managing the defined security policies by providing functionalities for modelling, translating, determining priority and dependency as well as status of security policies. By analysing the security posture of 5G enabled networks, informed and effective security policies can be enforced.

However, the complexity of 5G ecosystem calls for automated tools to reason about this posture. To meet this goal, INSPIRE-5Gplus provides "DiscØvery", a risk assessment tool that allows remote and automatic identification of hardware, software and even policy-related vulnerabilities, and advocates improvements accordingly. 5G and beyond networks are expected to support heterogeneous and flexible deployment scenarios on the same infrastructure by enabling network slicing. Thus, the incorporation of security management in the lifecycle management of slices from provision to decommission is paramount. In this regard, INSPIRE-5Gplus is proposing two enablers, namely "SFSBroker" and "Secured Network Slice Manager". The "SFSBroker" leverages Smart Contracts of Blockchain technology to automatically provision slice resources in compliance with the SSLAs. The "Secured Network Slice Manager" aims to automatically determine the best option (i.e., individually per each service or collectively) to apply the agreed SSLA within a Network Slice.

The **Security Orchestrator** enabler comes from research community as outcomes from Anastacia project, a cybersecurity framework that provides self-protection, self-healing and self-repair capabilities through dynamic orchestration and deployment of policies and actions. In INSPIRE5G-plus project, the Security Orchestration will be provided with greater flexibility to deploy and configure end-to-end security assets as well as to understand SSLAs, fully automatically in a dynamic environment, able to interact with the other levels of orchestration both inter- and intra-domain and to select the security services and VNFs needed to ensure compliance with the policy

The SSLA Manager enabler is a module integrated in MI's security monitoring and management framework (MMT) that implements the enablers Security Analytic Engine and Security Agents. It started to be developed in the H2020-MUSA project for defining negotiated security rules (SSLAs) that can be assessed and enforced in real-time in the context of federated clouds. It was then adapted for 4G mobile networks in the CelticPlus SENDATE project. In INSPIRE-5Gplus it is being extended and adapted for 5G networks. It offers notifications that indicate that an SSLA is not respected that can be used by other enablers such as the Security Orchestrator, Decision Engine...

The **Policy Framework** enabler come from also as outcomes from Anastacia project. In the context of INSPIRE-5Gplus, Policy Framework will be extended to manage E2E Multi Domain security policies by refining HSPL-OP into MSPL-OP for each specific domain that once they are distributed the MSPL-OP will be translated into specific security configuration for asset configurations. All this process will be trigger proactively due to policy or SSLA definition, or reactively due to changes in the environment.

The **SFSBroker** enabler is a novel security enabler designed and developed for INSPIRE-5Gplus project. 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 which communicates with the network slice managers.

The **Secured Network Slice Manager** enabler aims to increase the security around the deployment of network slices. ... By interacting with the SSLA Manager and the Security Orchestrator developed in the INSPIRE-5GPlus context. It aims to coordinate the deployment of network slices with an associated SSLA and the Security Functions to fulfill it. In case the SSLA requirements are not satisfied, the Secured Network Slice Manager reacts to solve the pending issue.

The **Katana Slice Manager** is a central software component responsible for controlling all the devices comprising the network, providing an interface for creating, modifying, monitoring and deleting slices. It was developed in 5GENESIS and will be upgraded in the context of INSPIRE-5Gplus in the following ways: support of Moving Target Defense (MTD) enablers to enforce policies, Slice Telemetry extension to integrate with the Security Data Collector, monitoring of shareable network slices among different tenants/services, provision of integrity in the SBI for the controlled southbound components, and extension of the NEST/3GPP template to further support SSLA deployment.

3.2 Security orchestrator

3.2.1 Problem statement and challenges

Network paradigms such as SDN and NFV, and new technologies such as Cloud-native services and ZSM Zero Touch Network and Service Management focus on automate programmable and flexible networks in order to ease the deployment of new network services, features or to apply patches. This automation has not achieved sufficient capabilities to support these deployments while ensuring the security aspects of the infrastructure and communications. For this purpose, orchestration techniques are needed at each required level:

- Application level: deploy an application, for example following the Cloud-native paradigm;
- Network service level: ETSI-MANO VNF Orchestrators;
- Network topology: SDN controllers;

The various orchestration solutions used at different levels can be used to orchestrate and configure some types of security assets and properties but not all of them. These solutions show very rapidly their limitations in terms of VNF descriptors and capacities to handle security specificities, such as configurations based on security policies. This problem is even more complex in a multi-domain context.

This work relates to the Security Gap defined as “Automation and Zero-touch Service Management” listed in D2.1 Chapter 5.7 table. (Security Gaps)

3.2.2 State of the art analysis

[32] identifies 17 production-ready Multi-Cloud Management Platforms (MCMP). Out of the 17, only two of them reside in Europe, most of the others are US based companies. [32] focuses on COTS solution, but open-source initiatives like Open-Source MANO, ONAP (Open Network Automation Platform) or OPNFV (Open Platform for NFV) are also represented.

Those MCMP solutions have in common that they started as a way to leverage the IaaS features of underlying cloud infrastructure to deploy VM-based workload and services. However today, according to [33] as the microservices and cloud-native paradigm foster the FaaS architecture (Function as a Service), the previous Multi-Cloud Management Platforms need to evolve toward cloud-native and FaaS, which is not an easy task. For instance, Open-Source MANO latest versions 7 and 8 claim to support Kubernetes-based containerised deployment. However, it is mandatory to plug a VM-based VIM (Virtualised Infrastructure Manager) to OSM [34] to use Kubernetes workloads, which does not make sense if the Kubernetes cluster is not deployed in a VIM. This highlights the difficulty of adapting solutions to newer paradigms.

Among all these solutions, the orchestration of security features is rarely seen as a stand-alone feature: the focus is more on the security of the orchestration rather than the orchestration of security features. Another key aspect to consider is how to manage the configuration of all the different components that constitute an End-to-End service. These components are scattered across multiple domains, multiple locations, they are owned by several entities and they are of various different types and shapes: different vendors, different purposes, and different needs. However, in order to guaranty that the configuration of all these components enforces a homogeneous and coherent level of security, there is a strong need for the management of all the configuration snippets across all domains. On top of that, there are numerous formats for the configuration: [4] identifies 19 Cloud Modelling Languages, such as TOSCA and other Domain Specific Languages, for example:

- Cloudify’s Blueprint files;
- OSM’s VNFD Descriptor, NSD Network Service Descriptor and NST Network Slice Template;
- Kubernetes Objects;
- YANG data model

Configuration management of components that are distributed across multi-domain topology is something that orchestrator frameworks do not address directly and making this even more complicated when it comes to security configuration.

3.2.3 Solution description and advancements

Based on the state-of-the-art analysis, current orchestration solutions are generally provided by management platforms for clouds and networks, security consideration is currently focused on the security of orchestration, but not on the orchestration of security itself. Current solutions do not provide any specific descriptors for security and cannot handle fine grained configurations of security assets.

In H2020 ANASTACIA[37], a dedicated security orchestrator was proposed [139-140]. This orchestrator is responsible for transforming the security policy provided by a policy interpreter to a security enabler configuration. Although the orchestrator is involved in refining the policy and selecting the security enablers, its main role is deploying the security enabler and executing the final configuration. It also supervises the underlying infrastructure for any potential flaws. The security orchestrator supports a variety of security capabilities of different categories, namely: SDN security capabilities, NFV security capabilities, and IoT security controls. The current implementation supports ONOS SDN controller, OSM, and UMU's IoT controller service. The current implementation does not support a fully automated or a flexible selection process of security enablers. The advancements that are required for the security orchestrator and that will be covered in INSPIRE-5Gplus are the following:

- the ability to provide a holistic view on end-to-end security at a vertical level (for example security deployment and configuration at a network level, IT level or application level)
- fully automate the deployment control and configuration of all security functions in a highly dynamic environment
- the ability to interact with each level of orchestration according to the security orchestration needs
- Ability to align the security policies in an automated way inside of a domain and inter-domain context
- takes into account SSLAs to orchestrate security according security policies
- fully automate the selection of security services/VSFs to be orchestrated based on an automated catalogue.

3.2.4 Integration-interactions with HLA enablers

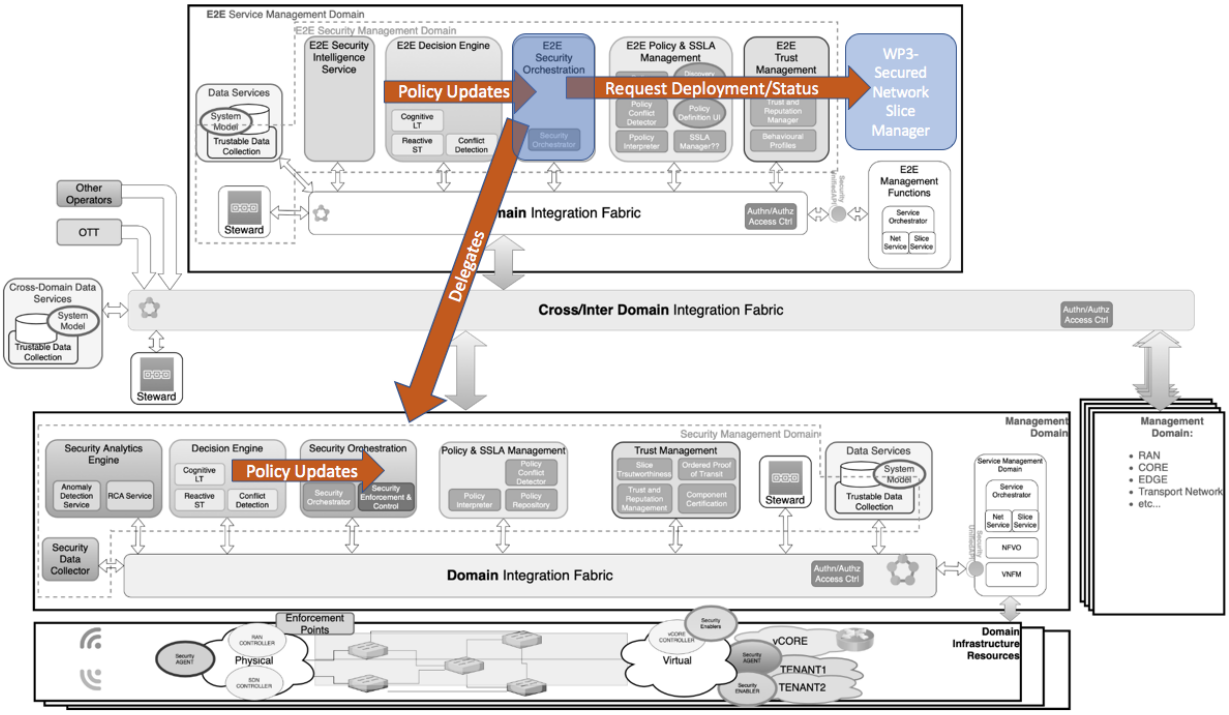


Figure 12. Integration of the security orchestrator in the HLA

As described in D2.2, the Security Orchestrator (SO) oversees the different security enablers to cover the security configuration requirements specified in the defined security policy. The SO drives the security management by interacting, through the integration fabric, with the different SDN controllers, NFV MANO and the security management services, such as the slice manager. The SO will enforce proactively or reactively the security policies through the allocation, chaining and configuration of virtual network security functions such as virtual Intrusion Detection System (vIDS), vFirewall, virtual Authentication, Authorization and Accounting (vAAA). The SO will be fed by the Decision Engine with new inferred security policies after any system evolvement or a new SSLA.

3.3 Threat assessment DiscØvery

3.3.1 Problem statement and challenges

5G networks are characterised by large-scale, interconnected infrastructure, dynamically virtualized assets, multiple stakeholders, and specific operational requirements. Assessing the security posture of such highly dynamic and complex systems requires us to rethink how we approach security. Traditional network security was based on exposing trusted components and services to authorised stakeholders. That approach encouraged strong external security mechanisms, but weak security mechanisms between trusted connections. In the current, networked environments, where the infrastructure and the borders of networks are fluid, the traditional security assessment techniques are no longer sufficient. Security analysts need to be able to have a holistic view of a network's connections.

Furthermore, a significant challenge is how to depict the assets and components of a network as close as possible to the assessment tool. Since 5G networks make use of virtual and dynamic components to improve their operational efficiency, having a consistent map of components is becoming more and more difficult. In today's world, everything is connected which results in significant security threats, such as threats towards confidentiality, authenticity, and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and 5G enabled networks. Security issues can result from the connectivity with legacy devices or devices that are inherently insecure. If that type of connection cannot be avoided, the stakeholders must be aware of the security risks. "Who must secure what?", is another important security issue, given the high number of people who are involved in a 5G network. During security analysis, the assets of the system are identified to prioritize the allocation of resources [38].

5G networks generate a large amount of data that is exchanged between different stakeholders (e.g., end-user devices, services, mobile networks, and application providers). The interconnected infrastructure of 5G networks leads to users losing the physical control of their data. To maintain data confidentiality, encryption has been the predominant mechanism used over the years. However, we note that IoT devices (e.g., the SE in the vehicles) may impose constraints on cryptographic algorithms because of limited computational resources[39]. This issue may be even more prominent given the low latency constraints of some use case scenarios described in D5.1 Definition of 5G security test cases, such as the Test Case 8: Security posture assessment and threat visualization of 5G networks. In Test Case 8, we use DiscØvery [130] to perform a threat assessment in a cross-border 5G application that promotes extended situation awareness by enabling vehicles and infrastructure to share the perception of the environment. In that specific scenario, we need to be able to assess the assets of our system during different operator jurisdictions, security configurations within specific operational requirements. The scale of 5G network, their interconnection to legacy infrastructure and devices, along with the increased number of stakeholders, increases the scope of threat assessment. To perform our assessment, we require tools that will enable us to reason about such distinct but connected systems.

3.3.2 State of the art analysis

With the changing threat environment, the cybersecurity needs of the future including the data that informs reports and controls the functionality of the 5G should be considered. Although not specific to information technology security, privacy, safety, authentication, and resilience provide contributions to information technology and cybersecurity. Evolutions in system security engineering approaches can aid in the reduction of the susceptibility of systems to a variety of simple, complex, and hybrid threats including physical and cyber-attacks, structural failures, natural disasters, and errors of omission and commission. One ongoing challenge is to reduce the susceptibility of systems to a variety of simple, complex, and hybrid threats including physical and cyber-attacks, structural failures, natural disasters, and errors of omission and commission. This reduction is accomplished by fundamentally understanding stakeholder protection needs and subsequently employing sound security design principles and concepts throughout the system life cycle processes.

The National Institute of Standards and Technology (NIST) organization developed a framework for cybersecurity. The framework can be used to design models of a system that complies with security standards. Security Requirements Engineering Process (SREP) used Common Criteria as a basis, trying to improve it by modernizing its components with policies for distributed networks and multiuser ownership. SREP is UML complaint, and the resulting security models evolve along with the development cycle of the product by performing some activities in each iteration step [40]. In [41] the authors propose a security framework that identifies security goals based on the assets of the system. From the security goal, the security requirements are derived, while they are validated using a process named satisfaction argument. Similarly, in [42] a framework is described that views security requirements from the agile development perspective while focusing on extreme programming. Microsoft's Trustworthy Computing Security Development Lifecycle (TCSDL) identifies security activities that take place in different stages in the development cycle. Compliance with standards is of high importance as are security requirements based on customer satisfaction [43], especially in industrial settings. A framework proposed in [44]suggests four steps in security analysis that should be performed by the developers instead of requirements engineers. Those are: (1) Identify the security environment and objectives; (2) Determine the threat model; (3) Choose a security policy that includes prioritizing according to the information's sensitivity; (4) Evaluate risk.

In summary, the presented works do not view networks in a holistic manner. They only aim to mitigate security issues in domain-specific areas. Accordingly, they cannot be used to offer a universal security analysis to any 5G relates scenario, but only aim to address particular instances of IoT systems. The ability to argue and reason about 5G security issues is necessary to address specific use cases. However, it is also necessary to be able to reason about 5G security holistically without hindering a security engineer[45].

3.3.3 Solution description and advancements

The process of threat assessment is used to analyse the security posture of 5G enabled networks. In the context of INSPIRE-5Gplus we use a security framework to design and analyse 5G systems using a model-driven approach. The threat identification assessment is based on system analysis and representation using a domain-specific language for INSPIRE-5Gplus. The domain-specific language is used to express systems in a way that facilitates reasoning about their security posture. A security engineer will be able to define assets of the system to protect, identify threats and vulnerabilities, get security insights on how to improve security and privacy, in a software aided analysis.

DiscØvery is a graphical security analysis tool for complex networking environments, such as 5G enabled networks. It leverages powerful state-of-the-art graph-based algorithms that support:

- Detecting network and system threats in complex distributed environments
- Remotely and automatically identifying hardware, software, and even policy-related vulnerabilities
- Provision of tailored reports (DiscØvery's cyber-insights), which are suggestions based on the unique characteristics of a system
- Visualising holistically the complete threat landscape, including the people, the systems, the networks, and the associated policies

The above innovations allow an organisation to:

- Reduce the attack surface of their infrastructure by identifying security issues that result from their hardware, software, network topologies, as well as in-house policies and interdependencies with third parties
- Reduce the cost of security monitoring by centralising the process

The DiscØvery tool provides a modelling language and analysis procedures for a system during the following engineering phases:

- design phase (model the idea of a system) [high-level concepts]
- implementation phase (model the implemented system) [low-level concepts]
- state diagrams (model the different states of a system)

Each phase has different concepts and rules on how those concepts interact with each other. The concepts of each phase are defined via UML class diagrams that in turn define the metamodels of the tool. The metamodels are translated into schemas that DiscØvery uses to validate models.

Using the properties of the domain-specific language’s metamodel, several automated processes can be performed through software tooling. Attributes in the metamodels&apos; concepts that take enumerated values can be used for providing security insights to the security engineer in an automated manner. Those insights can provide the security engineer with additional information about the security posture of the system by highlighting possible security issues of the system&apos;s configuration. The provided insights are independent of the security mechanisms or threats the security engineer has included in the model. For example, a system could have a connection that supports the TELNET protocol, which lacks encryption during data transmission. An insight could be to “use a secure transmission channel for wireless protocols that lack encryption”. The same insight would have been provided even if the security engineer had already added an encryption mechanism to the system. The reasoning behind this approach is that during the analysis stage, the security engineer should have as much information as possible to make informed decisions. The security insights are provided based on a high-level view of the security posture of the system and are independent of the system's implementation mechanisms. The effectiveness of the mechanisms is dependent on current best practices. For example, the DES encryption algorithm was considered a robust encryption algorithm during the first years of its implementation. Nowadays, it is regarded as an obsolete algorithm, and its use should be avoided. While assumptions on specific insights on which mechanisms are the best on the current model can be made, that does not necessarily mean that those mechanisms would be the best choice for the life cycle of the system. For the proposal of the mechanisms, the decision is up to the engineer.

During the INSPIRE-5Gplus project, the DiscØvery will be extended with 5G domain-specific cyber security insights. The insights are based on the work undertaken in WP2, specifically the D2.1 5G Security: Current Status and Future Trends and D2.2: Initial report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security. In D2.1 5G Security: Current Status and Future Trends we identified several limitation and gaps in existing security solutions for 5G. DiscØvery aims to address limitation in cyber threat intelligence and data sharing. One of the goals of the enabler is to allow a security analyst to move from a static threat assessment model with specific borders to a more dynamic border-less model. The deliverables included several security requirements that 5G networks need to be taken into account.

In D2.1 5G Security: Current Status and Future Trends, we defined the vertical domains of 5G applications. The domains were: 1) energy utilities; 2) vehicular communications; 3) enhanced content delivery; and 4) media production and delivery. In each vertical domain, we identified specific security requirements, such as low latency operation in the case of vehicular communications or high bandwidth in enhanced content delivery. Furthermore, we elicited several security requirements that impact all vertical domains of 5G. Those requirements were divided into the following categories: 1) subscriber authentication; 2) user privacy; 3) beyond hop-by-hop security; and 4) network security. Example of some of those requirements are, i) the 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system; and ii) the security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality. The requirements listed in the D2.1 and D2.2 will be added in the DiscØvery’s security insights library to provide security suggestions to security analysts of 5G networks.

Additionally, the cyber security insights will include, in addition to suggestions of security improvements, the identification of 5G specific threats and vulnerabilities depending on the specific configuration of the network. The threat identification for 5G with DiscØvery is based on the security threat taxonomy/ontology that was made in D2.1 5G Security: Current Status and Future Trends. The security threat taxonomy follows the same taxonomy as ENISA's threat taxonomy for 5G networks. The threats are classified based on their threat type such as eavesdropping, outages, or nefarious activity, and the location of the target 5G component such as, core network threats, or access network threats. Using that information, DiscØvery can visualize threats that impact specific components of 5G network models. DiscØvery enabler corresponds to D 2.1 security gaps as shown below.

Technology	Security Gap. Progress axis	DiscØvery enabler
Cyber threat intelligence and data sharing	Define the ad hoc usable sources for cyber threats to operators. Devise how to move from a static threat landscape to evolving or new threats. Consider the benefits of new risk assessment frameworks of complex ICT systems with notably the progress on risk assessment graph.	DiscØvery can allow a security analyst to assess networks and systems from a static analysis model to a dynamic borderless model. It can provide security suggestions specific to the network's configuration either directly on the enabler, or in the form of a report

3.3.4 Integration-interactions with HLA enablers

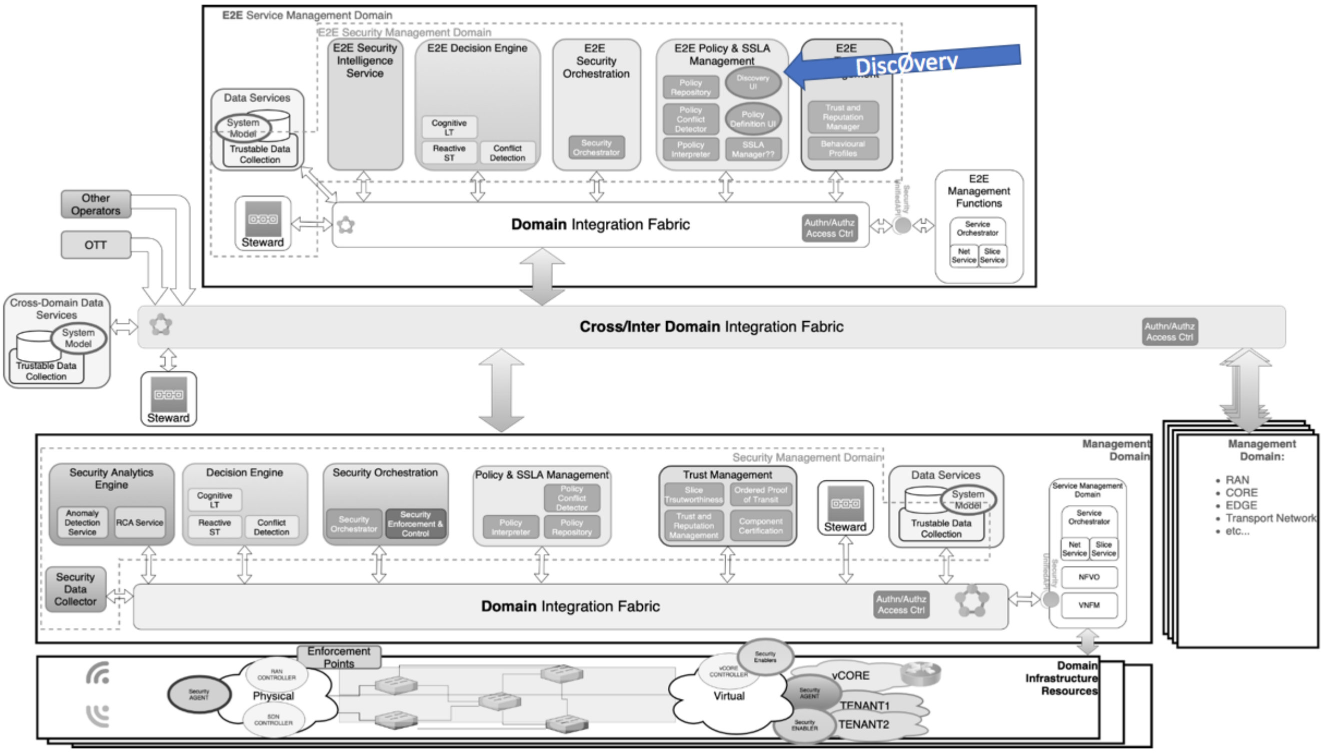


Figure 13. Integration of DiscØvery in the HLA

DiscØvery is part of the Policy & SLA management of the INSPIRE-5Gplus High-Level Architecture. As a results DiscØvery is an application directed to cyber security decision makers, such as security analysts. The outputs of the analysis will enable security analysts to better assess the security of their networks.

