2

Key Innovations in ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures

Jorge Bernal Bernabe[1], Alejandro Molina[1], Antonio Skarmeta[1], Stefano Bianchi[2], Enrico Cambiaso[3], Ivan Vaccari[3], Silvia Scaglione[3], Maurizio Aiello[3], Rubén Trapero[4], Mathieu Bouet[5], Dallal Belabed[5], Miloud Bagaa[6], Rami Addad[6], Tarik Taleb[6], Diego Rivera[7], Alie El-Din Mady[8], Adrian Quesada Rodriguez[9], Cédric Crettaz[9], Sébastien Ziegler[9], Eunah Kim[10], Matteo Filipponi[10], Bojana Bajic[11], Dan Garcia-Carrillo[12] and Rafael Marin-Perez[12]

[1]Department of Information and Communications Engineering, University of Murcia, Murcia, Spain
[2]Research & Innovation Department, SOFTECO SISMAT SRL, Di Francia 1 – WTC Tower, 16149, Genoa, Italy
[3]National Research Council (CNR-IEIIT) – Via De Marini 6 – 16149 Genoa, Italy
[4]Atos Research and Innovation, Atos, Calle Albarracin 25, Madrid, Spain
[5]THALES Communications & Security SAS, Gennevilliers, France
[6]Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland
[7]R&D Department, Montimage, 75013, Paris, France
[8]United Technologies Research Center, Ireland
[9]Mandat International, Research, Switzerland
[10]Device Gateway SA, Research and Development, Switzerland
[11]Archimede Solutions, Geneva, Switzerland
[12]Department of Research & Innovation, Odin Solutions, Murcia, Spain
E-mail: jorgebernal@um.es; alejandro.mzarca@um.es; skarmeta@um.es; stefano.bianchi@softeco.it; enrico.cambiaso@ieiit.cnr.it; ivan.vaccari@ieiit.cnr.it; silvia.scaglione@ieiit.cnr.it; maurizio.mongelli@ieiit.cnr.it; ruben.trapero@atos.net;

mathieu.bouet@thalesgroup.com; dallal.belabed@thalesgroup.com;
miloud.bagaa@aalto.fi; rami.addad@aalto.fi; tarik.taleb@aalto.fi;
diego.rivera@montimage.com; madyaa@utrc.utc.com;
aquesada@mandint.org; ccrettaz@mandint.org; sziegler@mandint.org;
eunah.kim@devicegateway.com; mfilipponi@devicegateway.com;
bbajic@archimede.ch; dgarcia@odins.es; rmarin@odins.es

This book chapter presents the main key innovations being devised, implemented and validated in the scope of Anastacia H2020 EU research project, to meet the cybersecurity challenge of protecting dynamically heterogenous IoT scenarios, endowed with SDN/NFV capabilities, which face evolving kind of cyber-attacks. The key innovations encompasses, among others, policy-based security management in IoT networks, trusted and dynamic security orchestration of virtual networks security functions using SDN/NFV technologies, security monitoring and cognitive reaction to countering cyber-treats, behavioural analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments as well as secured and authenticated dynamic seal system as a service.

2.1 Introduction

The Internet of Things (IoT) aims to leverage network capabilities of devices and smart objects, integrating the sensing and actuation features to create pervasive information systems, which are used as baseline to provide smart services to the industry and citizens. However, as a greater number of constrained IoT devices are connected to Internet, the security and privacy risks increase accordingly. The boosted connectivity and constrained capabilities of devices in terms of memory, CPU, memory, battery, the unattended behaviour of IoT devices, misconfigurations and lack of vendor support, increase potential kinds of vulnerabilities. Therefore, new advanced security frameworks for IoT deployments are needed to face these threats and meet dynamically the desired defence levels.

H2020 Anastacia EU project addresses the security management of heterogenous and distributed IoT scenarios, such as Smart Buildings or Smart Cities, which can benefit from a policy-based orchestration and security management approach, where NFV/SDN-based solutions and novel

monitoring and reaction tools are combined to deal with new kind of evolving cyber-attacks.