3.4 SSLA Manager

3.4.1 Problem statement and challenges

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 (SLAs) can play 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 (SPs) 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. This work relates to the Security Gap defined as “Automation and Zero-touch Service Management, SD-SEC and SECaaS, and Security Service Level Agreement” listed in D2.1 Chapter 5.7 table. (Security Gaps)

3.4.2 State of the art analysis

The SPECS [46]project aims at designing and implementing a framework for the management of the whole Service Level Agreement life cycle, intended to build applications (SPECS applications) whose security features are stated in and granted by a Security SLA.

Regarding the configuration of security requirements specified through SLA documents, a few proposal exist. Karjoth et al. [47]introduce the concept of Service-Oriented Assurance (SOAS), an assurance is a statement about the properties of a service as part of the SLA negotiation process. Smith et al. [48]present a WS-Agreement approach for a fine-grained security configuration mechanism to allow an optimization of application performance based on specific security requirements. Brandic et al. [49]presents a survey of the SLAs offered by commercial cloud providers.

3.4.3 Solution description and advancements

The objective is to provide a framework that manages the whole Security SLA lifecycle in a slice: a) it collects security requirements from verticals/end-users; b) deploys the security controls that are needed to enforce the agreed Security SLA by enriching the services of SPs or configuring them; c) monitors in real-time the fulfilment of Security SLAs d) detects violations in security provisioning level based on an analytics engine and notify both end-users and SPs; e) reacts in real-time to adapt the provided level of security or to apply proper countermeasures. In order to automate the Security SLA life cycle in a slice, a machine-readable format for Security SLAs will be adopted based on the SPECS Security SLA model that we will extend to support slicing. This model will be based on a WS-Agreement XML schema that will be extended with security-related information allowing to specify the following sections in a slice term description:

- Slice resource providers that describes the available infrastructure of the resource providers (appliances, networks, etc.);
- Security capabilities required in a slice. A capability is defined as a set of security controls. In our case, the NIST’s Control Framework [50] is used to specify these security controls;
- Security Metrics referenced in the slice service properties and used to define Security Service Level Objectives (SLOs) in the guarantee terms section. A metric specification includes

information about it and also information to process the SLOs, such as the metric name and definition, its scale of measurement, and the expression used to compute its value.

3.4.4 Integration-interactions with HLA enablers

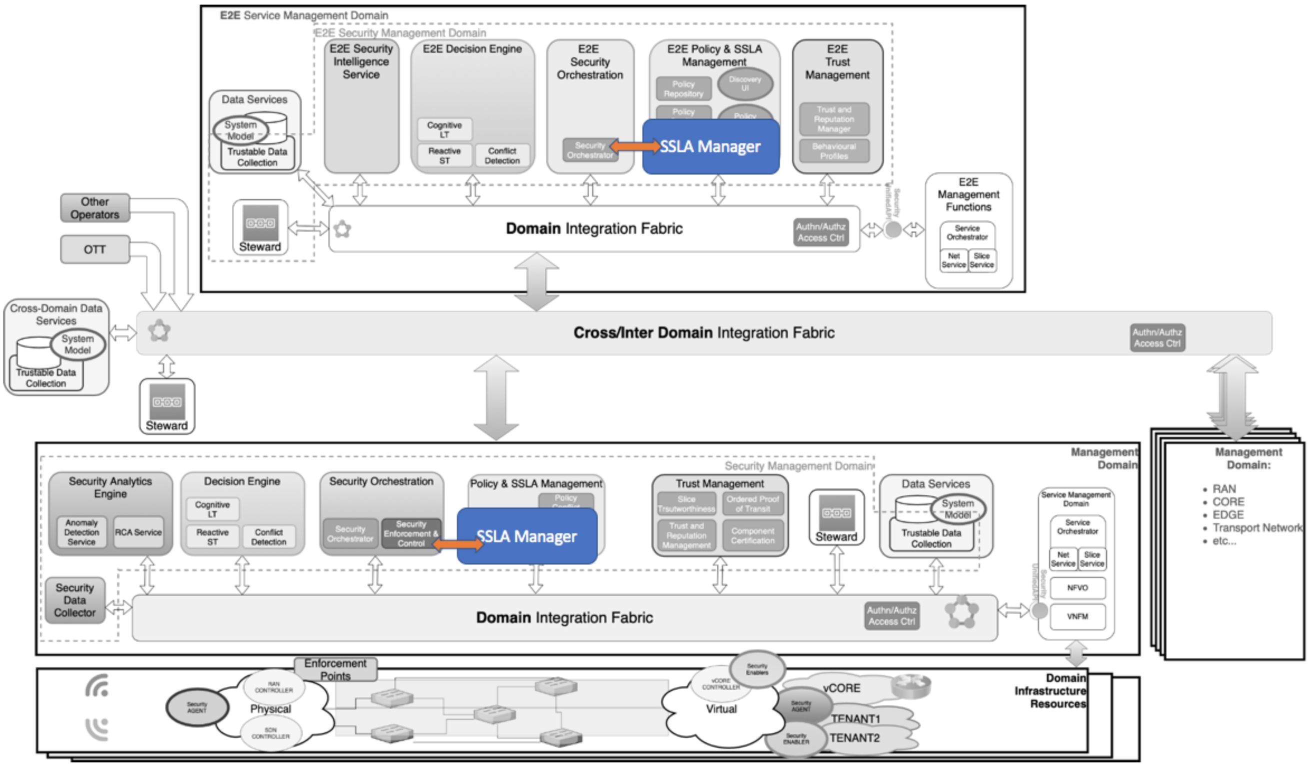


Figure 14. Integration of the SSLA manager with the HLA

The SSLA Manager makes available the SSLAs defined by the verticals mainly for the Security Orchestrators at the E2E domain or at local domain levels. These SSLAs can also be used by other management services and functions such as a slice manager.

3.5 Secured Network Slice for SSLAs

3.5.1 Problem statement and challenges

Network Slicing has been one of the most investigated and researched topics on the management of computing and networking resources when deploying services of the different existing verticals. Most of the work done up until now is focusing on how the resources are allocated or how to ensure expected Quality of Service (QoS) of the services deployed through the use of Service Level Agreements (SLAs). While the performance and monitoring of the services composing network slices has been (and still is) widely investigated, security on network slicing is an aspect that still needs a lot of research to be done.

The Secured Network Slice Manager relates to the specific Security Gaps identified in chapter 5.7 of deliverable 2.1 defined as: Automation and Zero-Touch Service Management. (Security Gaps)

3.5.2 State of the art analysis

Network Slicing aims to make use of the programmability of Software-Defined Networks (SDN) and the management of virtual elements defined in the ETSI Network Function Virtualisation (NVF). With these two elements (SDN/NFV), it is possible to create virtual networks specifically created and dedicated to a single service and so, to have a set of parallel virtual networks over the same physical infrastructure using the computing and networking resources available. As the idea of Network Slicing is to create a virtual infrastructure per each service, most of the work done on security in recent years is focused on how isolation may be applied at different layers [51]to protect from possible attacks as presented in[52]. In the context of the INSPIRE5G-plus project, we aim to look for the security of network slices from another point of view. Similarly to how QoS is validated and monitored at a Virtual Network Function (VNF) and a Network Service (NS) level, the objective of this enabler is to make use of SSLAs and monitor them at a Network Slice level. This enabler aims to ensure that a deployed network slice is secure and if an entity aims to attack a network slice, a response to solve the situation will be applied.

3.5.3 Solution description and advancements

The proposed solution is closely related with the previous INSPIRE5G-plus enabler, the SSLA Manager. The solution aims to make use of the SSLAs available in the SSLA manager and the Security Orchestrator to request the deployment of Network Slices with associated SSLAs and the necessary Security Functions (SFs) to fulfil them. Moreover, once the Network Slice is deployed this enabler will be in charge to receive the monitored data and evaluate/decide if the SSLA was violated and finally, if necessary, to trigger the procedure to apply a solution.

Based on the Network Slice Manager module within the NFV SONATA Service Platform software developed in the 5GTANGO project, we aim to improve it by developing an external module which is able to communicate with the SSLA Manager and the Security Orchestrator developed in INSPIRE-5GPlus. Some work with an initial architecture describing how the Secured Network Slice, the SSLA Manager and the Security Orchestrator should interact among them to apply SSLAs over deployed network slices was presented in[53]. In this conference paper, a first design and work-flows defining the relationship between Network Slices and SSLA were presented. Since then, this enabler had progressed on the design and initial implementation of a simple demonstration [54] based on the related test case 1 defined in D5.1 (Project Documents). This test case is focused on an automotive scenario. It deploys a Network Slice with a communication service and a set of SFs (e.g., firewall, Intrusion Detection System) and an associated SSLA. Once deployed, the traffic will be monitored and to identify when the SSLA is violated. This situation (i.e., SSLA violation) appears when a vehicle is not considered as benign. Then, the firewall is re-configured to block the specific traffic coming from the evil vehicle.

3.5.4 Integration-interactions with HLA enablers

As presented in the following figure, this enabler involves different HLA functionalities. First, it needs to deal with the SSLAs retrieved from the SSLA Manager (Policy & SSLA Management Functionality). Secondly, it will receive the information from the different SFs deployed for the security of a Network Slice (Security Analytics Engine Functionality) and finally, it will decide if an SSLA is violated and solution is necessary to be applied (Decision Engine Functionality). While its input data will come from different modules (i.e., OSS, SSLA Manager, etc.) its output information will be sent to the Security Orchestrator with the generation of the necessary policy to be applied.

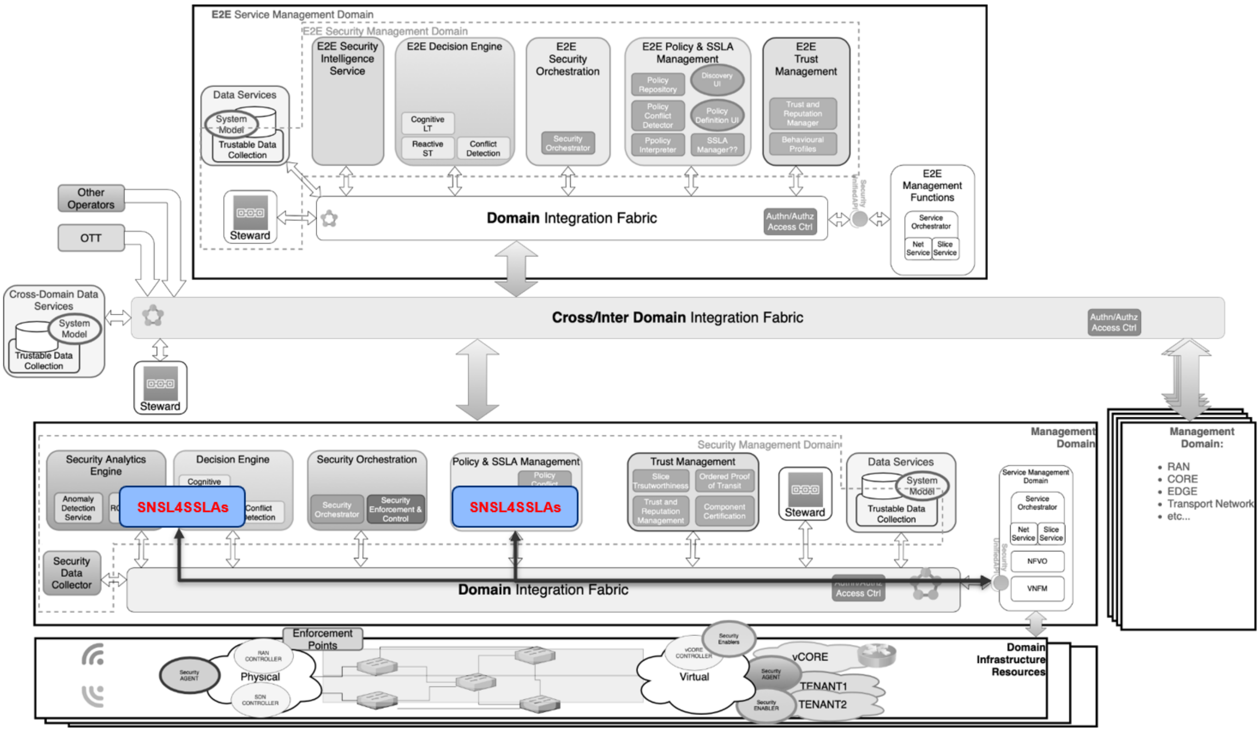


Figure 15. Integration of the Secured Network Slice for SSLAs

3.6 Policy Framework

3.6.1 Problem statement and challenges

5G infrastructure is characterized by multiple domains composed of different components and technologies and it makes use of SDN and NFV paradigms to provide as dynamic service deployments and dynamic network reconfiguration.

These dynamic actions to be implemented on the underlying infrastructure must be analysed, monitored and optimized, especially in terms of security, taking into account as much information as possible about the current status of the infrastructure to ensure the optimal sequence of actions and to avoid interferences with previously defined and established conditions. Security management has become a challenge due to the big amount of enforcement points as well as their heterogeneity, where conflicts and interferences during management activities are hard to amend. 5G architecture needs the capability to negotiate E2E security agreements between the different domains in a secured, optimized and automated infrastructure, consistent with the security requirements of the underlying components of each domain.

The Policy Framework enabler aims to cope with requirements related to the Security Gaps defined as “Multi MEC Security”, “Automation and Zero-touch Service Management”, “Security Service Level Agreement” listed in D2.1 Chapter 5.7 table.(Security Gaps)

3.6.2 State of the art analysis

Policies focus on abstracting layers complexity, easing the management, deployment and configuration of heterogeneous systems for different scopes. The inclusion of security requirements is one of the main concerns of policy related works, where multi-layer security complexity needs to be addressed in a comprehensive manner. In this context the enforcement of policies for different layers requirements becomes a need, where the network by itself can react to the environment conditions through the use of High-level policies (HSPL) previously defined, that are automatically translated into

Medium-level policies (MSPL), and these to concrete actions to the physical layer[55][56]. In fact, those models were extended to provide orchestration capabilities, priorities and dependencies management (HSPL-OP/MSPL-OP) [141-142]

Besides the complexity of the heterogeneous infrastructure, Manufactured Usage Description architecture (MUD) address the heterogeneity of potential devices by using Access List Control (ACL) that specify the necessary requirements of each device in form of policy in Yet Another Next Generation (YANG) and JavaScript Object Notation (JSON) format, well limiting the expected behaviour of devices to their intentions[58].

3.6.3 Solution description and advancements

Policy Framework provides orchestration of security policies at a high-level of abstraction, the orchestration includes the modelling, enforcement, priority and dependency of policies, as well as to gather information regarding the status of requested policies enforcement. The Policy Framework refines the High-level Security Policy Language (HSPL) defined in the E2E management domain into Medium-level Security Policy Language (MSPL) that are distributed to the different Management Domains and these to final security configurations for the different assets by selecting the best fitted implementation that deal with requirements using a modular plugin-based approach. The chain of actions is selected by priorities and dependencies avoiding conflicts with previously orchestrated policies. For this task, the Policy Framework includes a Policy Repository API that eases the traceability and management of security policies.

3.6.4 Interaction-Interactions with the HLA

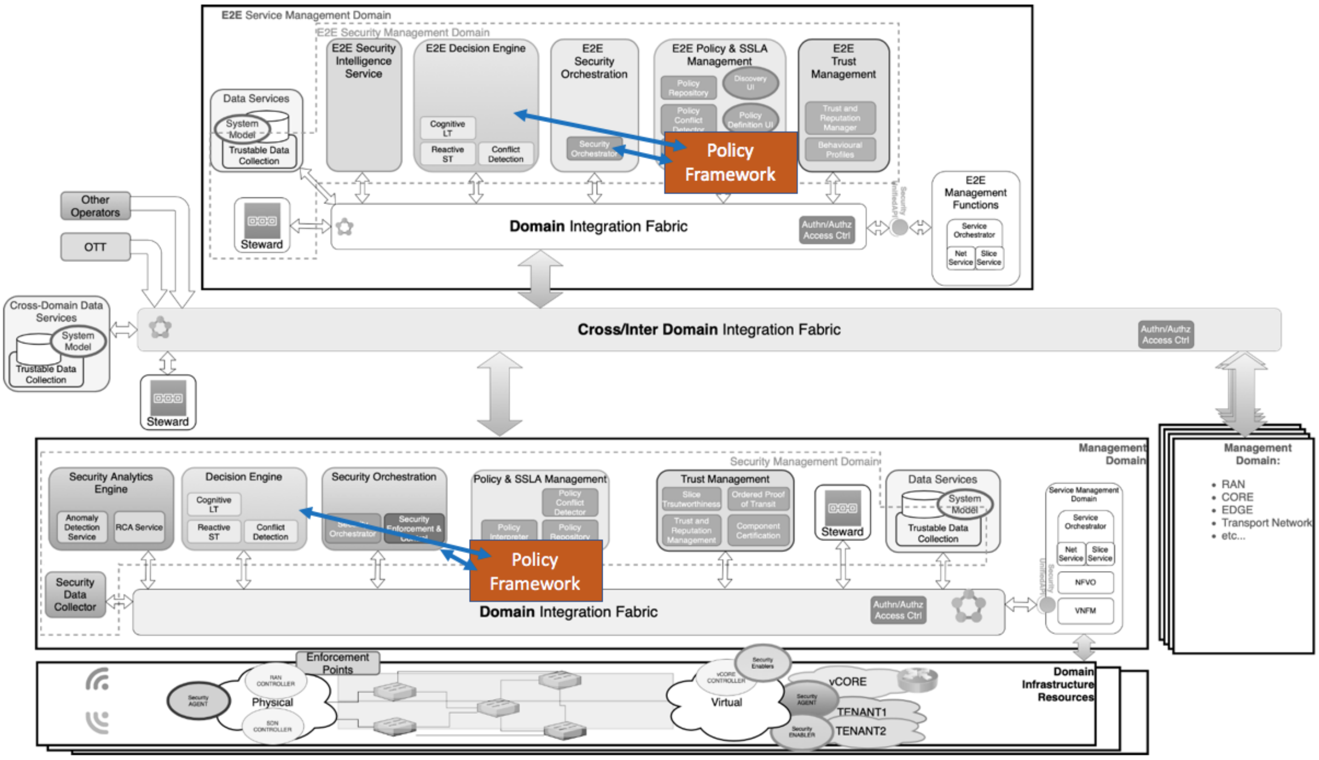


Figure 16. Integration of the Policy Orchestrator with the HLA

Policy Framework is positioned as an E2E management function for policies as well as for intra-domain management in INSPIRE-5Gplus High Level Architecture (HLA). It takes inputs from the Decision Engine and Security Orchestration and do the refinement and translation of the policies sending them to the Security Orchestrator.

3.7 SFSBroker

3.7.1 Problem statement and challenges

With the advent of the networking and computational services, the users may tend to lease networking and computational resources and data processing services from multiple service providers/operators. These may include larger scale mobile network operators, local 5G network operators, cloud service providers, etc. Local network operators may deploy their network infrastructure including both radio access and backhaul networks. A certain customer may request for a network slice that composed of resources offered by multiple operators. In such a scenario, a brokering mechanism that allows different service providers/operators to come to a common platform and formulate a network slice in a secure and automated way. The challenge is to evaluate the slice resource requirements against the resource availability over different network domains such as RAN, transport and core. Brokering mechanism should not be performed/hosted by a single entity. Which will be again become a centralized architecture. Therefore, using DLT for brokering mechanism will provide a good platform for distributed network architectures. The exploitation of DLT for a brokering mechanism relates to the identified Security Gaps listed in D2.1 Chapter 5.7 (Security Gaps). Accordingly, we intend to investigate the devised pragmatic paths to DLT usage over the networks over DDoS attacks, AAA and SLA management. However, when DLT is used, it needs to ensure the reduced latency as well as the easy implementation aspects.

3.7.2 State of the art analysis

The novel network slicing paradigm, made available by the latest developments on virtualization and softwarization technologies, enables advanced and dynamic resource allocation. The notion of the 5G Network Slice Broker has been introduced[59], which resides inside the infrastructure provider, detailing the required interfaces and functional enhancements for supporting on-demand multi-tenant mobile networks based on the latest 3GPP network sharing management architectures. The next generation networks are intended to use such brokering mechanisms for dynamic resource allocation without any human intervention. [60]. However, in the next generation networks, the role of network slice broker will be more advanced due to the interoperability of all sorts of networking services and computational operations offered by a wide range of service providers. Moreover, the business verticals or the clients will expect a more security, independence and autonomy to select the service providers.

We intend to use smart contracts with SFSBroker for security-oriented service level agreements (SSLAs) for local network operators and infrastructure providers running on a common platform.

3.7.3 Solution description and advancements

In this solution we intend to use a hierarchical Blockchain to develop a secure and privacy enabled federated network slice brokering mechanism (use the business model given in [59] under the umbrella of a multi operator platform. Secure and federated slice broker (SFSB) is an entity in charge of mediating between industry verticals' slice requests and the mobile infrastructure resource orchestrator. This mechanism uses smart contracts to allocate network resources offered by the multiple operators (i.e., Infrastructure Providers, mobile network operators, local network operators, computational resource providers, ...). Furthermore, it assigns and re-distributes the resources among end users in a secure, automated and scalable manner as in[60]. It is needed to perform privacy enabled, secured, dynamic and real-time resource allocation based on the users' requirements and the availability of resources at the service/resource providers. As identified in INSPIRE-5Gplus project, we target to use DLT over three key security aspects such as AAA (Authentication, Authorization and Accounting) and SSLA management, and mitigation of DDoS attacks. We intend to use dynamic profiling smart contracts and consensus algorithms with SFSBroker for managing security-oriented service level agreements (SSLAs) for local network operators and infrastructure providers running on a common platform. Through the dynamic profile status, the stakeholders are authorized to access the functions of SFSBroker. The smart contract decides whether the service requester grants access of the entire services or subset of the services based on the dynamic profile status. Through the smart contracts the authentication and access control to the SFSBroker functions enforced to the IoT tenants and service providers. Furthermore, the immutable decentralized ledger of the blockchain ensures accountability on the service access operations performed by IoT tenants and service providers.

3.7.4 Integration-interactions with HLA enablers

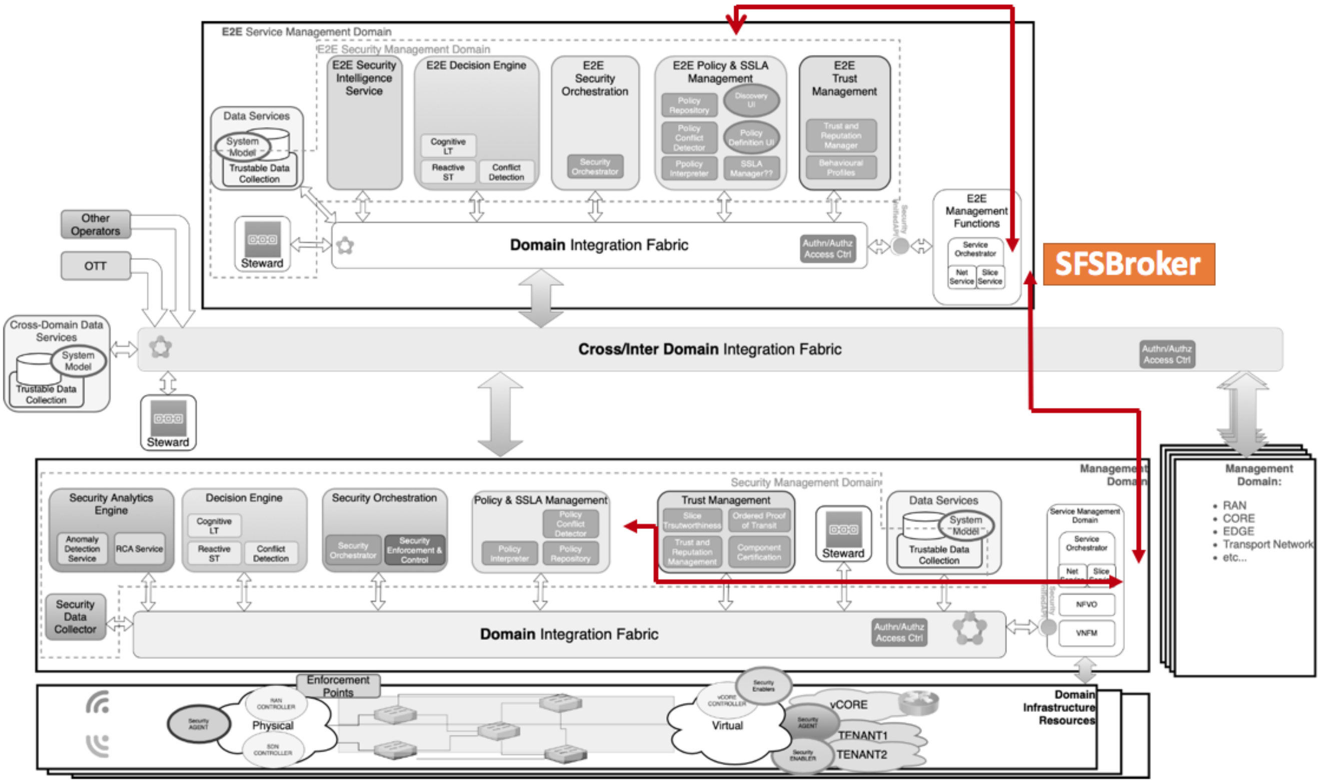


Figure 17. Integration of the SFSBroker in the HLA

SFSBroker can be positioned as an E2E management function for slice service in INSPIRE-5Gplus High Level Architecture (HLA). SFSBroker should take inputs from the SSLA manager to update the reputation index of the different operators/service providers. For slice creation process, it should also communicate with the network slice manager which is located in the service management domain.

3.8 Katana Slice Manager

3.8.1 Problem statement and challenges

With the advent of 5G technology one of the most innovative and promising features was the ability to utilize the deployed infrastructure and through virtualization and softwarisation to allow for the deployment of multiple concurrent services implementing the "one to fit all" principle. In this context the main challenges of network slice management in relation to the focus area of INSPIRE5G-Plus is during the deployment and provision times (i.e., time zero) the secure isolation of the network slices utilised by different services/verticals, the continuous monitoring of this isolation and the perseverance of isolation in case of events. Since network slicing by default includes various administration and technology domains i.e., core and edge cloud, 5G Core and RAN, the appropriate provision of resources in each domain as well as the mechanisms to enforce and monitor isolation may become too complex. The solution that will be developed in the frame of INSPIRE5G-Plus will extend the current Katana Slice Manager capabilities and will cooperate on additional services that the project will develop and integrate.

The considered improvement on KATANA slice management relates to Security Gaps referred as: *Automation and Zero-touch Service Management* in the Security Gaps table of Chapter 5.7 of the deliverable D2.1 (Security Gaps)

3.8.2 State of the art analysis

Network Slicing emerges as a key technology for new softwarized networks, including 5G, it also raises security concerns because of the impact that a vulnerability may have in such scenarios[61]. Prominent bodies, such as NGMN, issued recommendations for Network Slicing security in 5G [62], which aided the identification of threats in the general packet core. Recommendations in underlying technologies were also considered, such as ETSI's for NFV[63], which surveys the potential areas of security concern across the VNF life-cycle. In addition, 3GPP has released document TR33.811 study of Network Slicing security for 5G [64].

Because slicing builds atop other technologies, there are known security challenges attributed to the underlying SDN and NFV technologies, as well as the access networks. Cunha et al.[61] summarizes the main challenges that Network Slicing has to overcome wrt security due to the technologies the network slicing operates upon. The main security threats that affect Network Slicing are:

- Monitor SB/NB Interfaces – steal configuration, detect vulnerabilities, map system topology
- Inject traffic into management and control interfaces - make system unavailable/unmanageable
- Impersonation of either the Slice Manager or the south bound systems
- Compromise of NF running at control plane
- Shared network slices compromise (side channel attack e.g.
- Compromised end devices

Within INSPIRE5G-Plus, it is anticipated that some of these attacks will be tackled in defined Test Cases and remediation will be automated via integration with security enablers and INSPIRE5G architecture.

3.8.3 Solution description and advancements

The solution will be based on the already available implementation of Network Slice Manager being developed in the frame of 5GENESIS project [65] named KATANA[66]. The KATANA is based on a highly modular architecture, built as a mess of microservices, each of which is running on a docker container. The key advantages of this architectural approach are that it offers simplicity in building and maintaining applications, flexibility, and scalability, while the containerized approach makes the applications independent of the underlying system. At the current version the KATANA slice manager is more oriented on the deployment and operational features of the network slicing. In the frame of INSPIRE5G-Plus the advancement will focus on the support of security features and integration with INSPIRE5G-Plus platform components. Briefly the following advancements are considered:

- Generalisation of NEST/GST 3GPP template in order to introduce the required for the deployment SSLA technical specifications
- Slice Mapping and Scheduling components of KATANA extension to support for Moving Target Defence
- Extension of Slice Telemetry in order to integrate with the Sec Data Collector (SDC)
- Extension of SBI in order to provide integrity for the controlled southbound components.
- Monitoring mechanisms for network slices that are being shared among different tenants/services.

3.8.4 Integration-interactions with HLA enablers

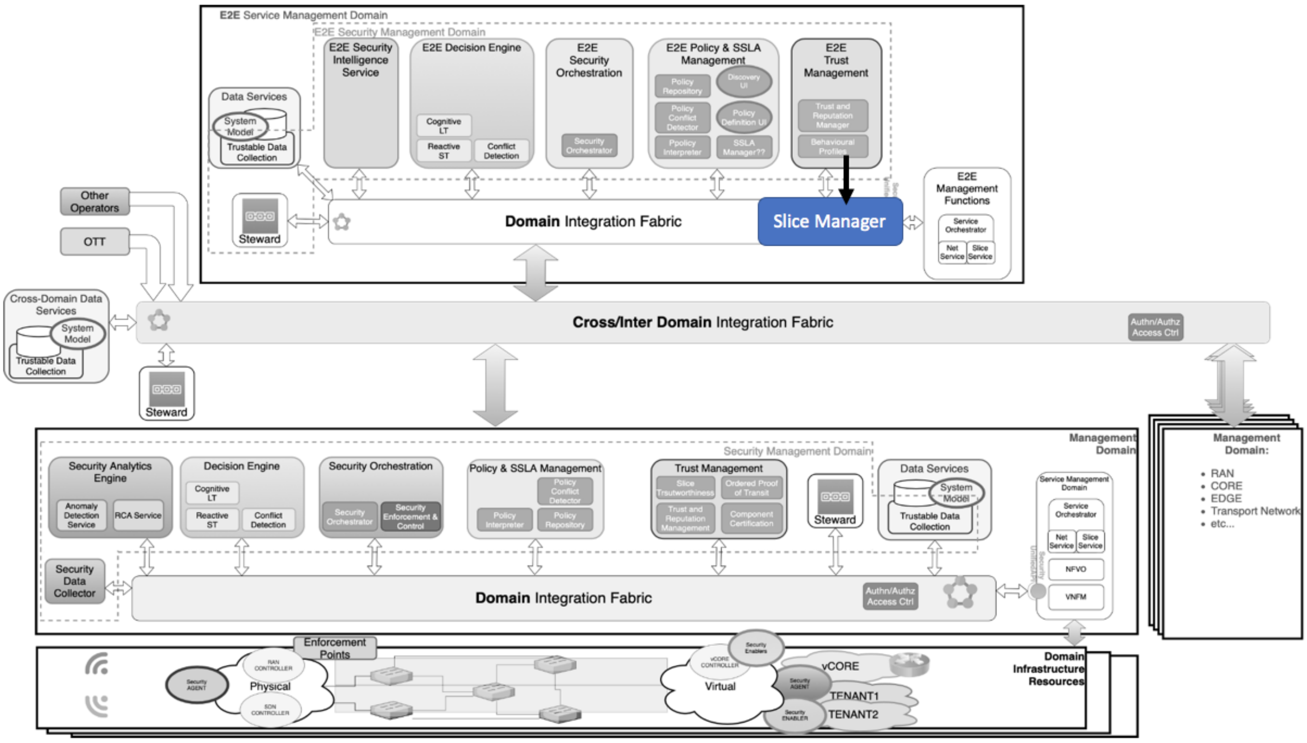


Figure 18. Integration of Katana slice manager in the HLA

The Katana Slice Manager belongs to the E2E Service Management Domain of the HLA. It receives the Generic Network Slice Template by the Service Orchestrator for creating the network slices and provides the API for managing and monitoring them. The Slice Manager communicates with the NFVO, the EMS, the VIM and the WIM in order to manage the network functions in the infrastructure.

3.9 Baseline assets used in the project

The following assets will be used by partners as baseline assets in the development of their enablers:

- WIM T-API (CTTC) resulted from 5G-TANGO project: Plugin within the SONATA Service Platform (SP) that allows to communicate with an SDN Controller based on Transport API.
- SONATA multi mano service platform (CTTC), developed in 5G-TANGO project: SONATA SP module in charge to deploy Network Services (NSs) and their Virtual Network Functions (VNFs) over any associated NVFI either using kernel-Virtual Machine (kVM) or container technologies such as OpenStack or Kubernetes.
- SONATA VNF V&V tool (CTTC), developed in 5G-TANGO project: SONATA Validation & Verification (V&V) module in charge to test NSs and VNFs before they could be uploaded to the SP and be used in production scenarios.
- WAN Infrastructure Manager (NCSRD) developed in 5GENESIS project: A custom open-source implementation to operate on SDN networks, interacting with the *OpenDayLight* Controller. It is a Python dockerized application.
- OSM implementation (NCSRD), resulting from 5GENESIS project: OSM is the Network Management and Orchestration by ETSI.
- Policy Based Security Manager (NCSRD), resulting from SHIELD project: The Policy Based Security Manager imposes policies based on the findings of IDSs.

- Virtualised and Physical infrastructure telemetry (NCSRD), resulting from SHIELD project: Several types of monitoring probes plugged on physical or virtualized infrastructure. All captured records are sent to the E2E Monitoring Framework, providing an overall overview of the network.
- ONOS Flows and intents (UMU), resulting from ANASTACIA project: Enables flow and intent forwarding installation on ONOS via Northbound interface.

4 Security Enforcement and Control

4.1 Introduction

5G comes along with new infrastructure and verticals where the heterogeneity of technologies has become challenging. The access technologies and the novel typology of devices lead into an increased attack surface that requires a flexible infrastructure capable of deploying services as close as possible to devices to ensure the correct behaviour with a negligible impact on performance. The following enablers are presented to support 5G infrastructure as Network Security Functions, designed using Network Function Virtualization (NFV) and Software Defined Networks (SDN) paradigms to be dynamically deployed and configured at the edge of the network, customizing their behaviour to the heterogeneity of device requirements, ensuring the security of communications; from access and authentication to transport, especially to constrained devices that are not able of computationally execute securization algorithms.

Given the highly dense scenarios characterized by the heterogeneity and mobility of the devices, 5G Inspire efforts focus on automating and optimizing responses to volatile conditions close to the source to ensure secure communications. In this context, the **following enablers** are dynamically deployed when required to ensure security aspects of devices accordantly with its requirements dealing with the heterogeneity of 5G scenarios.

vAAA enables a flexible and scalable authentication method based on device requirements, that could potentially deploy lightweight and space-efficient authentication for highly dense V2X environments. The securization and privatization of the communication channel is done by the deployment of proxies to whom the computation of security procedures is delegated. The behaviour and location of these proxies depend on devices capabilities and network constraints, while **DTLS proxy** is distinguished by UDP encryption per-packet which is desirable for mobility, it is constrained to application layer. IPsec proxy on the other hand, gives flexibility and abstraction to the application as it is deployed at the network layer; this is really useful in multi-tenancy scenarios where traffic must travel over third-party networks. On the other hand, **CP-ABE proxy** is deployed for privacy purposes.

The availability is one of the main concerns of 5G, particularly in mission-critical situations, where Drones among other UAVs will play a principal role to deploy the infrastructure needed for the establishment of services. This UAV heavily rely on its positioning, where GPS is the principal method due to its global coverage and accuracy. GPS metrics are especially vulnerable to spoofing attacks which nowadays are easy to perform due to Software Defined Radio based tools. This vulnerability is addressed by deploying **UAV anti GPS spoofing enabler** which makes use of RSSI indicators from trustable sources to infer UAVs position whereby detecting possible spoofing attacks. In this constantly moving environment where the attack surface has strongly increased, sophisticated permanent context monitoring is required to intelligently detect and amend the security of compromised communication or QoS. **OptSFC** offers an intelligent control and decision scheme based on Reinforcement Learning that provides intelligence to the network and optimizes the protection gain / deployment cost trade-off.

vAAA, **DLTS proxy** and **CP-ABE** come from research community as outcomes from Anastacia project, a cybersecurity framework that provides self-protection, self-healing and self-repair capabilities through dynamic orchestration and deployment of policies and actions, in the context of Inspire these AAA and proxying techniques will be employed to trigger device specific or user related actions and to protect communications respectively. **I2NSF IPsec proxy** is an IETF proposal that will enable the provision of secure tunneling for multitenancy and will be instantiated via the Security Orchestration of Inspire-5GPlus on Policy definition. **Lightweight and space-efficient authentication** constitutes an enabler introduced for the first time in the context of INSPIRE-5Gplus and expected to be entirely developed during the project duration. UAV anti GPS spoofing is also a new enabler that is introduced for the first time in the context of INSPIRE-5gplus and is envisioned to be entirely developed during the project duration. Similarly, **OptSFC** is being developed as a totally new security asset as part of INSPIRE-5Gplus. It will closely interwork with **MOTDEC** enabler for MTD related security scenarios.

4.2 VAAA

4.2.1 Problem statement and challenges

5G infrastructures provide connectivity and services to a wide amount of heterogeneous devices and technologies. While this heterogeneity enriches our lives in multiple ways, it is important to pay special attention to security. In fact, proper management of essential security fundamentals, such as Authentication, Authorisation and Accounting (AAA), can be a challenge considering different requirements, protocols and restrictions of the devices. Each device accessing the network should perform a bootstrapping process according to their capabilities and specifications which can differ significatively, and this process should be as fast as possible, avoiding overloads in authentication services.

In this regard, 5G properties like dynamic virtualization and softwarization of network functions can contribute to mitigate issues like heterogeneity and scalability. For instance, Fog computing can provide dynamic deployments of virtual network functions (VNF) at the edge by leveraging NFV (Network Function Virtualization) and SDN (Software Defined Networks). By using these techniques, it is possible deliver virtual security appliances in the edge and remote cloud data centres when required. In this context, vAAA Network Security Function (NSF) could be timely and dynamically deployed and configured at the edge in virtualized and softwarized fog entities, in order to facilitate the security management of heterogeneous networks. This work relates to the Security Gap defined as "ZSM, Authentication and MEC security" listed in D2.1 Chapter 5.7 table.(Security Gaps)

4.2.2 State of the art analysis

Beyond regular devices able to implement different protocols for accessing the network, other kind of devices such as the most constrained one requires special attention to this point. For instance, Kanda et al [68] discussed about the applicability of Protocol for Carrying Authentication for Network (PANA) in constraint environments. They also provide a possible extension to this purpose. In addition, in this topic, Garcia-Carrillo [70] provided a survey of different IoT bootstrapping techniques, also proposing a solution for CoAP + EAP which was compared with PANA. Besides, they provided a low-overhead version (LO-CoAP-EAP) of the previous work for LP-WAN infrastructures[70].

Regarding the applicability of virtual AAA in 5G infrastructures, Wong et al.[72] presented a theoretical approach for integrating a hierarchical and distributed approach on fifth-generation systems. The design is based on ETSI NFV standards. Han et al. [73]also provided a theoretical design, this time for the so-called Trust Zone, a security solution designed as an enhancement of the 5G AAA in the edge cloud. Considering previous works, Zarca et al. [74] provided the design, implementation and validation of an infrastructure for managing bootstrapping processes through vAAA security functions for constraint devices, based on NFV, SDN and orchestration features, key points in 5G environments.

In the line of cryptomaterial generation, the 3GPP has defined the AKMA (Authentication and Key Agreement for Applications) to be part of Release 16, that provides with a mechanism to generate cryptographic material for Services to be run between the UE and other entities. [75][76].

4.2.3 Solution description and advancements

AAA infrastructures virtualization, as well as the virtualization of part of them, such as the authentication agent, will allow providing dynamically different authentication agent implementations depending on the authentication requests observed in the 5G network. Thus, new specific authentication agents can be deployed at the edge dynamically according to the observed requirements for providing specific network authentication protocols as near as possible of the source of the authentication request. The solution also can be deployed for avoiding overloads in existing AAA services. These network monitoring and dynamic deployment features rely on NFV and SDN infrastructure. Thus, the solution provides scalability to bootstrapping process as well as it deals with devices heterogeneity. This asset is commonly used as part of the bootstrapping process which can be also enhanced with channel protection/privacy by default properties provided by other assets. In that line, being able to integrate ACMA as a Virtual Network Function is a desirable enhancement to reduce the need to authenticate for each service run on top of the 5G network, in particular communications directed to elements that may be already part of a VNF that is located within the ISP premises, such as the network EDGE.

4.2.4 Integration-interactions with HLA enablers

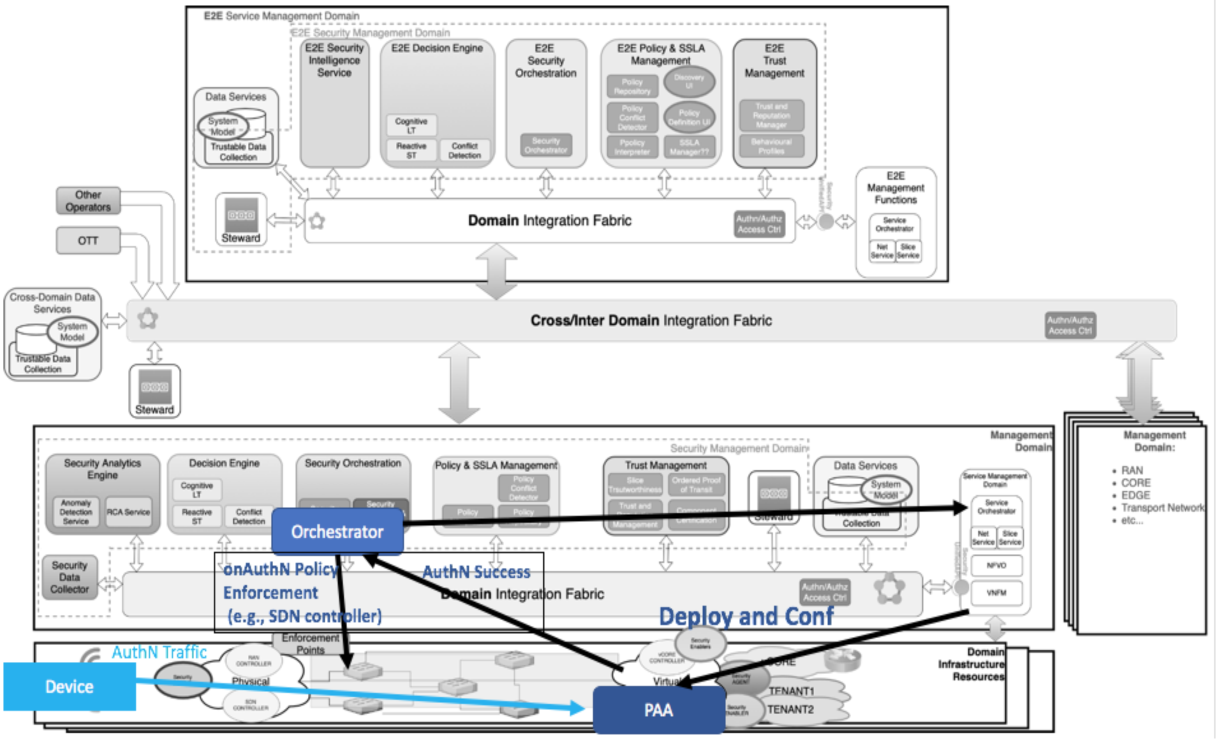


Figure 19. vAAA integration in the HLA

vAAA is an on-demand enabler, instantiated by the Service Management Domain when required from the Security Orchestrator. It ensures the most appropriate authentication method for a device access request based on device constraints.

4.3 OptSFC

4.3.1 Problem statement and challenges

Large scale networks are increasingly oriented towards computing at the edge and Multi-access Edge Computing (MEC), which enables local data storage and computation within a distributed and large-scale system. MEC enhances distributed systems performance by reducing communication latency compared to systems heavily relying on Cloud resources. However, this increases the importance of edge nodes within the system, and as they have low computational power, they are appealing targets to attackers who can perform attacks relatively easier, compared to big clouds that can perform effective attack recognition and mitigation. Therefore, edge devices must be secured by means that take into consideration their low computational power, as well as their power consumption constraints and the difficulty to manage them. The optimization of effective security solutions in such an environment becomes a key point.

A more global and pressing requirement for future networks is the need to minimize the energy consumption and complexity of ICT for green systems. On the cybersecurity front, this calls for resource-efficient defense (i.e., frugality and efficiency) even the resources are readily available in a computing & communication environment unlike edge computing or power-limited systems. This paradigm also has an economical aspect, namely minimization of OPEX/CAPEX for ICT system operators. Considering the trends on green security and requirements on resource-constrained network elements, efficient management of security function configuration, composition and resource allocation are crucial for future networks. However, this is not a trivial task since these systems are complex and hard to model appropriately. Moreover, the performance requirements for such schemes are challenging. There are also practical issues such as how to integrate them into practical 5G (and Beyond) security management frameworks. This work relates to the Security Gaps defined as “Artificial Intelligence and Machine Learning”, “Automation and Zero-touch Service Management” and “MEC Security” listed in D2.1 Chapter 5.7 table.(Security Gaps)

4.3.2 State of the art analysis

The optimization problems stated above can be addressed using AI/ML optimization techniques like Reinforcement Learning (RL). Reinforcement Learning (RL) is a process where an agent learns how to behave, and which actions to perform, based on a defined environment[77]. The agent obtains a reward/penalty when performing a specific action, in a specific state, and at a specific time. The aim of the agent then, is to maximize the return (i.e., to reach optimality), that is the sum of rewards he obtains during his interaction with the environment. During the learning process, the agent will define a policy to follow that allows him to achieve such goal. RL is based on the Markov Decision Process (MDP), which can use Model-free approaches like Q-learning (using Q-values, or Bellman Optimality), in order to find the optimal policy.

However, when applied to complex systems, the learning phase can be very inefficient, requiring a considerable amount of time before reaching optimality. Deep Q-learning (DQL[78] which approximate the Q-values using Deep Neural Networks (DNN), can overcome this issue and enables a complete exploration minimizing the approximation loss of DNN.

The DQL’s exploration can be efficiently narrowed using Game Theory Models to build an adversarial environment closer to the real-life scenario, where a defender is opposing an attacker. In such models the optimal policy is translated to a Nash Equilibria, where both agents cannot increase their reward. Different versions of DQL has been implemented and tested to increase its efficiency: Double DQL (DDQL), Prioritized DDQL, Dueling DDQL, Distributional DQL, Noisy Nets, or a combination of the mentioned versions (e.g., the Rainbow algorithm from DeepMind[79]).

Although RL has been applied to various learning problems in computation and decision problems, its application to cybersecurity optimization is still limited. Moreover, how its integration in a security management framework in 5G networks can be implemented is not explored in detail.

4.3.3 Solution description and advancements

Considering these requirements and challenges, OptSFC will implement smart control and decision schemes for optimizing protection gain vs. security function cost trade-off cost for cyber-defense. Specifically, it will utilize Reinforcement Learning (RL) as an enabler that allow the optimization of the resource usage and power consumption in 5G network elements/devices during functional operations and non-functional ones, like the detection and mitigation of cyber-attacks. It will provide this function as a service to the MTD module MOTDEC through open and simple APIs as shown in Figure 20.

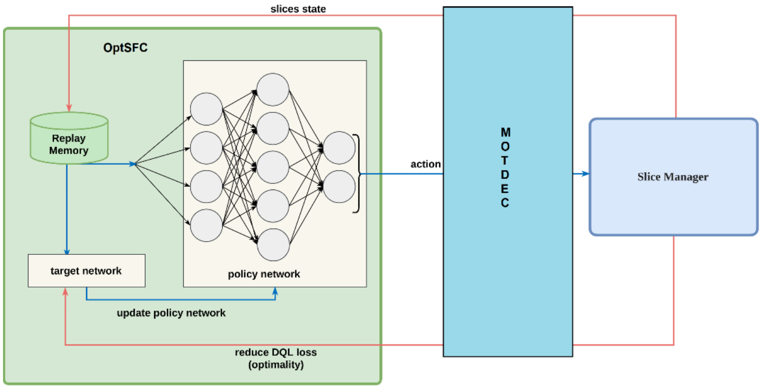


Figure 20. OptSFC and operation with MOTDEC module for slice protection.

In OptSFC, RL will be used to train the cognitive models for different components, like the MTD, which will use a tuned DQL algorithm and narrowed to a Game Theory model. This will enable the possibility to investigate on the usage of Neural Fictitious Self-Play (NFPS) [80]to create a Red Team/Blue Team camp where the two agents (the MOTDEC and the attacker in the MTD case) are autonomously learning without predefined knowledge. In that regard, OptSFC will come up with a new DQL based ML model for our specific use-case as a new enabler in INSPIRE-5Gplus project. It will also entail the potential for further advancements with additional AI/ML models to be embedded and more 5G security use-cases to be addressed in the future.