ANASTACIA is developing new methodologies, frameworks and support tools that will offer resilience to distributed smart IoT systems and Mobile Edge Computing (MEC) scenarios against cyber-attacks, by leveraging SDN and NFV technologies. Security VNFs can be timely and dynamically orchestrated through policies to deal with heterogeneity demanded by these distributed IoT deployments that can be deployed either at the core of at the edge, in VNF entities, to rule the security in IoT networks. Dynamic and reactive provisioning of Security VNFs towards the edge of the network can enhance scalability, necessary to deal with IoT scenarios.

The primary objective of the ANASTACIA project is to address cyber-security concerns by researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on Internet of Things (IoT) and Cloud architectures.

The heterogeneous, distributed and dynamically evolving nature of CPS based on IoT and virtualised cloud architectures introduces new and unexpected risks that can be only partially solved by current state-of-the-art security solutions. Innovative paradigms and methods are required i) to build security into the ICT system at the outset, ii) to adapt to changing security conditions, iii) to reduce the need to fix flaws after deploying the system, and iv) to provide the assurance that the ICT system is secure and trustworthy at all times. ANASTACIA is thus developing, integrating and validating a security and privacy framework that will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools.

Dealing with this general ambition and scenario raises several research challenges, being faced in Anastacia:

- Interoperable and scalable IoT security management: dealing with the level of abstraction, the language and new security models, contextual IoT aspects in policies, particularities in IoT security models, policy conflicts and dependencies in orchestration policies.
- Optimal selection of SDN/NFV-based security mechanisms: allocate multiple VNF requests on an NFV Infrastructure, especially in a cost-driven objective.
- Orchestration of SDN/NFV-based security solutions for IoT environments: the selection of the adequate mitigation plan and the fast

enforcement of the defined policies, as well as orchestration and the enforcement of the adequate countermeasures in a short time.
- Dealing with a new kind of cyber-attacks in IoT: providing advanced security from last generation threats on IoT environments.
- Learning decision model for detecting malicious activities: the development of novel defence and resilient detection techniques.
- Hybrid security monitoring for IoT enhanced with event correlation: The application of both signature-based and behavioural-based security analysis for IoT.
- Quantitative evaluation of incidents for mitigation support: combination of several factors to evaluate incidents to decide on the most convenient mitigation plan to enforce.
- Construction of a dynamic security and privacy seal that secures both organizational and technical data: generate trust by considering technical insights on security and privacy personal data protection requirements.

This chapter describes the main key innovations being devised, implemented and evaluated in the scope of ANASTACIA to cope with the aforementioned security challenges in IoT scenarios.

2.2 The Anastacia Approach

2.2.1 Anastacia Architecture Overview

The NIST Cybersecurity Framework identifies five steps for the protection of critical infrastructures: Identification, protection, detection, response and recovering. In general, these three steps are supported by the retrieval and management of security information extracted from the infrastructure to protect. On top of the five steps of the NIST Cybersecurity Framework, we can overlap the three main activities in what regards to the data lifecycle in ICT infrastructures for security protection, namely the data acquisition, data dissemination, data consumption and data processing. Data acquisition includes of the components and mechanisms to retrieve relevant data from the infrastructure, such as logs, heartbeats or reports. Data Dissemination regards to the elements that allow to distribute or store the acquired data among the relevant components of the infrastructure, such as monitoring agents, document or software repositories. Data consumption refers to the components involved in the usage of such data, either for its correlation, patterns finding for incident detection or forensic analysis. Finally, data

processing carries out activities based on the result obtained by the data consumers, such as mitigation actions to react to the incidents detected, their enforcement or the creation of security and privacy seals that inform about the security and privacy level of the platform.