4.3.4 Integration-interactions with HLA enablers

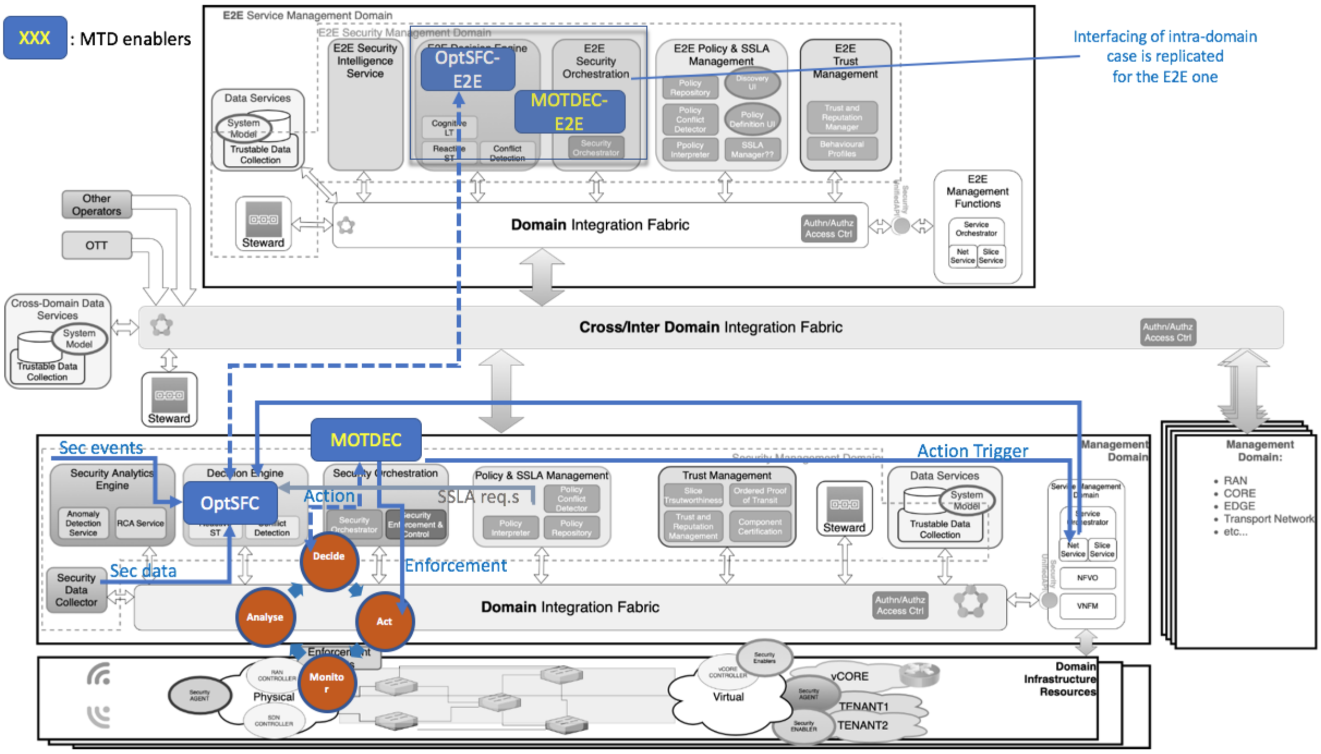


Figure 21. OptSFC (and MOTDEC) embedded in the INSPIRE-5Gplus security architecture

OptSFC controls MOTDEC actions to realize the smart MTD schemes in the protected network environment. It can optimize and steer MTD policies based on embedded models and cognitive functions. Please note that although the interactions between different INSPIRE-5Gplus functional blocks and OptSFC are shown as direct arrows, the actual information exchange occurs over the integration fabric.

4.4 Lightweight and Space-efficient Authentication

4.4.1 Problem statement and challenges

With the increasing level of driving automation in 5G-enabled vehicular use cases, vehicle-to-everything (V2X) communication becomes highly vulnerable to malicious actors, opening up entirely new questions from a security and privacy perspective that have not been addressed in a similar context before. The 5G authentication and key agreement (5G-AKA) constitutes one of the fundamental procedures for mutual authentication between each vehicle and the network and provides keying material that can be used in subsequent security procedures[81]. However, in highly dense vehicular scenarios, the excessive signalling overhead required for security context establishment in 5G-AKA may result in increased latency beyond the acceptable levels. This is especially important for i) mission-critical V2X use cases, e.g., road safety, where vehicle authentication should have minimum impact on the actual communication, and ii) roaming scenarios, where the signalling between the serving and the home network domains may introduce non-negligible latency.

In addition, authenticated vehicles may exhibit misbehaviour at any time instant after having been successfully authenticated. In particular, an already authenticated vehicle may be able to intentionally transmit false kinematic information (e.g., position, speed, acceleration, heading data) in its broadcast messages and cause disruption in the network which may in turn generate safety issues on the traffic. Seemingly abnormal vehicular activity originated from malicious actors (e.g., vehicles) may take the form of highly sophisticated attacks. Thus, real-time attack identification (detection and localization) becomes essential for mission-critical V2X services and should not come at the expense of the actual network performance (i.e., stringent latency constraints).

In direct alignment with the identified security gaps in WP2 Deliverable D2.1 Chapter 5.7 (Security Gaps), the proposed enabler provides security enhancements at vertical level, e.g., cooperative, connected, and automated mobility (CCAM) scenarios, while aiming to address authentication vulnerabilities and performance limitations in the 5G radio access.

4.4.2 State of the art analysis

Several vehicle authentication protocols have been recently proposed in the literature for mutual authentication among the involved network entities[82]. Group-based AKA approaches, e.g., [83], allow the serving network to authenticate clusters of vehicles and reduce the message exchanges with the home network. However, the dynamic V2X network topologies result in frequent local signalling for cluster formulation and head selection which may prove harmful for the V2X data exchange when the vehicle density exceeds a certain level. On the other hand, lightweight authentication protocols, e.g., [84], may reduce the required computation cost at the expense of a higher communication overhead in terms of required size of the exchanged messages.

Regarding the timely detection of internal malicious actors (e.g., vehicles), the vehicular public key infrastructure is only capable of protecting the network against external attackers by ensuring message integrity but with no guarantees on the semantic correctness of each message. A misbehaviour detection mechanism is deemed necessary to detect anomalous behaviour pertaining to vehicle dynamics. Unforeseen changes in traffic (e.g., due to either naturally drifting mobility patterns or unpredicted malicious activity patterns) in conjunction with insufficient training data, generally pose significant challenges (e.g., model overfitting) to conventional deep-learning-based attack identification methods. Instead, the investigation of mobility model-agnostic approaches poses merit in the absence of prior knowledge associated with physical traffic phenomena.

4.4.3 Solution description and advancements

Motivated by the aforementioned literature gaps, we introduce a novel vehicle authentication mechanism aiming to extend the 5G-AKA procedure and address highly dense V2X connectivity scenarios [85]. Our proposed scheme inherits the space-efficient advantages of a cuckoo filter implementation, i.e., a probabilistic data structure for approximate set membership tests, and allows for the authentication of multiple vehicles at a time with controllable false positive rates. An in-depth performance analysis of our vehicle authentication scheme reveals the impact of different filter configurations for varying vehicle load. In particular, a properly designed cuckoo filter can significantly improve the authentication efficiency and outperforms the standardized 5G-AKA scheme in terms of end-to-end latency and protocol overhead even for high vehicle load. In addition, the introduced space cost remains close to the information-theoretic lower bound even for stringent false positive rate requirements. Detailed performance analysis and results are provided in[85].

Ongoing work aims to enhance the proposed mechanism with a lightweight and online attack identification scheme for the detection of vehicles that were already authenticated but exhibit misbehaviour at a later stage. The mechanism relies on the processing of streaming vehicular data reports and the exploitation of spatio-temporal cross-correlations to extract the underlying vehicle dynamics. The processing of observed measurements reveals insights for the behaviour of communicating vehicle streams and allows the real-time identification (detection and localization) of malicious attacks, by post-processing the error sequence which occurs after subtracting the predicted data sequence from the actually observed data sequence during a prediction window. The intuitive idea is that if there is a misbehaving vehicle during the prediction window, then it should leave certain anomalous signature within the error sequence.

4.4.4 Integration-interactions with HLA enablers

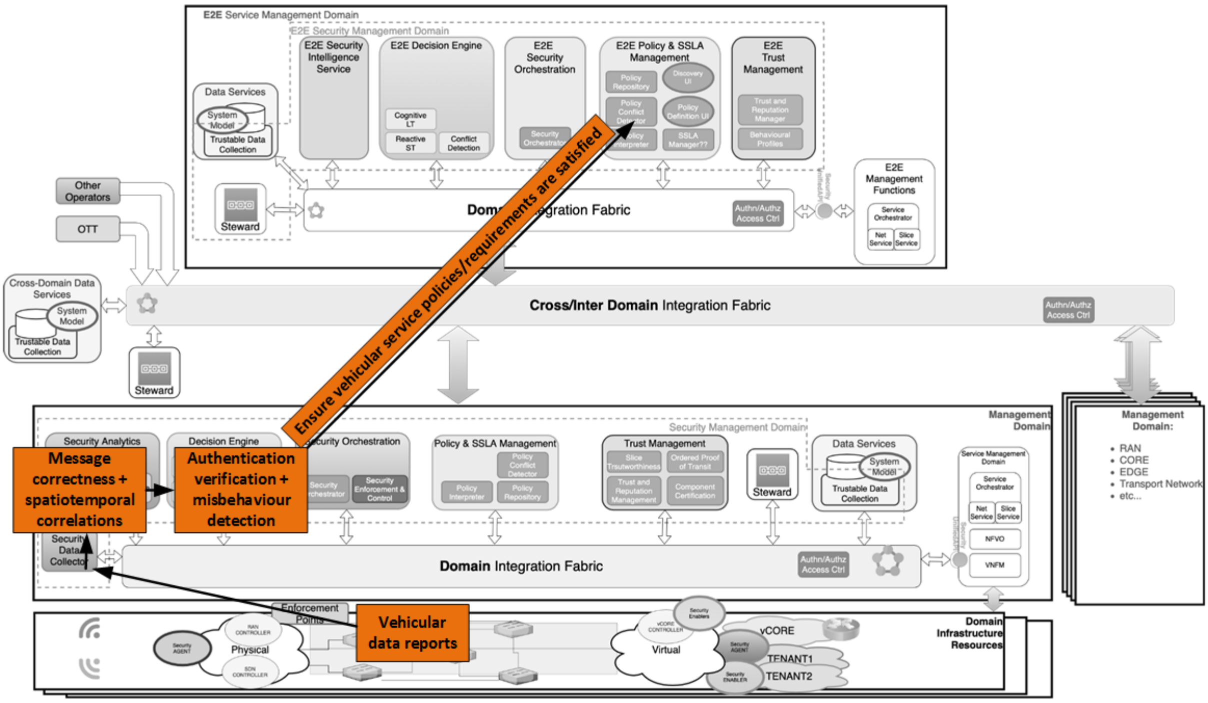


Figure 22: Integration of the Lightweight and Space-efficient Authentication in the HLA

The key HLA functional components involved are: 1) Security Data Collector: Responsible for collecting vehicular data reports and registration request messages; 2) Security Analytics Engine: Responsible for i) verifying the expected request/response messages for authentication and the freshness of the authentication tokens sent to the vehicles, ii) the detection of any potential vehicle misbehaviour after it is successfully authenticated by the system, iii) the exploitation of the spatio-temporal cross-correlations among vehicular data reports for extraction of the underlying dynamics in a network of vehicles; 3) Decision Engine: Responsible for i) determining whether the vehicle-towards-network and the network-towards-vehicle authentication fail or potentially succeed, ii) the verification that a seemingly abnormal vehicular activity (which may take the form of a highly sophisticated attack) is originated from malicious actors, iii) the identification of malicious activity patterns and for ensuring message correctness among neighbouring vehicles; 4) E2E Policy and SSLA Management: Responsible for ensuring that the achieved performance does not violate V2X service policies or requirements.

4.5 UAV anti GPS spoofing

4.5.1 Problem statement and challenges

Unmanned Aerial Vehicles (UAVs), or drones, are recognized as a promising technology to assist upcoming wireless networks in meeting the massive IoT requirements, thanks to their deployment and movement flexibility and their capability of establishing line-of-sight communication links. When the UAV execute flight mission, it needs to report its living position to Unmanned Aircraft System (UAS) Traffic Management (UTM) for safety and security purposes (e.g., collision avoidance, geofencing). The global navigation satellite system (GNSS), specifically GPS, is the primary location technology used by UAVs due to its global coverage and accuracy. However, the unencrypted civil GPS signals are inherently vulnerable to spoofing attacks. In fact, an attacker can use low-cost software defined radio (SDR) tools, such as USRP, to generate fake GPS signals to fool the GPS receiver into calculating false positions. A spoofed GPS position is not only used to hijack or confuse the UAV positioning system but also causing the collision between UAVs. Thus, it is imperative to incorporate appropriate measures into UTM systems to validate the positioning information and consequently counteract GPS spoofing attacks. Moreover, it is preferable that the envisioned measures do not require additional hardware or computation load at the UAV.

This enabler security motivation and engineering relate to the identified (security) limitation and gap of Chapter 5.7 of WP2 deliverable D2.1 defined as *Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats*. (Security Gaps)

4.5.2 State of the art analysis

Several solutions have been proposed for detection and mitigation of GPS spoofing attacks, which can be broadly classified into two categories, namely, GPS signal analysis methods and GPS information analysis methods. For instance, the authors in [86] devised a multi-antenna anti-spoofing technique for mitigating the spoofing signals. Similarly, in [87]presented a spatial signal processing approach for GPS spoofing detection and mitigation. The spatial signal processing takes advantage of multi-antenna reception for spatially filtering out fake GPS signals beamforming or null steering. In fact, multiple received signals having the same or very similar direction of arrival (DoA) is an indicator of GPS spoofing. In [88] and [89], the cross-correlation between the military and civil GPS signals is used for detecting the spoofing of unencrypted GPS signals. The cross-correlation strategy requires a communication link between a secure receiver and the defended receiver to perform the spoofing detection. The authors in [90] proposed Crowd-GPS-Sec, a solution that leverages the position messages periodically broadcast by the aircraft/UAV and their time of arrival to detect and localize GPS spoofing attacks. To safeguard civil GPS receivers against spoofing attacks, Wessonet al. [91] proposed to authenticate GPS signals by combining signature-based authentication of GPS navigation messages with a statistical hypothesis test. Similarly, Wuet al. [92] used SM cryptographic algorithms, to authenticate the BeiDou-II navigation messages. In [93], a trusted hardware is leveraged to generate cryptographically-signed GPS messages in order to resist spoofing attacks. The UAV's camera view is used in [94]to cross-check if the UAV's GPS position is spoofed or not.

Although the proposed GPS spoofing detection methods are effective, their adoption imposes more antennas and computational load on the receiver. In fact, the estimation of phase delay and direction of arrival requires an inertial measurement unit (IMU) or multiple reception antennas, while the cross-correlation induces computation overhead. Those methods can hardly implement into drone due to limited battery capacity and the extra weight load on the drone. Thus, a GPS spoofing detection mechanism that does not require additional hardware or computation load at the UAV is necessary.

The 5G new radio (NR) technologies is envisaged to play an essential role in enhancing positioning accuracy, owing to the high frequency bands and dense deployments[95]. Indeed, the characteristics of the uplink or downlink radio signals are utilized to infer the location of a user equipment (e.g., UAV). Potential radio signal-based localization approaches that will be supported by 5G NR include Time of Arrival (ToA), Angle of Arrival (AoA), and Received Signal Strength Indicator (RSSI) [96] In the aforementioned approaches, the node (e.g., UAV) position is estimated based on the distances or angles to the anchors (e.g., 5G base station), calculated using ToA, RSSI and AoA signal measurements[97]. Thus, 5G positioning services can assist the UTM in assessing the validity of UAV's GPS positions.

4.5.3 Solution description and advancements

The aim is to propose a novel cost-effective 5G-assisted method to detect the spoofed GPS positions reported to UTM by an UAV. Compared to other 5G signal-based localization techniques, RSSI measurements can easily be obtained from base stations without any extra hardware. Moreover, Mechanisms such as (Extended) Kalman Filter and Particle Filter can be used to reduce distance estimation error. For these reasons, an RSSI-based positioning scheme will be adopted to assist UTM in detecting GPS spoofing attacks. The Received Signal Strength (RSS) measurements collected from multiple 5G base stations are used to infer the UAV's residence area, enabling UTM to cross-check the validity of positioning information provided by the UAV. Machine Learning (ML) techniques will be leveraged to perform the cross-validation based on channel quality metrics extracted from the collected RSSIs.

4.5.4 Integration-interactions with HLA enablers

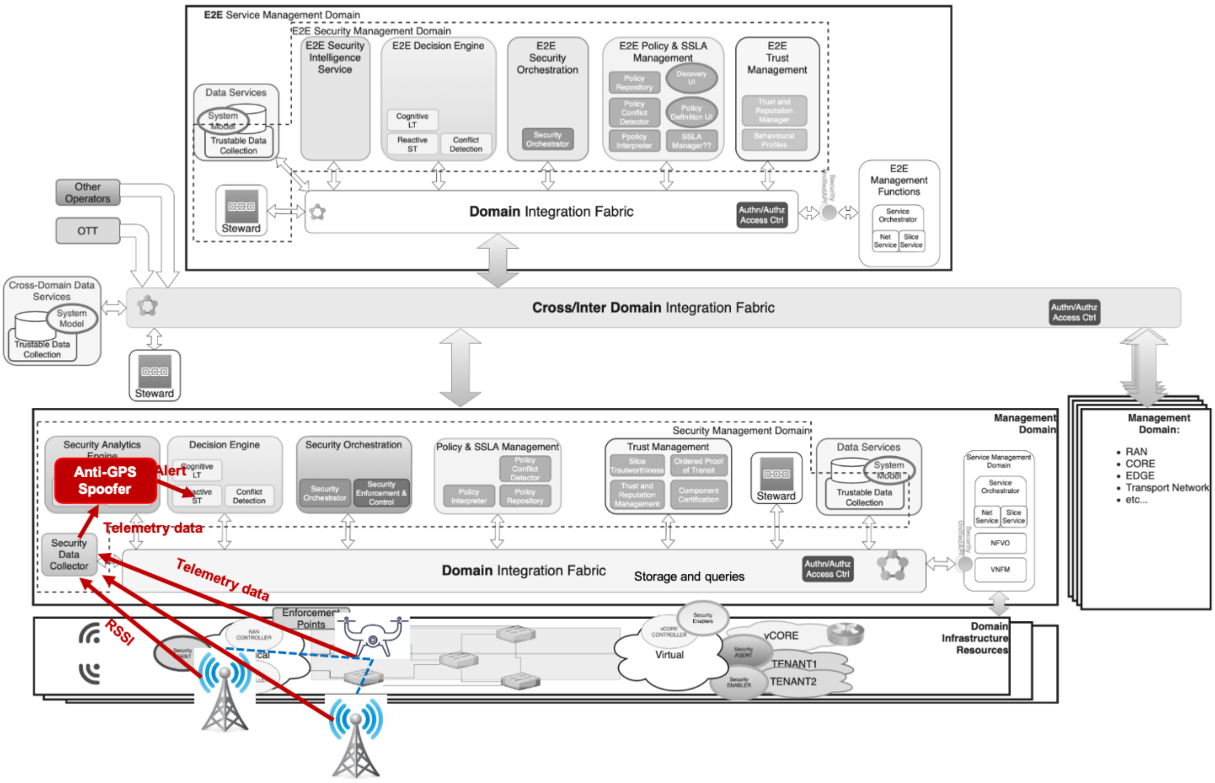


Figure 23: UAV anti GPS spoofing integration in the HLA

Telemetry data (including GPS positions) reported by the UAV and the path loss measurements reported by the base stations are collected by the “Security Data Collector” and forwarded to the ML-based GPS spoofing detector. If a spoofing is detected, an alert is sent to the “Decision Engine” for further mitigation actions.

4.6 I2NSF IPSEC

4.6.1 Problem statement and challenges

The new paradigm created by NFV allows to move some network security functions (NSF) from hardware appliance to Virtualized functions (vNSF). vNSF will apply to solve multiple security needs, such as authentication, access control, integrity or confidentiality, in a more dynamic and efficient way. Provide these functions jointly or separately with 5G network functions, physical (PNF) or virtualized (VNF), allows to provide a secure environment.

Nonetheless, most of the vNSF has kept proprietary format in order to enforce security policies, forbidding a common framework to enforce security Policies. Same situation arises in SDN, where when we talk in term of security, enforcement and policies are not following none a common standard interface. One relevant example IPsec. The standard defines ways to use IKE protocol to negotiate the keys and rules between 2 ends, but there is no standard defined for the management of the endpoints, such as policies to apply and nodes involved. SD-WAN and SASE [126] services, are examples of proprietary management and control plane with it owns interfaces to provide encrypted IPsec VPNs and end to end security services over it.

Additionally, increasing demands in latency and throughput promised in 5G are stressing the network access domain and transport domain. Increasing the fronthaul capillarity, to small cells, or the need of Edge computing solutions, requires network protections. Current standards ate 3GPP and GSMA, recommends solutions based on IPsec. As a consequence, multiple components are required to make translations between proprietary solutions, increasing TCO for 5G network operators that reduce it applicability.

This work relates to the Security Gap defined as " SDN security, SD-SEC and SECaaS " listed in D2.1 Chapter 5.7 (Security Gaps)where it is expected to deliver software-based security protections with interactions in several domains.

4.6.2 State of the art analysis

IPSec is standardized [127]to provide Authentication, access control, integrity and confidentiality of IP communications. These properties make it ideal to protect upper layers protocols, such the ones defined in 5G. GTP, eCPRI or DIAMETER as some example of protocols that delegate the security to IPsec.

IETF I2NSF working group has the aim to define a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual NSFs, enabling clients to specify rulesets. One of the first results in progress is a specification for IPsec [128] This specification allows to have a centralized Controller in charge of setup IPsec tunnels/transport and distribute the cryptographic policies and keys.

4.6.3 Solution description and advancements

The implementation of the I2NSF controller and agents for IPsec, will open a wide range of applications to protect 5G networks and communications. Above mentioned needs for transport protocols can be addressed with a Centralized E2E manager, to deploy different IPSec endpoints or gateways to protect the traffic. General architecture of the solution is shown in figure 24 below.

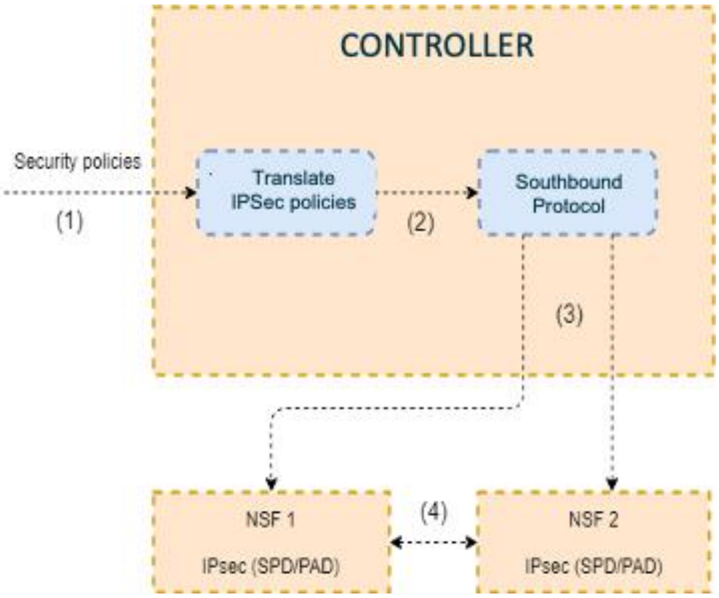


Figure 24: I2NSF for IPSec architecture.

The solution is composed of a I2NSF controller and 2 or more IPsec agents. The I2NSF controller can be and application of a SDN Controller or part of the NFV MANO orchestration policies. It is in charge of receive the security policies (1), e.g., a MSPL, translate them to a I2NSF model (2) and send to the IPsec Agents using a standard interface NETCONF. The model can include algorithms to use, keys for integrity and confidentiality, lifetime, etc. The agents can be deployed as stand-alone vNSF or can be integrated in exiting VNF with cryptographic operation capacity to enforce the policy and establish the IPsec tunnel (4).

Some potential applicability scenarios in 5G networks are:

- Secure slices. Using a Centralized controller that invoke the setup of a IPsec tunnel as part of the Slice configuration, could provide confidentiality and integrity in the slice traffic.
- IPX interconnection. Despite of the TLS adoption in the lasted 3GPPP standards, still there is IPX providers providing connectivity based on IPsec agreements. The use of centralized policies can provide more visibility and control for these providers.
- Small/remote cells protection. The expose of gNodeB or part of it (RRH, DU) in insecure sites, can open opportunities for attacks in the traffic and to the 5GCore. I2NSF-IPsec solutions close to remote functions of the gNodeB will be enforced by a controller in charge of IKE negotiation providing light solutions and centralized policies to protect the network
- Edge Computing security. Provide security in the Edge sites deploying IPsec connectivity with access and core.

I2NSF IPsec aims to provide solutions to two security gaps identified in D2.1 section 5.7 identified limitations and gaps: (Security Gaps)

- Coordinate authentication between network elements, such as VNFs, in multiples domains, through the unified E2E control plane that can inventory the end points nodes involved in the setup and provide the authentication based on the IPsec authentication/integrity cryptographic solutions.
- as a SDN Security in terms of SECaaS technology, respond and enforce traffic confidentiality with IPsec encryption between domains.

4.6.4 Integration-interactions with HLA enablers

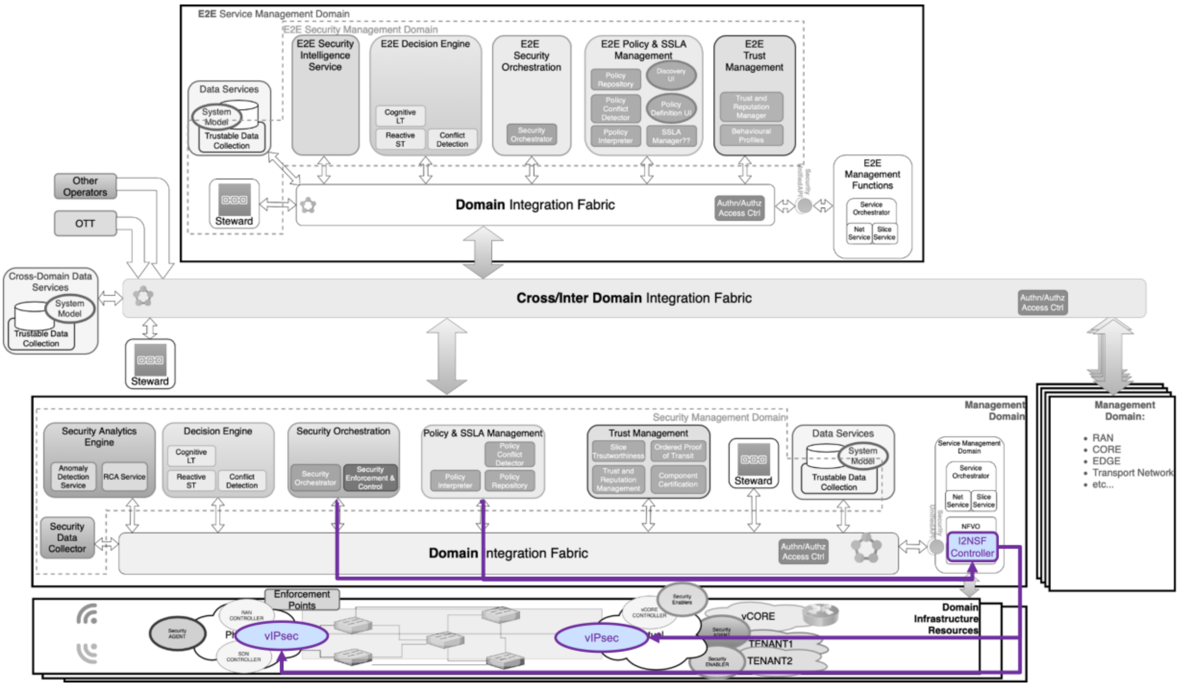


Figure 25: vIPsec and I2NSF controller components in HLA.

The I2NSF IPsec solution acts as an enabler on the 5G network. Their role includes the enforcement of security policies defined by the Policy & SSLA Management component. In fact, it is the Domain Security Orchestrator, who will request to the Service Management Domain (e.g. ,the Edge NFV MANO, the SDN Controller, etc..) to deploy and configure the IPsec tunnel, using the vIPsec assets as VNFs on the infrastructure. Although is not reflected in the Figure, in case of multiple domains involved, each I2NSF Controller can be orchestrated by the E2E Security Orchestrator.

4.7 Virtual Channel Protection

4.7.1 Problem statement and challenges

5G deployments are comprised by vast number of heterogeneous components, services and interconnections. In this regard, protecting the communications by different encryption approaches becomes fundamental for avoiding issues such as lack of confidentiality, spoofing or data manipulation. However, considering heterogeneous devices that can be connected to 5G networks, not all devices are able to manage all channel protection operations. In fact, there are a vast amount of constrained devices which can access 5G networks but are unable to implement the most recommended channel protection algorithms or procedures. For instance, most common IoT devices are not able to manage asymmetric cryptography, they are not even capable to manage complex ciphering algorithms for symmetric cryptography. Besides, even in regular scenarios we can find restrictions like law regulations, or organization policies which require that the traffic must be protected with specific mechanisms and algorithms, these mechanisms may not cover the whole path and therefore mechanism translation might be needed. In this regard, it is necessary to provide dynamically different channel protection solutions on demand depending on the security requirements. This work relates to the Security Gap defined as "ZSM, MEC security, multi-MEC security and Secure 5G radio access" listed in D2.1 Chapter 5.7 table. (Security Gaps)

4.7.2 State of the art analysis

5G infrastructure properties such as Network softwarization plays a key role providing with the desired scalability level in network management. In this sense, the Internet Engineering Task Force (IETF) is working towards managing IPSec Security Associations (SAs) in SDN networks and enabling end-to-end channel protection[98]. However, more efforts are required to get the benefits of SDN to facilitate channel protection in those networks in which IPSec is not directly supported, or which just require establishment of additional secure channels. In this regard, standardization organizations like IETF are working to define new protocols for channel protection and key exchange and distribution in more constraint environments, such as the OSCORE [99]and EDHOC [100]protocols; the former is used to secure the communications end-to-end, while the later generates the necessary key material. Nonetheless, the current standard to protect Constrained Application Protocol (CoAP) exchanges is DTLS. CoAP documentation defines DTLS as its secure communications mechanism. Therefore, DTLS is one of the first protocols to be considered in constraint security associations. In this regard, Bernal et al [101]designed, implemented and validated a by-default DTLS channel protection and key distribution during IoT bootstrapping processes.

4.7.3 Solution description and advancements

The solution will allow instantiating and configuring on demand channel protection capabilities depending on the security requirements. It includes the dynamic instantiation of channel protection proxies which are deployed in the 5G network as near as possible of the source and destination of the communication in order to guarantee the desired channel protection level across the path. For instance, a DTLS proxy can be instantiated as near as possible of those devices which are not able to perform the required security level in UDP communications. For covering other channel protection technologies such as TLS or IPSEC or new channel protection proxies could be provided.

It would be also possible to enforce encryption for devices that even if capable of managing encryption, might not be manageable by the entity managing the data, for instance, devices deployed and running on battery that are difficult to access physically or even not accessible at all. Another key situation is that of devices for which the vendor cryptographic material provided on factory that might have been compromised. In such cases re-encrypting the connection at the very edge would be a mitigation before leaving the 5G network towards the cloud.

4.7.4 Integration-interactions with HLA enablers

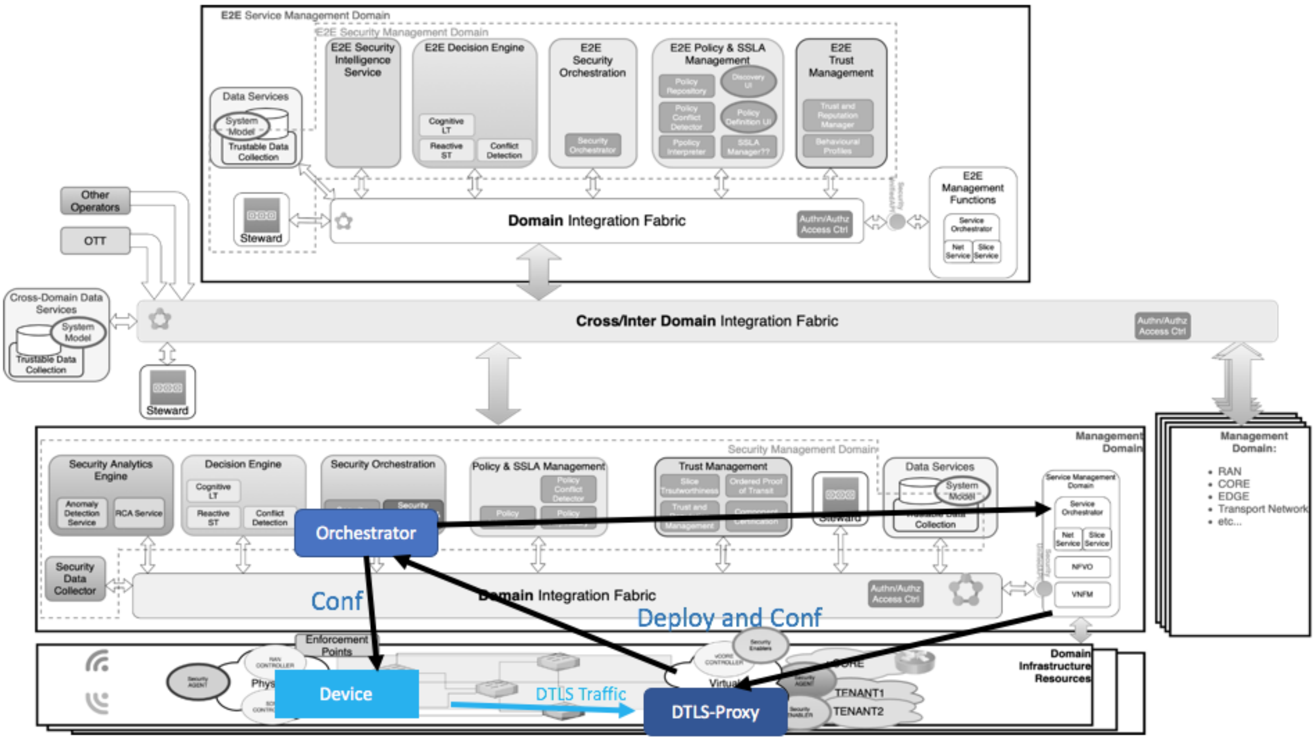


Figure 26: Integration of the virtual channel protection in the HLA

Virtual Channel Protection is an on-demand enabler, instantiated by the Service Management Domain when required from the Security Orchestrator. It guarantees the channel protection required from the access type of the device by deploying or configuring requested asset in the infrastructure.

4.8 Virtual Privacy (CP-ABE proxy)

4.8.1 Problem statement and challenges

Whereas the benefits of 5G networks generations are becoming day by day in a reality, the ability to interconnect almost everything also generates a critical privacy challenge that must be addressed. In this regard, end to end data privacy should be ensured by default to guarantee that only the involved parties of the communications are aware of the content. However, not all devices able to connect to the 5G infrastructure are able to implement security properties like this one. For instance, most common IoT devices are not able to manage specific algorithms for data privacy (e.g., attribute-based encryption). In this regard, it is necessary to provide different mechanisms to protect data privacy, able to deal with the heterogeneity nature of new and future network generations. This work relates to the Security Gap defined as "ZSM, MEC security, multi-MEC security and Secure 5G radio access " listed in D2.1 Chapter 5.7 table. (Security Gaps)

4.8.2 State of the art analysis

Regarding data privacy, if well it is true there are multiple approaches, Bethencourt et al. [102]provided the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) which allows that encrypted data be kept confidential even if the storage server is untrusted. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, these methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). Authors also provided an implementation as well as performance measurements. Following this approach, Perez et al. [103]introduced an attribute-based lightweight symmetric cryptography solution for smart building scenarios. Specifically, the solution is focused on CP-ABE, in order to allow specific subjects access to specific pieces of data for privacy-preserving. Matheu et al. [104]also applied this promising approach over an IoT infrastructure for enforcing data privacy security profiles.

4.8.3 Solution description and advancements

Privacy is one of the main concerns of IoT, where resource constrained devices send sensible data every day without the capability of performing cryptography operations to ensure privacy at data level. In this regard, E2E data privacy is achieved with this solution by enforcing data privacy security policies that dynamically instantiate and configure on demand data privacy proxies capabilities depending on the privacy requirements of the communication. The dynamic instantiation of data privacy proxies which are deployed in the 5G network as near as possible of the source and destination of the communication, and they perform as well as the keys distribution among other processes in order to guarantee the desired privacy protection level for the data. For instance, the Ciphertext-Policy -Attribute-Based Encryption (CP-ABE) proxy can be instantiated as near as possible of those devices which are not able to encrypt data through the capability-based approach, so the traffic coming/from those devices will be transparently redirected to the CP-ABE proxy as a middle-box which will apply the required data privacy encryptions/decryptions.

4.8.4 Integration-interaction with HLA enablers

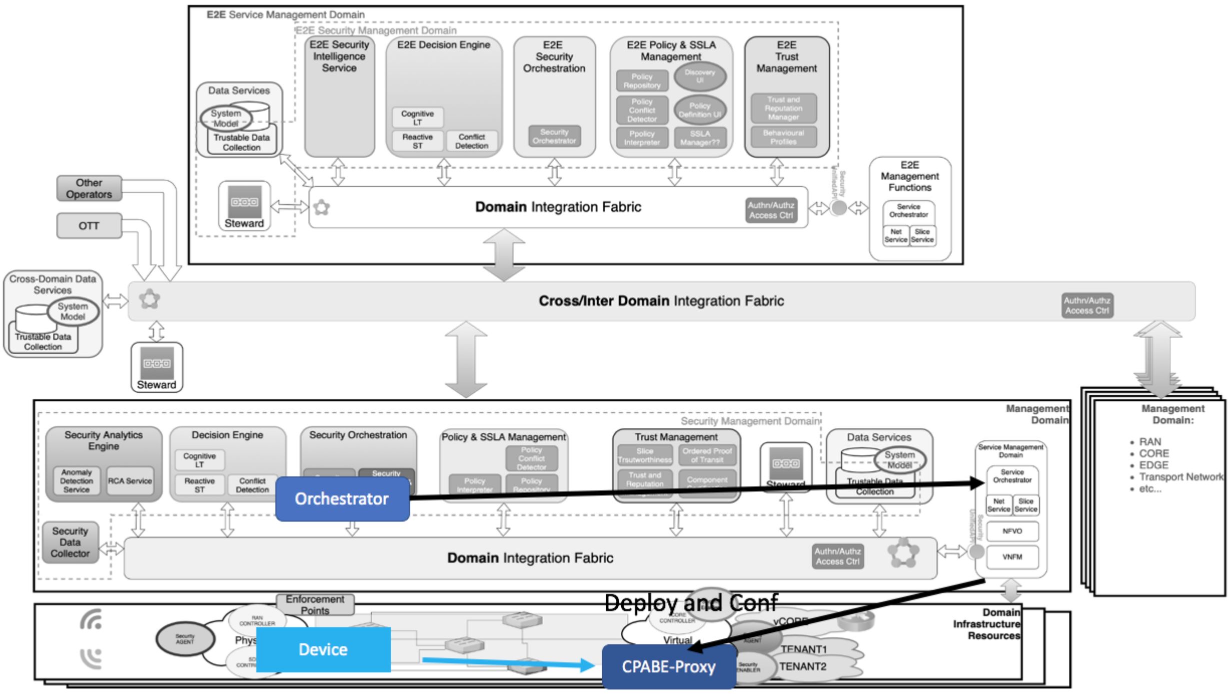


Figure 27: Integration of Virtual Privacy Protection in the HLA

Virtual Privacy is an on-demand enabler, instantiated by the Service Management Domain when it is required from the Security Orchestrator. It ensures the privacy protection throughout the infrastructure for the device accessing the 5G network by deploying or configuring requested asset in the infrastructure.

4.9 Baseline assets used in this project

The following assets will be used by partners as baseline assets in the development of their enablers:

- **IAMaaS** **[129]**(TSG), developed as part of Sendate Tandem project, provides:
    - Digital Identity Services;
    - Directory Services;
    - Credentialing Services;
    - Authentication Services;
    - Security Token Services;
    - Identity Federation Services;
    - Privilege Management Services (incl. role/group management).

5 Security Analytics

5.1 Introduction

The objective of Security Analytics in cybersecurity is the proactive and reactive protection of network infrastructure by collecting and analyzing data to detect unusual traffic patterns, anomalies and zero-day threats. The immense amount of data generated by network assets calls for automated monitoring and alerting processes in order to reduce cyber resilience KPIs, including Mean Time to Detect (MTTD), Mean Time to Contain (MTTC) and Mean Time to Resolve (MTTR). In this context, ML is a significant enabler towards this goal and an important tool for security teams that often struggle with complex processes, employee shortage and extended detection and resolution times.

Towards this objective, INSPIRE-5Gplus includes two enablers for Security Analytics, namely the "Security Analytics Framework" and "The SSLA Assessment and Enforcement". The Security Analytics Framework provides anomaly detection services and is based on the Apache Spot version developed in the SHIELD Project and further refined in 5GENESIS, or the MMT security monitoring framework developed by Montimage. In the course of INSPIRE-5Gplus, the ML engine of these Frameworks will be further upgraded to include: i) appropriate algorithms that will improve their detection accuracy in different attack scenarios; ii) extend their data ingesting capabilities by including data from the infrastructure and applications; iii) improve their visualization capabilities for more effective presentation of results; and iv) improve their interoperability with other enablers by defining open APIs.

The SSLA Assessment and Enforcement enabler provides versatile probes for collecting and processing data coming from different sources as well as SSLA assessment capabilities for specifying and managing security policies in real-time. The SSLA assessment enabler was introduced in the H2020 MUSA [124]and CelticPlus-SENDATE projects [125]and is based on real-time monitoring of metrics. Its main functions include assessment of security functions (i.e., that they are doing what they are expected to do), detection of security breaches, and translation between different formalisms (e.g., SSLA, Tosca, MSPL). In the context of INSPIRE-5Gplus, the SSLA assessment enabler will be extended to support interaction with the Security Orchestrator, translation of high-level policies to lower-level actionable policies and management of SSLAs, and remediation strategies in both the control and data planes.

5.2 SSLA assessment and enforcement

5.2.1 Problem statement and challenges

To provide the automation promised by ZSM (Zero Touch Network and Service Management) one needs the means to define security requirements that can be assessed and controlled at all times. This implies formally specifying these requirements that will regulate the level of security, verify that the security functions are correctly implemented, and that the security properties are not violated. Defining the level of security is necessary because security has a cost and thus a compromise needs to be found between the desired quality of service or experience and the security controls. The violations of the SSLAs need to be detected and must trigger self-healing or self-protection strategies. Thus, security monitoring and analysis is a challenge that needs to be addressed to guarantee the desired security level and achieve remediation and prevention of security breaches and vulnerabilities in a fully automated fashion.

The ability to define and manage Security-oriented SLAs (SSLAs) is essential for operators offering managed services. Similar to the SLAs concerning performance, SSLAs is a contract between an operator and a customer that defines the services and the security levels that both parties expect. In other words, SSLAs are needed by operators, service providers and end-users to “contractualised” the requirements related to security capabilities of the provided networks, slices and services. The defined SSLAs allow end-to-end controlling, that the security functions are correctly implemented and that the security properties are not violated.

The solution or techniques recognised here addresses the challenge described in the table 4 found in Sec. 5.7 of the deliverable D2.1: *Security service level agreement* (Security Gaps)In particular to assess and automate the enforcement of security policies in real-time that is an enabler addressing part of the challenge: *Automation and Zero-touch Service Management.*

5.2.2 State of the art analysis

In the literature, SSLAs have been defined for managing security and privacy in the Cloud[105], [106],[107],[108]. The H2020 MUSA project has defined SSLAs for multi-cloud environments (109). In this project a first prototype was developed that showed how the SSLAs can be specified for federated cloud systems. The originality of this work is the use of real-time monitoring to assess and enforce SSLAs. On the other hand, SSLAs have not been applied to 4G and 5G mobile environments. The use of SSLAs has been demonstrated for 4G environments in the CelticPlus SENDATE-TANDEM [125]project and showed how they facilitate the agreements between different components concerning the expected cyber-security level and remediation strategies. In this project, SSLAs are defined for assessing and controlling that:

- The security functions are correctly implemented
- The security properties are not violated
- The violations trigger self-healing and self-protection strategies
- SSLA metrics examples:
- Data and service availability
- Geo-localisation of data/services
- Frequency of security analysis
- Number of GTP per subscriber
- Isolation access from other slices
- Security enforcement techniques:
- Time to deploy new technique
- Delay in applying patches
- Delay in reconfiguring
- Delay in revoking users/operators
- Delay in replicating services and switching instances.

5.2.3 Solution description and advancements

The solution relies on the MMT monitoring framework. This framework consists of probes (i.e. , Security Agents) and applications for managing them, and analysing the data captured from different sources (network packets and sessions, application traces, system logs, etc.).

The analytic functions use different techniques to detect anomalies and perform complex event processing.

The versatile probes can capture and process data, and extract the meta-data needed for security and performance analysis and control.

The framework includes the following capabilities (some more evolved than others):

- Interaction with orchestrators (e.g., OSM, ONAP) to obtain the network topology, determine the changes needed to protect the network, and provide the specification of the changes to be performed by the orchestrator.
- Capture events (monitoring of network, apps, system...)
- DPI, DFI, application and system traces

- Monitoring in slices and E2E
- Dashboards, alarms
- Rule-based and behaviour-based analysis
- Anomaly detection
- ML/AI-based analysis
- Optimised packet processing (using DPDK, P4 language, microservices)
- Triggering self-protection and self-healing strategies
- Deployed as VNF or SECaaS

The SSLA assessment enabler, that was started to be developed in the H2020-MUSA and CelticPlus-SENDATE projects, allows specifying, managing and performing real-time assessment of security policies called Security Service Level Agreements. The specified SSLAs can detect anomalies caused by security breaches and determine if the security functions and controls are operating as expected. The main functions are:

- Assessment of security functions
- Detection of security breaches
- Management of Security Service Level Agreements (SSLA)
- Extension of Tosca with security event management and reactions.
- Translation between different formalisms, e.g., SSLA, HSPL, MSPL, Tosca.

The solution that is being extended in INSPIRE-5Gplus concerns how SSLAs can be defined for formalising the requirements related to a wide variety of cyber-security issues and concerns in 5G. It goes far beyond current intrusion detection and prevention systems, as well as policy control systems, in that:

- It is based on real-time metrics that allow fine-grained or more abstract assessment of the security requirements of the different stakeholder involved.
- It allows detecting security breaches as well as malfunction of security functions.
- It integrates remediation strategies that can be triggered automatically with the goal of enforcing the specified SSLAs.

To better automate the process of defining and enforcing SSLAs, real-time monitoring of network, application and system activity based on distributed probes is needed. The probes, or Security Agents, capture the data, meta-data and statistics that allow measuring the parameters implicated in the specified SSLAs. Then, complex event processing and machine learning can be used to analyse and detect breaches at the local level by the Security Agents or at the domain or cross-domain level by the Security Analytics Engine. Finally, when breaches are detected, corrective actions (e.g. ,self-healing or self-protection techniques) need to be taken. These actions can be triggered manually by the operators, or automatically by the Decision Engine that interacts with the Orchestrators and Controllers to perform the necessary actions.