The ANASTACIA approach is based on the flow and management of data gathered from IoT infrastructures. Following the aforementioned model, ANASTACIA designs and uses proper mechanisms to retrieve information from the underlying infrastructure and accurate ways to interpret it them to know the real status of the infrastructure and to make accurate decisions based to automatically react to incidents. ANASTACIA relies on the concept of automation when referring to the dynamic protection against security incidents, considering the cycle depicted in Figure 2.1 for identifying sources of relevant security information, deployment of security probes for the protection of IoT infrastructures, the detection of security incidents, responding to them by generating security alerts that are used to enforce mitigation actions to recover from the detected security incidents.

To this end ANASTACIA has designed a plane-based architecture [1] where the information flows from the data acquisition from the IoT infrastructure to their dissemination and consumption by the monitoring infrastructure and to the data processing by the reaction module to decide about mitigations to enforce. Figure 2.2 represents the plane-based approach of ANASTACIA. On top of the data plane, which represents the data to obtain from the IoT infrastructure, and on top of the control plane, which represents the

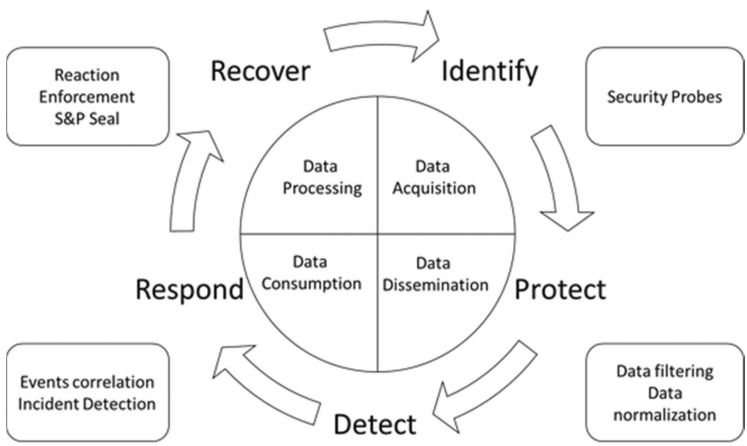

Figure 2.1 Main stages of ANASTACIA framework.

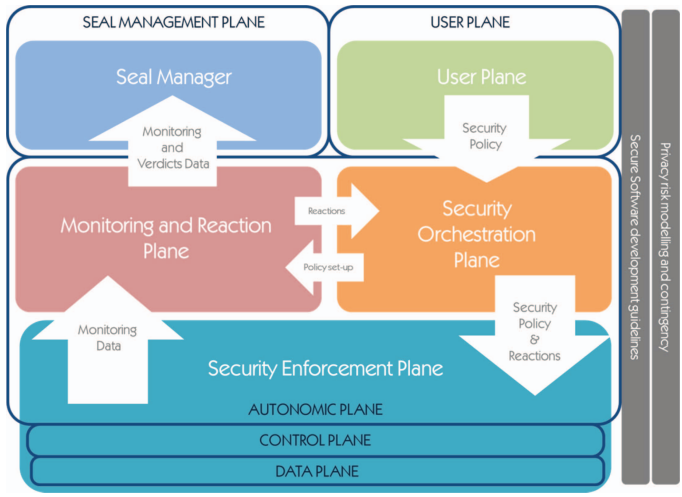

Figure 2.2 Anastacia high-level architectural view.

elements (software defined networks or virtual network functions) that allows to interact with the IoT infrastructure, are: (i) the enforcement plane that uses the control plane to obtain monitoring data from the infrastructure, (ii) the monitoring and reaction plane, which correlates the monitoring data to detect incidents and propose reactions to mitigate them, (iii) the security orchestration plane, which enforce the reactions using the enforcement plane. On top of them, the Seal Management plane uses monitoring data and reactions to provide with a snapshot of the security and privacy level of the infrastructure, and the user plane that provides interaction with human administrators for the establishment of security policies.