Starting from the results obtained in the SENDATE-TANDEM project and with the objective of obtaining an industrial-grade commercial solution, INSPIRE-5Gplus has started extending the solution to better address the needs of 5G. This includes the specification (that will be followed by the implementation) of features at different levels (see Figure 28):

- “Extract”: SSLAs and remediation strategies for both the data and control planes.
- “Specify and manage”: Translation of high-level policies (HSPL) and SSLAs to lower-level actionable policies (MSPL, TOSCA).
- “Self-protect”: Interaction with the Security Orchestrator or Orchestrator

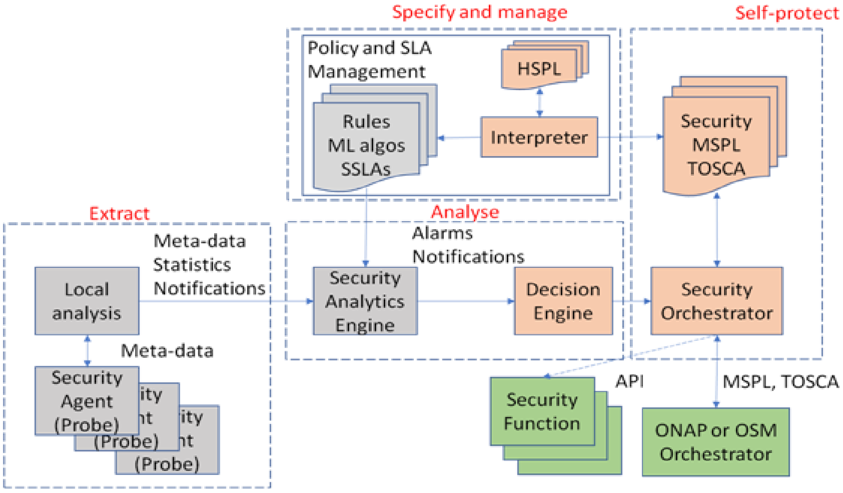


Figure 28. SSLA functional architecture diagram

5.2.4 Integration-Interaction with HLA enablers

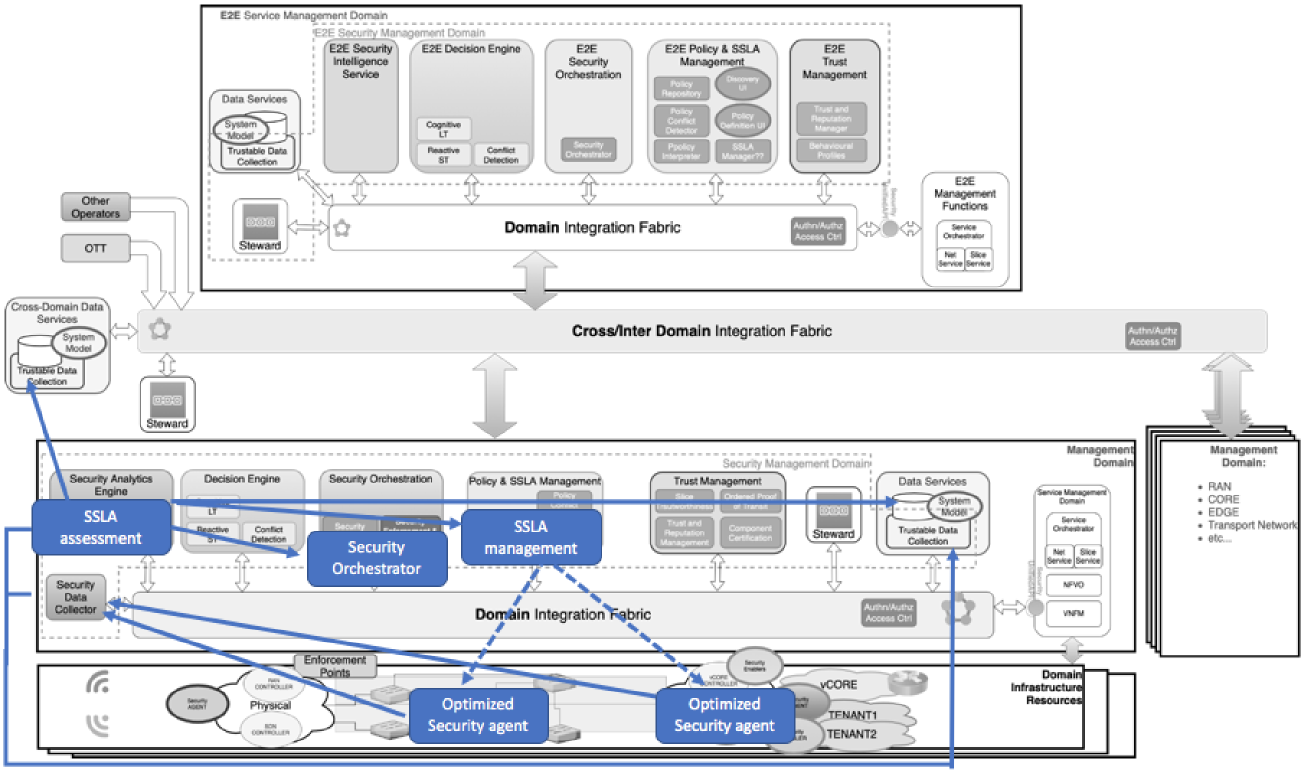


Figure 29. Integration of the SSLA manager in the HLA

The real-time SSLA assessment module is part of the Security Analytics Engine. It is configured with rules defined by the operators and end-users, i.e., derived from the agreed upon security policies managed by the Policy & SSLA Manager. At the same time, the SSLA manager will inform the Security Agents what information is needed to assess the SSLAs (doted lines in the figure). The module will analyse data captured provided by the Data Services (for historical data) and Security Data Collector (for real-time data captured by the Security Agents). When an SSLA is not respected, it will notify the Security Orchestrator that will trigger corrective actions.

5.3 Security Analytics Framework

5.3.1 Problem statement and challenges

5G comes with extensive features and capabilities, allowing the realization of advanced Use Cases, not feasible with legacy mobile networks. However, this advancement comes with various side effects, including the increased attack surface due to new flavours of technologies introduced in 5G, such as SDN, Network Slicing, Multi-tenancy and more complex architectures. Under certain circumstances, these could constitute potential sources of vulnerabilities, increasing the probability of security incidents.

On the other hand, 5G network components are highly heterogeneous and distributed across the network, thus creating an enormous amount of diverse data, whose analysis can lead to proactive remediation of malicious events. As a result, the problem revolves around investigating feature engineering aspects of the mobile data, as well as the application of proper ML-driven algorithms that are most relevant to an anomaly detection system. An important challenge remains data availability, collection and evaluation, as well as data pre-processing, including labelling. In the context of INSPIRE-5Gplus, this work relates to the Security Gap defined as "Artificial Intelligence and Machine Learning" listed in Table 5.7 (Security Gaps)

5.3.2 State of the art analysis

Intrusion Detection Systems (IDSs) are one of the most significant parts of a network. In general, IDSs use mechanisms that can be classified in three distinct categories: i) misuse detection, ii) anomaly detection and iii) hybrid detection. In misuse detection, the IDS maintains a set of rules for detecting known attacks. In anomaly detection, the IDS detects attacks based on the hypothesis that attacker's behaviour differs from normal behaviour. Finally, hybrid detection is a combination of misuse and anomaly detection techniques. ML techniques have been extensively applied in anomaly detection frameworks, both in wired and wireless networks. The massive increase of data foreseen in 5G networks calls for automation in detecting well known and novel attacks. In [110], the authors provide a detailed investigation on machine learning techniques for the above categories of IDSs. The paper reports the results of multiple combinations of ML algorithms found in the literature, namely Single Classifier with all features, Single Classifier with limited features, Multiple Classifiers with all features and Multiple Classifiers with limited features. It is shown that no particular ML algorithm is able to detect all types of attacks and it is important to define the optimal feature set for each type of attack.

INSPIRE-5Gplus Deliverable [111] also provides references in anomaly detection frameworks. Specifically, the authors in [112]describe an anomaly detection system for 5G networks based on Deep Belief Networks (DBN), Stacked Auto-Encoders (SAE) and Long Short-Term Memory (LSTM). Authors in [113] proposed an anomaly detection and diagnosis solution for RANs self-healing in 5G networks. The anomaly diagnosis process relies on Case-Based Reasoning (CBR), transfer learning and active learning techniques to allow for autonomous self-healing actions. In[114], the authors evaluate the performance of Gaussian probabilistic latent semantic analysis (GPLSA) model and Gaussian Mixture Model (GMM), comparing their results a real dataset captured from a wireless network. They also propose a novel algorithm with model log-likelihood.

Another interesting approach is graph based anomaly detection that has been applied to intrusion detection datasets in[115]. The authors propose a graph representation that combines different kinds of events, allowing a rich description of the network activities and then apply an autoencoder, which follows the unsupervised learning approach, in order to detect anomalies. The results obtained in the CIDIS2017 dataset are better than other supervised solutions.

5.3.3 Solution description and advancements

The Security Analytics Framework provides anomaly detection services and is based on the Apache Spot [116]version developed in the SHIELD Project and further refined in 5GENESIS[117].

It will include multiple monitoring probes distributed across the 5G infrastructure (RAN, CN, TN) for collecting heterogeneous data. The solution shall collect, process, detect and classify anomalies associated with security incidents, notifying the Security Administrators or other enablers across the INSPIRE-5Gplus ecosystem via appropriate APIs. In addition, the Security Analytics Framework will support multiple data models for different technologies and vendors, as well as appropriate ML algorithms for detecting anomalies in multiple points of the network domains, increasing the overall detection accuracy.

Advancements include upgrading the ML engine of the Framework using appropriate ML paradigms and extending its ingesting and visualization capabilities. Specifically, new ML algorithms for anomaly detection stemming from State-of-the-art analysis will be implemented, tested and evaluated against different attack scenarios. Such scenarios include attacks on edge services, resulting in compromised edge functions used for eavesdropping user traffic and attacks on the infrastructure, such as DDoS attacks using edge functions for draining edge infrastructure resources. Another attack scenario under consideration is alerting the system in case of potential radio security incidents, such as jamming.

An additional advancement is the extension of the Framework’s ingesting and visualization/alerting capabilities. The current version is able to collect and process DNS logs, Proxy logs, and Netflow traffic (sflow). It is imperative to support data coming from the Radio Access and Core Networks, in order to capture not only infrastructure related metrics, such as CPU and RAM utilization, but also mobile network specific metrics, including but not limited to radio conditions (RSRP, RSRQ, RSSI, SINR, CQI), signalling events, throughput, usage data records, bearer information etc per UE. Furthermore, the Security Analytics Framework will support APIs for alerts and information fusion across INSPIRE5G-plus enablers.

The final advancement will revolve around extending the graphical user interface of the Framework using *Graphana*, *Prometheus* and *InfluxdB*, in order to support metrics analytics, as well. The current version of the graphical user interface supports only flow analytics and this needs to be updated to support the future attack scenarios we want to study over the course of INSPIRE-5Gplus.

5.3.4 Integration-Interaction with HLA enablers

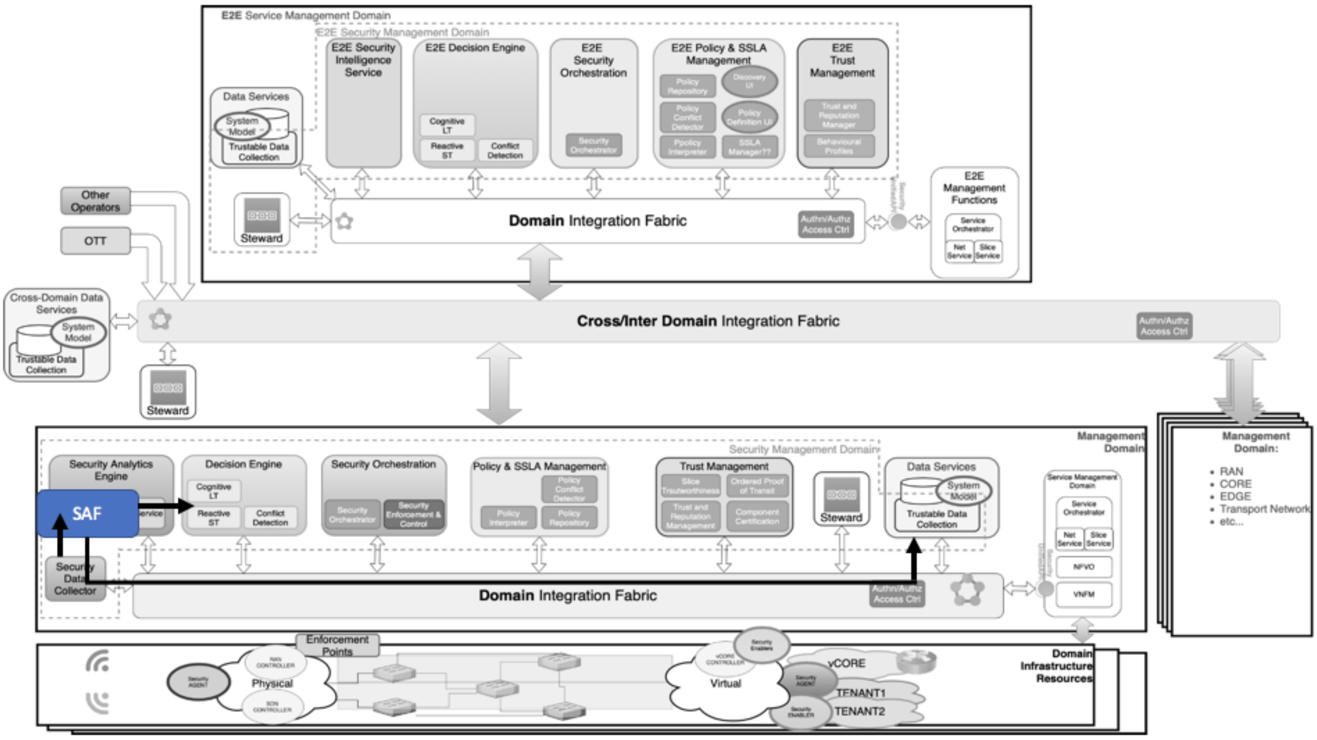


Figure 30: Security Analytics Framework in the HLA

The Security Analytics Framework (SAF) belongs to the Domain Security Analytics Engine of of the HLA and specifically to the Anomaly Detection Service Block. It sources network data from the Security Data Collector, pre-processes and transforms the data to appropriate formats, executes machine learning inference and provides the results to other entities, including the Decision Engine and the Data Services.

5.4 Baseline assets used in the project

The following assets will be used by partners as baseline assets in the development of their enablers:

1. IDS, IPS and DPI Security VNFs (NCSRD), developed as part of SHIELD project: Intrusion Detection, Intrusion Prevention and Deep Packet Inspection VNFs for network security monitoring.
2. IAMaaS (TSG), developed as part of Sendate Tandem project:
    a. Digital Identity Services: manage the lifecycle of identities of all subjects and objects, e.g. network entities of a 5G system, as well as end-users.
    b. Directory Services: provide standard interfaces to store and search for identities, associated attributes, esp. security-relevant attributes (roles, groups, organisation, etc.); and user self-services where they can manage their own account.
    c. Credentialing Services: bind credentials (certificate, public key, password, hardware tokens, etc.) to an identity for authentication.
    d. Authentication Services.
    e. Security Token Services: issue security assertions, preferably in form of self-contained signed tokens, that can be reused as access token for most if not all protected interfaces of the 5G system that require authentication.
    f. Identity Federation Services: provide mechanisms to reuse identities of a third-party domains; this is essential when entities have identities and authentication

capabilities pre-existing to the 5G system since it gives the opportunity to reuse those and perform just-in-time provisioning of their identities in the 5G system. This requires establishing a trust relationship between the 5G system's IAM service and the third-party identity management system.

g. Privilege Management Services (incl. role/group management): for access control purposes (e.g. allowing only tenant admins to access the MANO interfaces), it is necessary to assign and manage roles, groups and other authorisation attributes of end-entities.

3. WAF (TSG), developed inside SPIDER project: A firewall protecting against OWAPS known vulnerabilities to secure applications
4. HONEYPOT (TSG), developed inside SPIEDER project: Create an honeypot emulating an operating system or a small topology to trap corrupted traffic / behaviour
5. DDOS-dbScan (TSG), developed inside SPIDER project: A DDoS detector using the machine learning DBSCAN clustering algorithm

6 Security Data Collection

6.1 Introduction

Security data collection category focuses on the data manageability and security related information that can be obtained from the network. This information is the source for security analytics process that will trigger decision. Aspects related to how the data is generated, collected and treated are important to provide efficient and valid insights.

One of the main problems in the data engineering and data science, is the quality and validity of the data. The first stage in any AI based solution is the design and testing process. To this end high quality datasets are needed, furthermore contextual information is mandatory. For example, labelling dataset are required in supervised ML, and in order to train and validate the performance. Other example is in unsupervised ML, where labels are not needed for training, but a context of some of the data is needed to discern correct or not and evaluate the performance. As a consequence, access to the data of 5G telecom production environments is not always the best solution in terms of the context, because the privacy restrictions, encryption of the traffic or the scale of the data collection.

One alternative solution is the use of Network Digital Twins (NDT) enablers, such as MOUSEWORLD enabler. Similar to Industry 4.0 Digital twin concept, that simulate physical systems to improve the processes, Telecom networks can be simulated to generate traffic in similar conditions to production, so different ML techniques and tools can be trained and evaluated. The ML based tools and enablers, such as Smart Traffic Analysis (STA), can evaluated and certified in repeatability conditions.

Other relevant area to provide context to the information is the generation of this metadata or context, jointly with the data itself by the network. STA propose a solution to increase network information value including relevant metadata for specific security attacks, using ML previously trained in distributed probes, to detect attacks. This solution can be integrated in normal probes such as netflow as a complement.

Analytic engines require works with specific data sources and formats. Security is not an exception. Multiple formats are available in the network from legacy ones (SNMP, Netflow) to recent ones (gRPC, IPFIX, NETCONF), and each one of them bring it's contextual information from the network. A mechanism to aggregate and transform this information is usually an ad-hoc process. Data collection enabler propose to adoption of ETSI CIM, standard to collect different formats and source, and their transformation previously to be used by analytic engines.

6.2 Dataset generation based on Network Range-Digital twin (MOUSEWORLD)

6.2.1 Problem statement and challenges

Network attacks detection and classification is an important task for telecom operators and for 5G infrastructure protection. Currently, techniques based on the inspection of packet payload are used for this matter (e.g., Firewall, DPI, IDS). However, these techniques need a nearly constant signatures of each class of traffic. Machine Learning and in particular Deep Learning techniques have started to be successfully applied to address those problems.

ML supervised methods need to be trained initially with a selected set of examples (i.e., a labelled dataset) and, in order to obtain an accurate classifier, the examples utilized during the training phase should be as close as possible to network traffic that is going to be classified later. In many scenarios, the extraction of a representative dataset is a difficult task. Gaining access to collections of production or clients network traffic data is not possible, mainly by data privacy protection or IPR. Secondly, even having access to a relevant data source, we need to put a label on each element of the dataset in order to train/validate the ML models, impractical when we deal with the size of the typical datasets for an acceptable training (hundreds of thousands of samples, and not even a security expert would be able to attach the right label to each sample due to the intricate nature of the traffic and the attacks.

The MOUSEWORLD aims to address a couple of security Gaps listed in D2.1 Chapter 5.7 table related to Artificial Intelligence and Machine Learning (Security Gaps) On one hand provide a network Digital Twin infrastructure created for AI and in the other produce datasets related to network threats.

6.2.2 State of the art analysis

Machine Learning and deep learning are techniques already considered in cybersecurity area. In [118], relevant techniques evaluation and the dataset sources are referred. Most of these sources are a few ones well-known: KDD-99 [119], CIC (120] or private sources. These datasets could not be valid for ML developing by the format, imbalance or the labelling used.

6.2.3 Solution description and advancements

MOUSEWORLD allows to make an offline dataset generation tool for training ML models by other tools and to validate performance models.

MOUSEWORLD follow the approach of setup a Network range-digital twin (NDT) focused on network traffic for different types of applications, including security. MOUSEWORLD emulate a specific network configuration and generate the required realistic traffic and capture and process to produce datasets to be used subsequently.

The main components we consider for the MOUSEWORLD are:

- A topology generator that instantiates the required number of virtual applications (clients and servers), and networks devices to interconnect them. The current MOUSEWORLD version provides a dynamic generator of topologies, clients and servers (using Open Source MANO) based on *Openstack*, and it is planned to support Kubernetes and dockers.
- An experiment scheduler. This component allows to configure and run realistic scenarios in a totally controlled way in order to (a) gather the network packets injected in the network and (b) be able to automatically put the corresponding classification labels to each packet flow. The current version has a simple configuration file to schedule a limited set of experiments (including some security attacks). The goal would be to add evolve this file into a complete configuration and scheduling environment.
- Label generator. This component in collaboration with the experiment scheduler will produce a (realistic) labelled network traffic dataset ready to be used as input for a classifier training process. This labelling process is associated to specific traffics.

Current activity is focused in use MOUSEWORLD to generate datasets on demand. Some DDoS attacks have been produced during the activity on INSPIRE. Advancement plans envision to automate the scenarios deployment for dataset generation using a common defined model, evolved from OSM data model.

Related to Security gaps identified in D2.1 Chapter 5.7, MOUSEWORLD Tackles with the concept of Network Digital Twins, in the area of Artificial Intelligence and Machine Learning technologies.

6.2.4 Integration-Interaction with HLA enablers

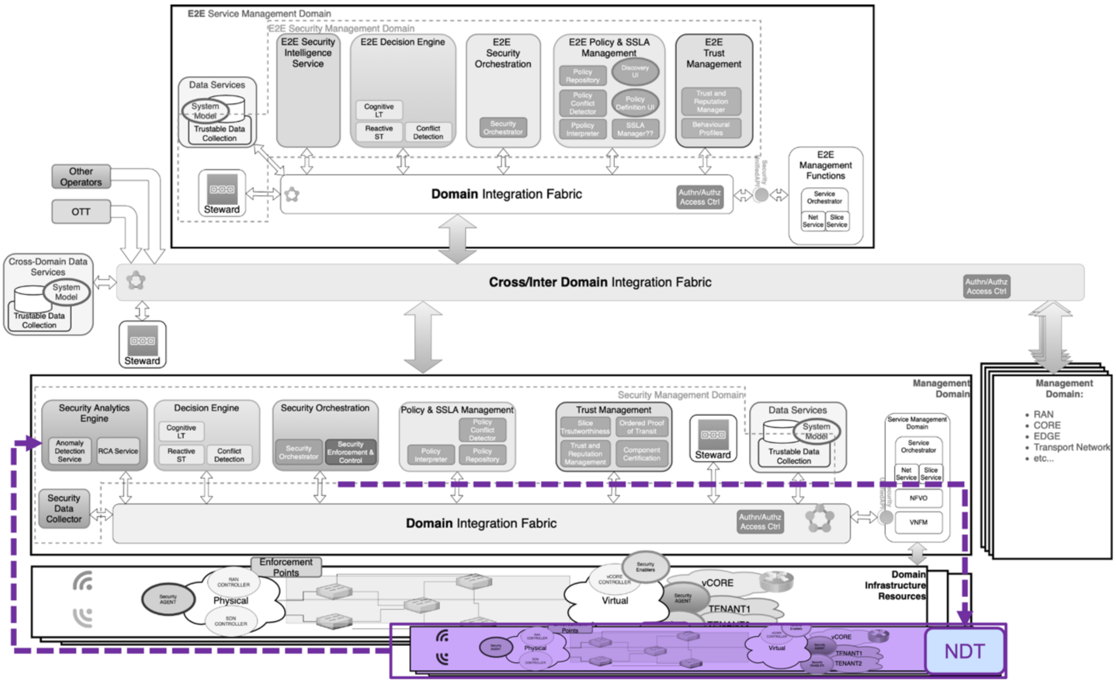


Figure 31. Integration of Mouseworld in the HLA

A NDT such as *Mouseworld* is represented as virtual environment of a network domain, and should be treated as an detached enabler from the HLA. Nonetheless, offline interactions with INSPIRE-5Gplus HLA is possible. The Security Orchestrator topologies jointly with Service Management Domain can be exported to the NDT, so it can reproduce some of the scenarios attacks and generate the associated data to train and deliver ML engines to the Security Analytics Engine.

6.3 Data collector

6.3.1 Problem statement and challenges

Data collection becomes a key piece in the E2E and close-loop management mechanisms. This step will support the other part of the management process and it should be able to collect as much information as possible. The more information the system owns, the larger knowledge it will have and the better decisions it will make. The problem arises when the infrastructure that is going to be managed is composed by multiple different data sources. Effective E2E monitoring requires a well-constructed data collector that is able to gather information from all parts of the system, no matter the nature of the data source. Current systems implement an ad-hoc model in which each data source is added to the data collector module in a very tight perspective. Thus, these solutions only fit to the management system for which it is built, and it does not follow standard interfaces that allows to interact with the whole system in a standard way.

This work relates the Security Gap, listed in D2.1 Chapter 5.7 table (Security Gaps), that requires to simplify the processing and selection of data telemetry and flows for the AI and ML technologies.

6.3.2 State of the art analysis

In the field of network telemetry and data collection, legacy models, such as SNMP protocol, despite to be supported is being surpassed by data modelling language YANG [RFC7950], to define the data organization and restriction over the data. The management and use these models in networks started with NETCONF and XML for codification [RFC6241]. State of the art today allows the network devices and enablers to choose between different codifications (XML, JSON or Protobuf) and transport protocols (NETCONF, RESTCONF, gRPC) to generate metrics. additional protocols and standards exists, such as Cisco Netflow v9 or IPFIX (RFC7011-15), with proprietary and customized templates.

6.3.3 Solution description and advancements

Security data collector sets up and launches the mechanisms for collecting and aggregating data from the different security agents, security enablers and network devices. The collector is based on different mechanisms such as telemetry models that enables access to real-time, model-driven, and analytics-ready data that can help with network automation, traffic optimization and preventive troubleshooting in networks. Apart from that, the natural variety of the data sources will require a highly scalable architectural framework for the security data collector implementation, with more data point granularity and superior performance. The following image represents a possible architectural framework to implement the security data collector.

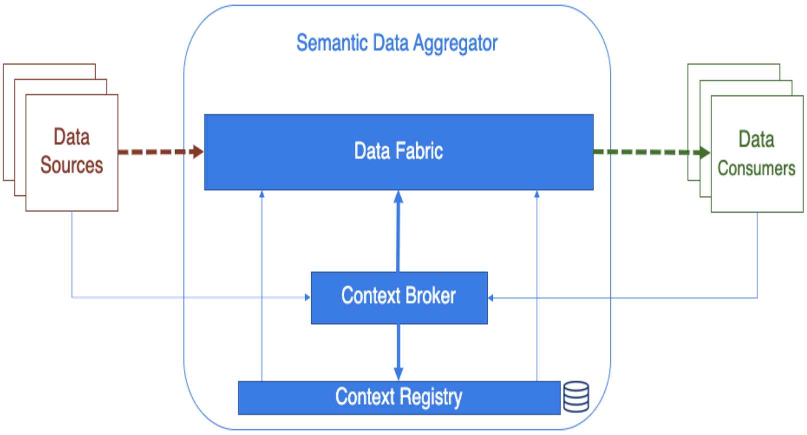


Figure 32. ETSI CIM based Framework Architecture

The data aggregator solution accepts multiples data sources and using a Data fabric the information can be transformed and aggregated to deliver to different data consumers. The Context broker and context registry are based on the framework architecture defined by ETSI ISG Context Information Management (CIM). This architecture allows addressing the lack of open and standardized approach for the exchange of context information. For this end, ETSI ISG CIM defines an open framework based on the use of RESTful APIs named NGSI-LD for a consistent, cross-cutting context exchange.

The data collector tool is adopted from ICT-19 project in 5Growth where an initial prototype is being created to monitor 5G performance, using infrastructure data sources. The INSPIRE-5Gplus progression focuses on developing the capacity to manage specific data sources for security needs. The output will be used for advanced functions in higher level, such as the Security Analytics service that provide security machine learning inference models or interact with data services that provides persistent storage for additional analysis of different security functions in each domain or in an end-to-end vision.

6.3.4 Integration-interaction with HLA enablers

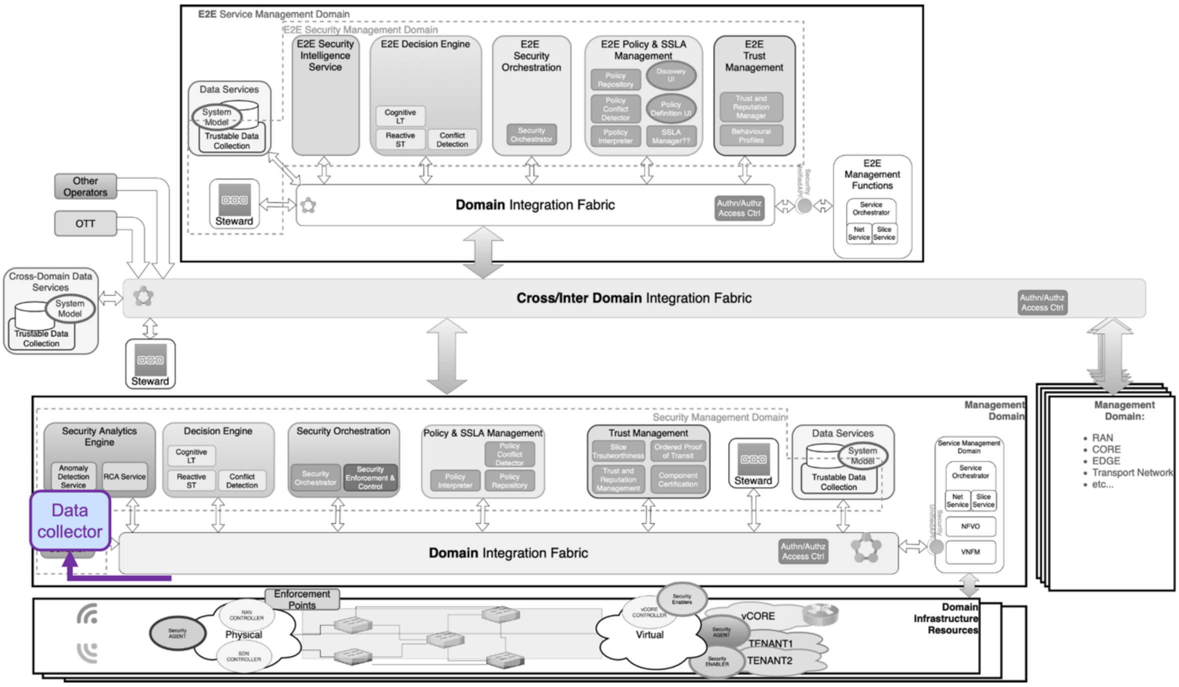


Figure 33. Integration of the Data Collector in the HLA

Data collector gather and aggregate some representative data sources from the network to be delivered to security analytic engine. The data sources could be part of the 5G network infrastructure, (for example NFVI or SDN controllers), a specific security agents (for example network probes, or security devices), VNFs, or directly from Service Management Domain (for example MANO monitoring modules such as *Prometheus*) The different data sources, and their associated metadata will be identify by the Data collector in each domain. Other enablers will be able to interact with Data Collector to require this information.

6.4 Smart Traffic Analysis

6.4.1 Problem statement and challenges

Pervasive E2E encryption is being progressively adopted in the network in the recent years. Specifically, the 3GPP R15 for 5G defines the Service Base Architecture (SBA) for signalling traffic and the use of Service Base Interfaces (SBI) implemented with HTTPS REST API as the reference protocol. The adoption of microservices and Cloud environment for 5G Core, Edge computing, and Central Offices, will lead to expose 5G critical services in shared environment, highly dynamic, with multiples versions, instances scaling up or down, internal connectivity, private address and NAT, etc. The lack of network monitoring capacity based on common tools such IDS or DPI will complicate the detection and mitigation of network attacks ante different TCP/IP levels. Also, it is well known that most of the attacks and malicious activity by malicious actors are being hide through encryption, especially with HTTPS.

This AI and ML based technology is proposed to solve the Security Gap, “AI-based threat detection over encrypted data flows” listed in D2.1 Chapter 5.7 (Security Gaps)

6.4.2 State of the art analysis

Network traffic related information is essential to leverage advanced machine learning techniques in the cybersecurity are[121]. The capacity to detect some attacks in specific fields of the cybersecurity are evolving to be close to real time[122].

Alternative method exists to identify and classify the HTTPS related traffic. Use Service Name Indication (SNI) [RFC 6066] provides info about the domain to reach (not the URL), and could provide hints on malicious activity. Additionally, fingerprinting technologies are proposed such as JA [123]that identify applications (including malware) based on the TLS extensions.

6.4.3 Solution description and advancements

Smart traffic analyser is a solution based on Machine Learning models based on network traffic analysis, using open source tool Tstat, to detect attacks over encrypted (HTTPS) traffic. Currently cryptomining traffic is supported and other malicious activities detection are planned. The solution can be deployed as a VNFs (Virtual Machine) that monitor the traffic and predict the traffic attack depending on the model loaded.

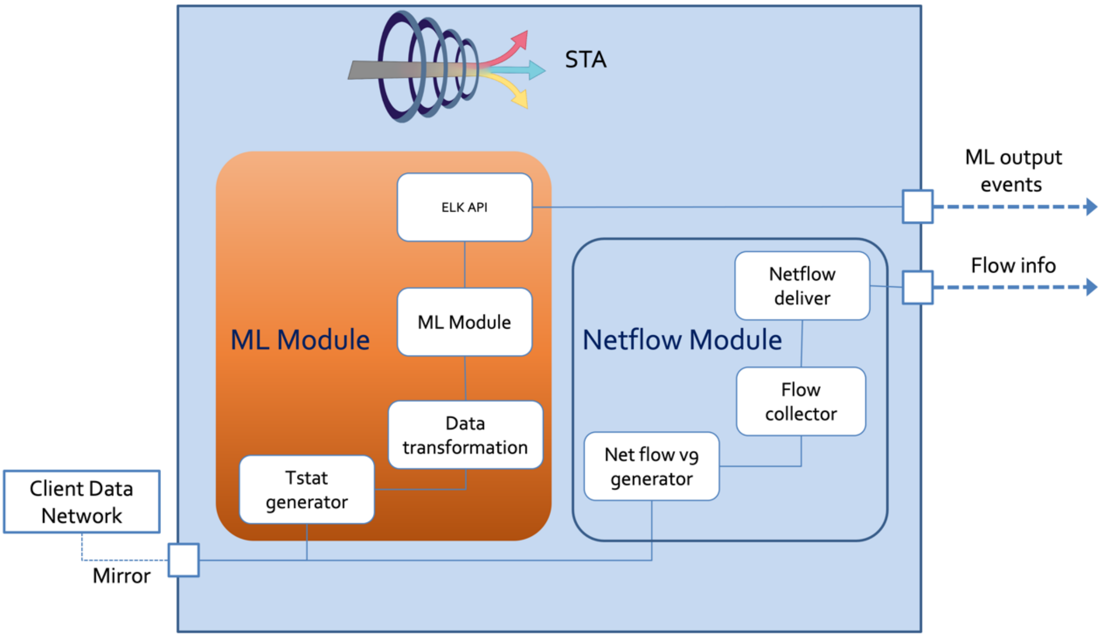


Figure 34: Smart Traffic Analyzer (STA) internal components

The solution is composed of a traffic capture (mirror or TAP), a flow aggregation and feature extraction and an AI inference engine, customized for detection at real-time. Events generate can be exposed through APIs to the management or the data collector.

Current version is implemented as a Linux virtual Machine and has the capacity to detect crypto-mining activity related with public mining pools using massively exploited scripts. Current work is focused in expand the functionality to make it modular to be able add new inference engines, through configuration files and support additional virtual environments (dockers).

Related to Security gaps identified in D2.1 Chapter 5.7, Smart Traffic Analysis relates to: Investigate one unexplored space: AI-based threat detection over encrypted data flows (as 50% of today traffic is encrypted, listed in Artificial Intelligence and Machine Learning technology.(Security Gaps)

6.4.4 Integration-Interactions with HLA enablers

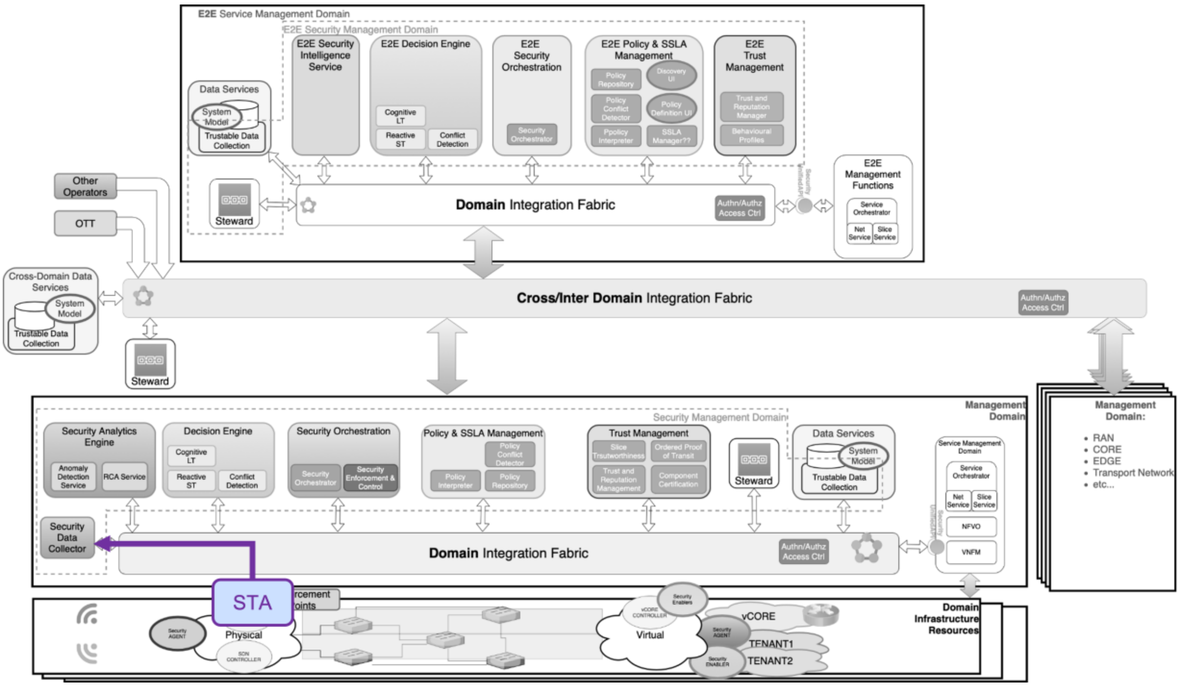


Figure 35: Integration of STAr in the HLA

STA acts as an intelligent probe that collect information from the network and deliver some aggregated metrics to the security data collector.

6.5 Baseline assets used in the project

The following assets will be used by partners as baseline assets in the development of their enablers:

1. Virtualised and Physical infrastructure telemetry (NCSRD), resulting from SHIELD project: Several types of monitoring probes plugged on physical or virtualized infrastructure. All captured records are sent to the E2E Monitoring Framework, providing an overall overview of the network.

7 Enabler to security gap mapping table

Below table shows for each Enabler which specific security gaps it solves or brings advancement. The security gaps have been identified in Deliverable D2.1 (Chapter 5.7 table) as the main areas of progress.

Enabler (Holder)	D2.1 Chapter 5.7 Security Gaps	Enabler Short Description
MOTDEC (ZHAW)	-MTD and Cyber Mimic Defence Techniques -Artificial Intelligence and Machine Learning	Solution for Moving Target Defense based slice protection for proactive security protection.
Cyber Threat Intelligence (MI)	-Cyber threat Intelligence and data sharing	ML techniques to aggregate information on malicious activity, detect anomalies in the network. Later on, will Include data from darknet and specialised honeypots deployed in the different network domains and verticals.
Stealthy DDoS Detection & Mitigation: (AALTO/UMU), composed of: A/ AI-based DDoS detection and mitigation in network slicing (AALTO) B/ Multi-domain Multi-tenant AI-based DoS detection (UMU)	-Artificial Intelligence and Machine Learning. Its first strand: Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats	A/ Application layer DDOS self-protection framework, capable of detecting stealth low noise DDoS adversarial attacks. The framework is a web-server including P4 switches management to block these DDOS attacks. B/ Solution coping with DoS detection in multi-tenancy context. The solution is a 3 modules structure, dealing respectively with real time monitoring, conversation processing and AI-inference attack detection, bringing the benefit of early-stage detection on traffic transit from edge to core.
Decision Engine (TSG)	-Automation and Zero-touch Service Management. -Artificial Intelligence and Machine Learning.	Oversees the different actions emitted by the security assets and the security analytic engine to select the best decisions to apply for securing a running targeted application. This centric component acts as an arbitrator between securities assets and the platform within a domain.
Security orchestrator (TSG, UMU)	-Automation and Zero-touch Service Management	Multi-domain security orchestrator. End-to-end meta-orchestrator of security assets on top of various levels of orchestration (network orchestration, service orchestration etc.) based on security policies and SSLAs
DiscØvery threat assessment (CLS)	-Cyber Threat Intelligence and Data Sharing. Its two first strands: Define the ad hoc usable sources for cyber threats to operators. -Devise how to move from a static threat landscape to evolving or new threats.	DiscØvery generates system policies and other high-level security improvements based on a model's information in the form of security insights. DiscØvery is a graphical security analysis tool for IoT and 5G systems, designed for system and policy analysis. Discovery is able to generate system policies and other high-level security improvements based on a

Enabler (Holder)	D2.1 Chapter 5.7 Security Gaps	Enabler Short Description
	-Consider the benefits of new risk assessment frameworks of complex ICT systems with notably the progress on risk assessment graph.	model's information in the form of security insights
Secured SSLA Manager (TSG)	-Automation and Zero-touch Service Management, -SD-SEC -SECaaS -Security Service Level Agreement	The solution deploys slices in a multi-VIM environment, make use of the SSLAs available in the SSLA manager by looking different option on how the SSLA may be applied within a Network Slice.
Secured Network Slice Manager for SSLAs (CTTC)	-Automation and Zero-Touch Service Management	Targeting SONATA and OSM MANOs, it delivers slice templates for several verticals. SONATA SP module is in charge to deploy and to manage the life-cycle of network slices. Among its possibilities, it can deploy slices in a multi-VIM environment (due to geographical or technological reasons like the use of VNF and CNF within the same slice).
Policy Framework (UMU)	-Multi MEC Security -Automation and Zero-touch Service Management -Security Service Level Agreement	Policy Framework is a policy based MEC management platform that automatically in a proactive or reactive manner, deploy and enforce Security Service Level Agreements by translating into security policies and this into specific security asset configurations.
SFSBroker (UOULU)	-DLT	Secure and federated slice brokering mechanism using a hierarchical blockchain to build reliable End-to-End network slices in a multi-operator platform.
KATANA slice manager (NCSRD)	-Automation and Zero-touch Service Management	Extended secure network slicing solution with support for Moving Target Defence, Slice Telemetry in order to integrate with the Sec Data Collector (SDC), integrity for the controlled southbound components and monitoring mechanisms for network slices that are being shared among different tenants/services.
vAAA (UMU)	-ZSM, -Authentication, - MEC security	VNF for AAA function to be deployed on demand at any part s of the network
OptSFC (ZHAW)	- Artificial Intelligence and Machine Learning -Automation and Zero-touch Service Management - MEC Security	Optimization theory applied to security function configuration, placement and chaining for detection and/or mitigation phases
Lightweight and Space efficient Authentication for V2X (CTTC)	-Vertical CCAM.	Delivers improvements on the 5G-AKA to minimize the signalling overhead involved in the authentication and security phase in 5G RAN

Enabler (Holder)	D2.1 Chapter 5.7 Security Gaps	Enabler Short Description
UAV anti GPS spoofing (AALTO)	-Artificial Intelligence and Machine Learning. Its first strand: --Devise efficient and effective AI-driven mechanisms for intelligently detecting Mitigating 5G security threats	ML powered detection of GPS spoofing
I2NSF IPSEC (TID)	-SDN security, SD-SEC and SECaaS	The solution is composed of a I2NSF controller and 2 o more IPsec agents. The I2NSF controller can be and application of a SDN Controller or part of the NFV MANO orchestration policies.
Virtual Channel protection (UMU)	-ZSM, -MEC security, -Multi-MEC security -Secure 5G radio access	The solution will allow instantiating and configuring on demand channel protection capabilities depending on the security requirements
Virtual Privacy CP-ABE (UMU)	-ZSM, -MEC security, -Multi-MEC security -Secure 5G radio access	The solution will allow instantiating and configuring on demand data privacy capabilities depending on the privacy requirements of the communication
MMT security monitoring framework and SSLA assessment and enforcement (MI)	Rule and behaviour-based intrusion detection integrating flexible probes and DPFI/CEP/CPD/ML (Deep Packet and Flow Inspection, Complex Event Processing, Change Point Detection, Machine Learning) analysis. Real-time SSLA assessment. Enabler of Automation and Zero-touch Service Management.	Monitoring framework with plug-in architecture to integrate parsers for analysing any structured information, embedded functions for adding analysis techniques, and dashboards for supporting custom visualisation and management. Specifying, managing and real-time assessment of SSLAs. Complex event processing and machine learning can be used to analyse and detect breaches at the local level by the Security Agents or at the domain or cross-domain level by the Security Analytics Engine.
Security analytics framework (NCSRD)	-Artificial Intelligence and Machine Learning	Collects, process, detects and classifies anomalies associated with security incidents, notifying the Security Administrators or other enablers across the INSPIRE-5Gplus ecosystem via appropriate APIs. Supports multiple data models for different technologies and vendors, as well as appropriate ML algorithms for detecting anomalies in multiple points of the network domains, increasing the overall detection accuracy.
MOUSEWORLD dataset generation. Network digital twin (TID)	-Artificial Intelligence and Machine Learning	Allows to make an offline dataset generation tool for training ML models by other tools and to validate performance models
Data collector (TID)	-Artificial Intelligence and Machine Learning. Fourth strand: --Telemetry. Simplification of the selection of data telemetry and flows for the AI and ML technologies.	Sets up and launches the mechanisms for collecting and aggregating data from the different security agents, security enablers

Enabler (Holder)	D2.1 Chapter 5.7 Security Gaps	Enabler Short Description
Smart traffic analyser (TID)	-Threat detection on encrypted traffic	ML model based on network traffic analysis to detect attacks over encrypted (HTTPS) traffic.

Table 1: Mapping of enablers to security gaps

A rapid analysis of Table 1 shows:

- All Security Gaps referring to WP3 are covered at least once by one (and often) several enablers. To be noted, WP4 enablements for trustworthy and liability-aware are not covered in this table.
- Several enablers are addressing one identical security gap with similar technology (e.g., SSLA manager or AI-based DDoS detection and mitigation). The table shows them in their diversity at the current stage. Further work and progress in the project will devise if and how separate enablers can be regrouped in one single enabler.

8 References

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

[2] Ankur Chowdhary, Adel Alshamrani, Dijiang Huang, and Hongbin Liang. 2018. “MTD Analysis and evaluation framework in Software Defined Network (MASON),” In Proc. of the 2018 ACM Int. Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Sec&apos;18). ACM, 43–48, 2018.

[3] S. Wang, Q. Pei, J. Wang, G. Tang, Y. Zhang and X. Liu, "An Intelligent Deployment Policy for Deception Resources

[4] https://sissden.eu/

[5] https://www.project-saint.eu/

[6] https://www.defense.gouv.fr/english/aid/actualites/challenge-synapse-les-deux-laureats

[7] Bahaa Al-Musawi, Philip Branch, Grenville Armitage:BGP Anomaly Detection Techniques: A Survey. IEEE Commun. Surv. Tutorials 19(1): 377-396 (2017)

[8] 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

[9] Praseed and P. S. Thilagam, “DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Appl.” IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661 – 685, 2019.

[10] C. Benzaid, M. Boukhalfa, and T. Taleb, “Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment,” in Proc. IEEE WCNC 2020, Seoul, Korea, Apr. 2020.

[11] N. Agrawal and S. Tapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3769-3795, Fourthquarter 2019

[13] C. Benzaid and T. Taleb, “AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?” in IEEE Network Magazine.

[14] Bosshart, Pat, et al. "P4: Programming protocol-independent packet processors." ACM SIGCOMM Computer Communication Review 44.3 (2014): 87-95.

[15] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020, doi: 10.1109/ACCESS.2020.2997702.

[16] NGMN 5G Security Network Slicing, NGMN Alliance, 2019.

[17] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," 2019 IEEE Conference on Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 82-90, doi: 10.1109/CNS.2019.8802852.

[18] F. Messaoudi, P. Bertin and A. Ksentini, "Towards the quest for 5G network slicing", Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC), pp. 1-7, Jan. 2020.

[19] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, et al., "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges", Proc. Federated Conf. Comput. Sci. Inf. Syst., pp. 783-792, Sep. 2017.

[20] A. Praseed and P. S. Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 661-685, Firstquarter 2019.

[21] W. Zhijun, L. Wenjing, L. Liang and Y. Meng, "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 43920-43943, 2020, doi: 10.1109/ACCESS.2020.2976609.

[22] ETSI GR ENI 001 V2.1.1 “Experiential Networked Intelligence (ENI); ENI Use Cases,

References:

[23] Raghavendra Chalapathy and Sanjay Chawla. Deep Learning for Anomaly Detection: A Survey. pages 1–50, 2019. URL http://arxiv.org/abs/1901.03407.

[24] Bashar Ahmed Khalaf, Salama A. Mostafa, Aida Mustapha, Mazin Abed Mohammed, and Wafaa Mustafa Abduallah. Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7:51691–51713, 2019. ISSN 21693536. doi: 10.1109/ACCESS.2019.2908998.

[25] Ana Serrano Mamolar, Zeeshan Pervez, Jose M. Alcaraz Calero, and Asad Masood Khattak. Towards the transversal detection of ddos network attacks in 5g multitenant overlay networks. Computers & Security, 79:132 – 147, 2018. ISSN 0167-4048. doi: 10.1016/j.cose.2018.07.017. URL http://www.sciencedirect.com/science/article/pii/S0167404818309313.

[26] S. Alzahrani, L. Hong, Detection of distributed denial of service (ddos) attacks using artifcial intelligence on cloud, Proceedings - 2018 IEEE World Congress on Services, SERVICES 2018 (2018) 37-38. doi:10.1109/SERVICES.2018.00031.

[27] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. M. del Rincón, and D. Siracusa. Lucid: A practical, lightweight deep learning solution for ddos attack detection. IEEE Transactions on Network and Service Management, 2019. doi: 10.1109/TNSM.2020.2971776.E2E ZSM Security Management

[28] ETSI. Zero-touch network and Service Management (ZSM); Reference Architecture. URL https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf.

[29] Kaushik Veeraraghavan and Justin Meza and Scott Michelson and Sankaralingam Panneerselvam and Alex Gyori and David Chou and Sonia Margulis and Daniel Obenshain and Shruti Padmanabha and Ashish Shah and Yee Jiun Song and Tianyin Xu. Maelstrom: Mitigating Datacenter-level Disasters by Draining Interdependent Traffic Safely and Efficiently. URL https://www.usenix.org/conference/osdi18/presentation/veeraraghavan

[30] Agathe Blaise, Mathieu Bouet, Vania Conan, Stefano Secci, “BotFP: FingerPrints Clustering for Bot Detection”, https://hal.archives-ouvertes.fr/hal-02501912/document

[31] PunchPlatform website: https://punchplatform.com/

[32] Kyriakos Kritikos, "Are Cloud Platforms Ready for Multi-cloud?," 8th IFIP WG 2.14 European Conference, ESOCC 2020, 28 September 2020.