2.3 Anastacia Main Innovation Processes

2.3.1 Holistic Policy-based Security Management and Orchestration in IOT

In distributed smart IoT deployments scenarios like those previously described, the system security management is crucial. At this point, it is important to highlight that to the diversity of the current systems and services they are added a vast amount of different devices in the IoT domain, being the latter quite different among the previous approach and even among themselves. From this point of view, the current state of art shows that it is highly valuable to provide different levels of security policies to provide

different levels of abstraction for different profiles of management. It is also important to highlight the difference between generic models and specific extensible models, as well as to remark then relevance of policy orchestration features and policy conflict detection. Main ANASTACIA's contributions on policies reside in the unification of relevant, new and extended capability-based security policy models (including ECA features), as well as policy orchestration and conflict detection mechanisms, all under a unique policy framework. To this aim, the holistic policy-based solution provides different components and features like **Policy Models**, **Policy Editor Tool**, **Policy Repository**, **Policy Interpreter**, **Policy Conflict Detection** and **Policy for Orchestration**.

ANASTACIA's **Policy Models** thus improve the current state of the art as well as provide novelty approaches to be able to increase the security measures and countermeasures in the whole system at different levels. To this aim, ANASTACIA adopts and extend concepts and features from the state of art, to provide a unified security policy framework. I.e., ANASTACIA involves and evolves previous works by extending the already existing features as well as by providing new IoT-focused features.

The Policy Models can be instantiated using the **Policy Editor Tool** which allows defining security policies at a high-level of abstraction through a friendly GUI. In this way, the security administrator is able to manage the security of the system by instantiating new security policies, as well as supervise the existing security policies by the Policy Repository. **The Policy Repository** registers all policy operations as well as the current status for each one. It also provides valuable policy templates to make the security management easier.

Since the security policies are instantiated in a High-level Security Policy Language (HSPL), it must be transformed in configurations for the specific devices which will enforce the security policy. To this aim, the **Policy Interpreter** is able to refine the HSPL in one or several Medium-level Security Policy Language (MSPL) policies depending on a set of identified capabilities (filtering, forwarding, etc.). This process transforms the high-level concepts into more detailed parameters but still independent to the specific technologies. Finally, these MSPL policies are translated in final configurations using specific translator plugins for each technology. Once the configurations have been obtained, they can be enforced in the specific security enablers, understanding a security enabler as a piece of hardware or software able to implement a specific capability. Of course, a security policy only can be enforced if it does not present any kind of conflict with the already

enforced ones. In this sense the **Policy Conflict Detection** engine verifies that the new security policy will not generate conflicts like redundancy, priorities, duties (e.g. packet inspection vs channel protection), dependences or contradictions. To this aim, the security policy is processed against the rule engine which extracts context information from the policy repository and the system model to perform the necessary verifications.

Regarding the dependences, ANASTACIA also includes as part of the policy model the Policy for Orchestration concept. The **Policy for Orchestration** model allows the security administrator to specify how a set of security policies must be enforced by defining priorities and dependencies, where a security policy can depend on other security policies or even in system events like an authentication success.

Through these components and features, the policy-based ANASTACIA framework aims to cope with research challenges related with interoperability and scalability IoT security management. That is, the policy-based approach aims to deal with the heterogeneity and scalability by defining different level of abstractions, models and translation plugins. In this way, the scalability is also benefited since the policy-based approach with a high-level of abstraction makes easier to manage a large amount of devices. The policy conflict detection allows the framework to deal with several conflict types, and finally the policy for orchestration considers policy chaining by priority or dependencies to cover an orchestration plan.

Currently, the project is validating the related components and features by experimenting on IoT/SDN/NFV Proof of Concepts for different security capabilities like authentication, authorization and accounting (AAA), filtering, IoT management, IoT honeynet and channel protection as it can be seen in the research outcomes.