[33] 5G Americas, "5G and the Cloud," December 201

[34] OSM RelEight Kubernetes Support: https://osm.etsi.org/docs/user-guide/06-osm-platform-configuration.html#platform-configuration-for-kubernetes

[35] B. Alexander, B. Uwe, F. Nicolas, R. Alessandro, S. Arnor, W. Manuel and L. Frank., "A Systematic Review of Cloud Modeling Languages," ACM Computing Surveys, 2018. https://events19.linuxfoundation.org/wp-content/uploads/2018/09/Evolving-Cloud-Native-Landscape-Dec-2018-ContainerDays-Japan.pdf

[36] Evolving Cloud Native Landscape, presentation by Chris Anisczyk, Cloud Native Computing Foundation. Container Days, Japan. December 2018. https://events19.linuxfoundation.org/wp-content/uploads/2018/09/Evolving-Cloud-Native-Landscape-Dec-2018-ContainerDays-Japan.pdf

[37] [http://www.anastacia-h2020.eu/

[38] Ahmad, Ijaz, et al. "Overview of 5G security challenges and solutions." IEEE Communications Standards Magazine 2.1 (2018): 36-43.

[39] Schneider, Peter, and Günther Horn. "Towards 5G security." 2015 IEEE Trustcom/BigDataSE/ISPA. Vol. 1. IEEE, 2015.

[40] Mellado, D., Fernández-Medina, E., and Piattini, M. (2007). A common criteria-based security requirements engineering process for the development of secure information systems. Computer Standards & Interfaces, 29(2):244–253.

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

[42] Bostrom, G., Wäyrynen, J., Bodén, M., Beznosov, K., and Kruchten, P. (2006). Extending xp practices to support security requirements engineering. Proceedings of the 2006 international workshop on Software engineering for secure systems – SESS ’06.

[43] Lipner, S. (2004). The trustworthy computing security development lifecycle. 20th Annual Computer Security Applications Conference, pages 2–13.

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

[45] Ji, Xinsheng, et al. "Overview of 5G security technology." Science China Information Sciences 61.8 (2018): 081301.

[46] V. Casola, A. D. Benedictis, M. Rak and U. Villano, "SLA-Based Secure Cloud Application Development: The SPECS Framework," 2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Timisoara, 2015, pp. 337-344, doi: 10.1109/SYNASC.2015.59.

[47] G. Karjoth, B. Pfitzmann, M. Schunter, and M. Waidner, Service-oriented assurance, comprehensive security by explicit assurances, in Quality of Protection, ser. Advances in Information Security, D. Gollmann, F. Massacci, and A. Yaut-siukhin, Eds., vol. 23. Springer US, 2006, pp. 13–24.

[48] M. Smith, M. Schmidt, N. Fallenbeck, C. Schridde, and B. Freisleben, Optimising Security Configurations with Service Level Agreements, in Proc. of the 7th International Conference on Optimization: Techniques and Applications (ICOTA 2007).IEEE Press, 2007, pp. 367–381.

[49] L. Wu and R. Buyya, Service Level Agreement (SLA) in Utility Computing Systems, in Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions, IGI Global, USA, 2011, pp. 1–25.

[50] NIST, “NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations,” 2013.

[51] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," 2019 IEEE Conference on Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 82-90, doi: 10.1109/CNS.2019.8802852.

[52] A. Marotta, D. Cassioli, M. Tornatore, Y. Hirota, Y. Awaji and B. Mukherjee, "Reliable Slicing with Isolation in Optical Metro-Aggregation Networks," 2020 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 2020, pp. 1-3.

[53] P.Alemany, D.Ayed, R.Vilalta, R.Muñoz, P.Bisson, R.Casellas, R.martínez, “Transport Network Slices with Security Service Level Agreements,” 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 2020.

[54] R. Vilalta, P. Alemany, R. Sedar, C. Kalalas, R. Casellas, R. Martínez, F. Vázquez-Gallego, J. Ortiz, A. Skarmeta, J. Alonso-Zarate, R. Muñoz, "Applying Security Service Level Agreements in V2X Network Slices," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Leganes - Madrid, Spain, 2020, pp. 114-115, doi: 10.1109/NFV-SDN50289.2020.9289861.

[55] A. L. Shaw, L. Jacquin, A. Lioy, C. Pitscheider, C. Basile, F. Risso, R. Bonafiglia, F. Ciacca, M. Nemirovsky, J. Kuusijärvi, D. Montero, R. Serral-Gracià, M. Yannuzzi, and F. Bosco, "Specification of the secured architecture (alpha version)," Tech. Rep.

[56] A. L. Shaw, L. Jacquin, A. Lioy, C. Pitscheider, C. Basile, F. Risso, R. Bonafiglia, F. Ciacca, M. Nemirovsky, J. Kuusijärvi, D. Montero, R. Serral-Gracià, M. Yannuzzi, and F. Bosco, "Policy specification" Tech. Rep.

[57] Lear, Droms, and Romascanu, "Manufacturer Usage Description Specification," RFC 8520, 2019. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8520.txt

[58] V. Jethanandani et al., "Yang data model for network access control lists (acls)," RFC 8519, March, Tech. Rep., 2019. [Online]. Available: https://tools.ietf.org/html/rfc8519

[59] Samdanis, K., Costa-Perez, X. and Sciancalepore, V., 2016. From network sharing to multi-tenancy: The 5G network slice broker. IEEE Communications Magazine, 54(7).

[60] Sciancalepore, V., Costa-Perez, X. and Banchs, A., 2019. RL-NSB: Reinforcement learning-based 5G network slice broker. IEEE/ACM Transactions on Networking, 27(4).

[61] Cunha, VA, Silva, E, Carvalho, MB, et al. Network slicing security: Challenges and directions. Internet Technology Letters. 2019; 2:e125. https://doi.org/10.1002/itl2.125

[62] NGMNAlliance.5GSecurityRecommendationsPackage#2:NetworkSlicing.NGMN2016.

[63]ETSINFV.NetworkFunctionsVirtualisation(NFV);NFVSecurity;ProblemStatement.ETSIGSNFV-SEC-0012014.

[64] 3GPPP, TR 33.811 Study on security aspects of 5G network slicing management

[65] 5GENESIS Project, 5th Generation End-to-end Network, Experimentation, System Integration, and Showcasing, On-oline: https://5genesis.eu

[66] Katana Slice Manager, On-line: https://github.com/5genesis/katana-slice_manager

References

[67] M. Kanda, Y. Ohba, S. Das, and S. Chasko, "Pana applicability in constrained environments,"

in Smart Object Security Wksp., 2012.

[68] B. Sarikaya, M. Sethi, and D. Garcia-Carillo, "Secure iot bootstrapping: A survey," Internet

Engineering Task Force, 2018.

[69] M. Kanda, Y. Ohba, S. Das, and S. Chasko, "Pana applicability in constrained environments,"

in Smart Object Security Wksp., 2012.

[70] B. Sarikaya, M. Sethi, and D. Garcia-Carillo, "Secure iot bootstrapping: A survey," Internet

Engineering Task Force, 2018.

[71] D. Garcia-Carrillo and R. Marin-Lopez, "Lightweight coap-based bootstrapping service for the

internet of things," Sensors, vol. 16, no. 3, 2016.

[72] Wong, S., Sastry, N., Holland, O., Friderikos, V., Dohler, M., & Aghvami, H. (2017). Virtualized authentication, authorization and accounting (V-AAA) in 5G networks. 2017 IEEE Conference on Standards for Communications and Networking (CSCN). doi:10.1109/cscn.2017.8088618

[73] Bin Han, Stan Wong, Mannweiler, C., Dohler, M., & Schotten, H. D. (2017). Security Trust Zone in 5G networks. 2017 24th International Conference on Telecommunications (ICT). doi:10.1109/ict.2017.7998270

[74] Molina Zarca, A., Garcia-Carrillo, D., Bernal Bernabe, J., Ortiz, J., Marin-Perez, R., & Skarmeta, A. (2019). Enabling Virtual AAA Management in SDN-Based IoT Networks †. Sensors, 19(2), 295. doi:10.3390/s19020295

[75] 3GPP. 2018. Study on authentication and key management for applications based on 3GPP credential in 5G (Work Item Description). https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=SP-180443.

[76] Mohsin Khan, Philip Ginzboorg, and Valtteri Niemi. 2019. Privacy Preserving AKMA in 5G. In Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop (SSR&apos;19). Association for Computing Machinery, New York, NY, USA, 45–56. DOI:https://doi.org/10.1145/3338500.3360337

[77] Bertsekas, D. P.,“Reinforcement Learning and Optimal Control”, Athena Scientific, July 2019.

[78] K. Arulkumaran, M. P. Deisenroth, M. Brundage and A. A. Bharath, "Deep Reinforcement Learning: A Brief Survey," IEEE Signal Processing Magazine, vol. 34, no. 6, pp. 26-38, Nov. 2017, doi: 10.1109/MSP.2017.2743240.

[79] Hessel, Matteo, et al. "Rainbow: Combining improvements in deep reinforcement learning." arXiv preprint arXiv:1710.02298 (2017).

[80] Heinrich, Johannes, and David Silver. "Deep reinforcement learning from self-play in imperfect-information games." arXiv preprint arXiv:1603.01121 (2016).

[81] ETSI TS 133 501 v15.4.0, “5G; Security architecture and procedures for 5G System ,” May 2019.

[82] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, “Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges,” IEEE Access, vol. 8, pp. 54314–54344, 2020.

[83] A. Dua, N. Kumar, A. K. Das, and W. Susilo, “Secure Message Communication Protocol Among Vehicles in Smart City,” IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4359–4373, 2018.

[84] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. Goutham Reddy, K. Park, and Y. Park, “Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks,” IEEE Access, vol. 5, pp. 14966–14980, 2017.

[85] C. Kalalas and J. Alonso-Zarate, “Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter," in Proc. of IEEE 5G World Forum 2020 (IEEE 5G-WF ’20), virtual event, September 2020.

[86] Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A. and Lachapelle, G., 2012. A low-complexity GPS anti-spoofing method using a multi-antenna array. aa, 2, p.2.

[87] Magiera, Jaroslaw, and Ryszard Katulski. "Detection and mitigation of GPS spoofing based on antenna array processing." Journal of applied research and technology 13, no. 1 (2015): 45-57.

[88] Psiaki, Mark L., Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. "GPS spoofing detection via dual-receiver correlation of military signals." IEEE Transactions on Aerospace and Electronic Systems 49, no. 4 (2013): 2250-2267.

[89] O'Hanlon, Brady W., Mark L. Psiaki, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. "Real-time GPS spoofing detection via correlation of encrypted signals." Navigation 60, no. 4 (2013): 267-278.

[90] Jansen, Kai, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina Pöpper, and Jens Schmitt. "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 1018-1031. IEEE, 2018.

[91] Wesson, Kyle, Mark Rothlisberger, and Todd Humphreys. "Practical cryptographic civil GPS signal authentication." NAVIGATION: Journal of the Institute of Navigation 59, no. 3 (2012): 177-193.

[92] Wu, Zhijun, Yun Zhang, and Rusen Liu. "BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication." IEEE Access 8 (2020): 23759-23775.

[93] Liu, Tianyuan, Avesta Hojjati, Adam Bates, and Klara Nahrstedt. "Alidrone: Enabling trustworthy proof-of-alibi for commercial drone compliance." In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 841-852. IEEE, 2018.

[94] Zhu, Haibei, Mary L. Cummings, Mahmoud Elfar, Ziyao Wang, and Miroslav Pajic. "Operator strategy model development in UAV hacking detection." IEEE Transactions on Human-Machine Systems 49, no. 6 (2019): 540-549.

[95] 3GPP TR 38.855. Study on NR Positioning Support. March 2019.

[96] NGMN. 5G E2E Technology to Support Verticals URLLC Requirements. 2019.

[97] W. Dargie, C. Poellabauer. Fundamentals of Wireless Sensor Networks: Theory and Practice. John Wiley & Sons, 2010.

[98] Lopez, R.; Lopez-Millan, G. Software-Defined Networking (SDN)-Based IPsec Flow Protection; Internet-Draft: draft-ietf-i2nsf-sdn-ipsec-flow-protection-03;Work in Progress; Internet Engineering Task Force: Fremont,CA, USA, 2018.

[99] Selander, G.; Mattsson, J.; Palombini, F.; Seitz, L. Object Security for Constrained RESTful Environments (OSCORE); Work in Progress; Internet Engineering Task Force: Fremont, CA, USA, 2018.

[100] Selander, G.; Mattsson, J.; Palombini, F. Ephemeral Diffie-Hellman Over COSE (EDHOC); Internet-Draft draft-selander-ace-cose-ecdhe-07; Work in Progress; Internet Engineering Task Force: Fremont, CA, USA, 2017.

[101] Molina Zarca, A., Garcia-Carrillo, D., Bernal Bernabe, J., Ortiz, J., Marin-Perez, R., & Skarmeta, A. (2019). Enabling Virtual AAA Management in SDN-Based IoT Networks †. Sensors, 19(2), 295. doi:10.3390/s19020295

[102] Bethencourt, J.; Sahai, A.;Waters, B. Ciphertext Policy Attribute Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.ISSN: 2375-1207, doi:10.1109/SP.2007.11.

[103] S. P´erez, J. L. Hern´andez-Ramos, S. N. Matheu-Garc´ıa, D. Rotondi, A. F. Skarmeta, L. Straniero, and D. Pedone, "A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios," IEEE Access, vol. 6, pp. 11 738–11 750, 2018.

[104] Matheu, S. N., Robles Enciso, A., Molina Zarca, A., Garcia-Carrillo, D., Hernández-Ramos, J. L., Bernal Bernabe, J., & Skarmeta, A. F. (2020). Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems. Sensors, 20(7), 1882. doi:10.3390/s20071882

[105] Lee,Raymond, Mahadevan, Gomathisankaran: Ontology of Secure Service Level Agreement

. HASE 2015: 166-172

[106]Elena Lisova, Mohammad Ashjaei, Syed Usman Ashgar: On Incorporating Security Parameters in Service Level Agreements. CLOSER 2019: 48-57

[107] Neminath Hubballi, Amey Kiran Patel, Amit Kumar Meena, Nikhil Tripathi: Cloud Security Service Level Agreements: Representation and Measurement. INFOCOM Workshops 2019: 145-150

[108] Sultan Alasmari, Weichao Wang, Tuanfa Qin, Yu Wang: Proof of Encryption: Enforcement of Security Service Level Agreement for Encryption Outsourcing. DSC 2019: 1-8

[109] Erkuden Rios, Eider Iturbe, Xabier Larrucea, Massimiliano Rak, Wissam Mallouli, Jacek Dominiak, Victor Muntés, Peter Matthews, Luis Gonzalez: Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems. IET Softw. 13(3): 213-222 (2019)

[110] P. Mishra, V. Varadharajan, U. Tupakula and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 686-728, Firstquarter 2019, doi: 10.1109/COMST.2018.2847722.

[111] INSPIRE-5Gplus Consortium, "D2.1: 5G Security: Current Status and Future Trends," 2020, [Online], Available: https://www.inspire-5gplus.eu/wp-content/uploads/2020/05/i5-d2.1_5g-security-current-status-and-future-trends_v1.0.pdf [Accessed October 2020]

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

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

[114] Z. Li, Y. Ouyang, L. Su, W. Jiang, Y. Hu and Z. Lin, "Detecting traffic anomaly in wireless networks, an analytics methodology," 2018 Wireless Telecommunications Symposium (WTS), Phoenix, AZ, 2018, pp. 1-6, doi: 10.1109/WTS.2018.8363936.

[115] Leichtnam L., Totel E., Prigent N., Mé L. (2020) Sec2graph: Network Attack Detection Based on Novelty Detection on Graph Structured Data. In: Maurice C., Bilge L., Stringhini G., Neves N. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2020. Lecture Notes in Computer Science, vol 12223. Springer, Cham. https://doi.org/10.1007/978-3-030-52683-2_12

(116] https://spot.apache.org/

[117] https://5genesis.eu/wp-content/uploads/2021/03/5GENESIS_D3.14_v.1.0.pdf

[118] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122.

[119]Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set.In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications(CISDA), Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.

[120] Canadian Institute for Cybersecurity. Available online: https://www.unb.ca/cic/datasets/index.html

[121] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122.

[122] Pastor, A., Mozo, A., Vakaruk, S., Canavese, D., López, D. R., Regano, L., ... & Lioy, A. (2020). Detection of encrypted cryptomining malware connections with machine and deep learning. IEEE Access.

[123] Gancheva, Zlatina, Patrick Sattler, and Lars Wüstrich. "TLS Fingerprinting Techniques." Network 15 (2020)

[124] https://www.musa-project.eu/

[125] https://www.celticnext.eu/project-sendate-tandem/
[126] Secure Access Service Edge. https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

[127] IETF RFC 4301. https://tools.ietf.org/html/rfc4301

[128] draft-ietf-i2nsf-sdn-ipsec-flow-protection-08. https://tools.ietf.org/html/draft-ietf-i2nsf-sdn-ipsec-flow-protection-08

[129] Project SENDATE-TANDEM (CELTIC-NEXT), D4.4.1 Security as a Service concepts and applicability, Design & SLA,2019

[130] CyberLens/Discovery. (2021). Retrieved 27 April 2021, from https://github.com/CyberLens/Disc0very

[131] Seunghyun Yoon, Jin-Hee Cho, Dong Seong Kim, Terrence J. Moore, Frederica F. Nelson, Hyuk Lim, Nandi Leslie, and Charles Kamhoua, "Moving target defense for in-vehicle software-defined networking: IP shuffling in network slicing with multiagent deep reinforcement learning", Proc. SPIE 11413, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II, 114131U (21 April 2020).

[132] Shetty, Sachin & Yuchi, Xuebiao & Song, Min. (2016). Moving Target Defense for Distributed Systems. Springer International Publishing, 2016.

[133] Jason R. Hamlet and Christopher C. Lamb. 2016. "Dependency Graph Analysis and Moving Target Defense Selection," In Proceedings of the 2016 ACM Workshop on Moving Target Defense (MTD '16). ACM, 105–116.

[134] Sridhar Venkatesan, Massimiliano Albanese, George Cybenko, and Sushil Jajodia. 2016. "A Moving Target Defense Approach to Disrupting Stealthy Botnets" In Proceedings of the 2016 ACM Workshop on Moving Target Defense (MTD '16). ACM, New York, NY, USA, 37–46.

[135] D. P. Sharma, J. Cho, T. J. Moore, F. F. Nelson, H. Lim and D. S. Kim, "Random Host and Service Multiplexing for Moving Target Defense in Software-Defined Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.

[136] E. Serrano-Collado, M. García-Valdez and J. J. Merelo-Guervós, "Improving evolution of service configurations for moving target defense," 2020 IEEE Congress on Evolutionary Computation (CEC), Glasgow, United Kingdom, 2020, pp. 1-8.

[137] Hooman Alavizadeh, Dong Seong Kim, Julian Jang-Jaccard, "Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud," Future Generation Computer Systems, Volume 111, 2020, Pages 507-522.

[138] R. Peretz, S. Shenzis and D. Hay, "Moving Target Defense for Virtual Network Functions," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2020, pp. 1-9.

[139] Bagaa, J. B., Taleb, Zarca, A. M., A. F. (2020).Final Security Orchestrator Report. Anastacia H2020 European project deliverable D, 3.5

[140] Zarca, A. M., Bagaa, M., Bernabe, J. B., Taleb, T., & Skarmeta, A. F. (2020). Semantic-aware security orchestration in SDN/NFV-enabled IoT systems. Sensors, 20(13), 3622.

[141] Zarca, A. M., Bernabé, J. B., Ortíz, J., & Skarmeta, A. Policy-based Definition and Policy for Orchestration Final Report. Anastacia H2020 European project deliverable D, 2.1

[142] Zarca, A. M., Bernabé, J. B., Ortíz, J., & Skarmeta, Final Security Enforcement Manager Report. Anastacia H2020 European project deliverable D, 3.4

Appendix A Security gaps (Abstract of D2.1, para 5.7)

Each enabler described in the present document refers to the Security Gaps as identified in the table below and resulting from the analysis work as part of Task 2.1 and listed in its paragraph 5.7 (table) as below. The table includes both WP3 and WP4 security gaps while the present document covers only WP3 security gaps.

Technology	Security Gap. Progress axis	WPs
Artificial Intelligence and Machine Learning	• Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats. • Investigate one unexplored space: AI-based threat detection over encrypted data flows (as 50% of today traffic is encrypted). • Tackle with the concept of Network Digital Twins. • Tackle with the concept of (data) streaming telemetry (based on Yang-based model) to ease and experiment the selection and processing of most relevant and restricted data flow (best qualifiers).	WP3 WP4
Authentication	• Lack of coordinated authentication processes for services and consumers for multi-domain applications	WP3
Automation and Zero-touch Service Management	• Define a minimal viable ZSM, avoiding the "calamity of over-arching solutions", which spans over a complete E2E slice over several domains. Practical implementations delivering measured improved security are to be drawn and implemented. • Comprehend the research and standardization works by ETSI and ITU-T: GANA architecture, ZSM concept and its derivations at ONAP and OSM frameworks, ENI working group, ITU FG-ML5G and its unified high-level architecture (ML pipeline, ML sandbox and ML function orchestrator).	WP3
Cyber threat intelligence and data sharing	• Define the ad hoc usable sources for cyber threats to operators. • Devise how to move from a static threat landscape to evolving or new threats. • Consider the benefits of new risk assessment frameworks of complex ICT systems with notably the progress on risk assessment graph.	WP3
DLT	• Devise pragmatic paths to DLT usage over the networks over three possible implementations: DDoS attacks, AAA and SLA management.	WP4
Dynamic Liability and Root Cause Analysis (based on ML)	• Deliver fast and timely faulty source information. • Ability of the RCA to grasp the network structure (model representation) ever evolving. • Devise the most relevant learning and diagnostic methods-approaches with a special focus on Deep learning • Reduce the domain space to highly signing datasets only. • Define the most relevant network status indicators, possibly with the help of Principal Component Analysis.	WP4
Formal method applied to network authorization enforcement	• Devise and define how these techniques (as defined in the SoTA) can be deployed in a multi VNF where security is AI-defined. • Confront and define possible convergence (associated use) for the paradigms of formal method and AI processing.	WP3
MEC security	• More exposed to introspection, MEC security is a main concern. Devise a resource-efficient security solutions resident in the MEC	WP3
MTD and Cyber Mimic Defence Techniques	• Devise the real benefits of these techniques (which by-default generate network structure automatic variations and instabilities) when applied in a complex multi-domain, multi-operator, multi-tenant and cross slice scenario (with their set of security constraints). • AI for MTD	WP3
Multi-MEC Security	• Lack of integration and inter-working of MEC and associated MEC platform management	WP3
NFVI, VNF, MANO and interface security (API	• Investigate the security and the performance of latest controller North Bound and South Bound APIs including NETCONF, TAPI, JOX	WP3

SDN security, SD-SEC and SECaaS	• Investigate how software security service (dealing with Identify, Protect, Detect, Respond and Recover) can be expanded in a multi domain/multi-tenant environment.	WP3
Secure 5G radio access	• Devise and define a smart (more secure for delivering both confidentiality and integrity, performance acceptable, easy workflow) E2E data flow encryption.	WP3
Securing Artificial Intelligence - SAI	• Embrace, comprehend and advance the works made at ETSI Industry Specification Group on securing artificial intelligence 3ISG SAI)	WP4
Security service level agreement	• Define an open (i.e., adaptive to any liable parties of the agreement), dynamic (i.e., QoS or security rules can evolve) and secure SLA template management framework enabling SLA in the context of the varying 5G services and of the complexity and size of a service value chain (made up of several suppliers).	WP3
Security solutions oriented towards verticals	• Devise solutions for securing network slicing and hardware root of trust (when highly security-sensitive OT in vital infrastructure are concerned)	WP3
Service isolation	• Lack of secure hardware infrastructure to deploy isolated services.	WP3
Trust models and liability analysis in 5G	• Devise a trust management solution and its associated processed metrics, inputs, aggregation methods delivering accurate and pertaining trust level assessment in the context of 5G complex service value chain. • Grasp the concept of forwarding accountability and strong accountability concepts to elaborate trustworthiness. • Grasp the work related to liability expressiveness (and associated domain specific language) as well as delegation of obligation • Grasp the practical aspects on defective algorithm accountability, packet proof of transit (how effective, benefits and trustworthiness of brought information.	WP4
Trusted Execution Environments	• Define a smart way to bring to network functions provable integrity and confidentiality guarantees, through a by-default, zero-touch workflow, generating low overhead.	WP3