Regarding the research outcomes and associated publications, [2] provides a first PoC performance evaluation focused on a sensor isolation through different SDN controllers as well as a traditional firewall approach. [3] shows the potential of the policy-based framework focused on a AAA scenario. The paper entitled "Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks" shows the dynamic deployments of IoT-honeynet networks on demand by replicating real IoT environments by instantiating the ANASTACIA IoT-honeynet policy model. It also provides performance for different kind of IoT devices and topologies. In [1], the authors present the architecture focusing on the reaction performance of the policy-based framework.

2.3.2 Investigation on Innovative Cyber-threats

The CNR team involved in ANASTACIA has multi-year experience in the cyber-security field, concerning both the development of innovative cyber-attacks and intrusion detection algorithms. By exploiting the knowledge of the team, in the ANASTACIA context, deep work has been accomplished in the cyber-security context. Such work led to the identification of two innovative threats, related to the IoT and Slow DoS Attacks contexts. The novelty of such threats is demonstrated by their acceptance from the research world [4, 5]. In the following, based our description on the published works just mentioned and on the descriptions reported in the project deliverables, the introduced new attacks are briefly described (how they work and how it is possible to protect from them).

2.3.2.1 IoT 0-day attack

Being exchanged information extremely sensitive, due to the nature of IoT devices and networks, security of IoT systems is a topic to be investigated in deep. The work behind the proposed attack goes in this direction, by investigating the domotic IoT context and exploiting its components, to identify weaknesses that attackers may exploit.

The proposed attack is part of the ZigBee security context. ZigBee is a wireless standard introduced by the ZigBee Alliance in 2004 and based on the IEEE 802.15.4 standard, used in the Wireless Personal Area Networks (WPAN) context [6]. In particular, we identified a particular vulnerability affecting AT Commands capabilities implemented in IoT sensor networks. Our work focuses on the exploitation of such weakness on XBee devices, supporting remote AT commands, exploited to disconnect an end-device from the ZigBee network and make it join a different (malicious) network and hence forward potentially sensitive data to third malicious parties. Given the nature of IoT end-devices, often associated with a critical data and operations, it may be obvious how a Remote AT Command attack represents a serious threat for the entire infrastructure. Early evaluation of the effects of the proposed attack on a real network led to validate the success of the proposed threat [4]. Obtained results prove the efficacy of the proposed attack.

Moreover, since just a single packet is sent to the victim by the attacker to reconfigure it, the proposed attack should be considered as dangerous as scalable. Particularly, the time required to send such packet is minimal, so in case of multiple targeted sensors, the attack success is guaranteed.

By adopting an external level protection approach [4], the protection system is directly employed on the nodes, since agents implemented on the IoT devices are responsible for monitoring the device status and verifying that all the parameters are correct. In case the device is affected by a remote AT reconfiguration command attack, such alert information is forwarded to the IoT coordinator, and the device is designed to mitigate the attack (by autonomously reconfiguring itself, as previously described). Since not all the devices may embed a detection and mitigation system, the IoT coordinator is supposed to also monitor devices status periodically to identify disconnections, hence report them to the other ANASTACIA modules.

2.3.2.2 Slow DoS attacks

Among all the methodologies used to successfully execute malicious cyber-operations, denial of service attacks (DoS) are executed with the aim of exhaust victim's resources, compromising the targeted systems' availability, thus affecting availability and reliability for legitimate users. These threats are particularly dangerous, since they can cause significant disruption on network-based systems [7]. The term Slow DoS Attack (SDA), coined by the CNR research group involved in the project, concerns a DoS attack which makes use of low-bandwidth rate to accomplish its purpose. An SDA often acts at the application layer of the Internet protocol stack because the characteristics of this layer are easier to exploit to successfully attack a victim even by sending it few bytes of malicious requests [8]. Moreover, under an SDA, an ON-OFF behaviour may be adopted by the attacker [9], which comprises a succession of consecutive periods composed of an interval of inactivity (called off-time), followed by an interval of activity (called on-time).

The innovative attack proposed is called SlowComm, sending a large amount of slow (and endless) requests to the server, saturating the available connections at the application layer on the server inducing it to wait for the (never sent) completion of the requests. As an example, we refer to the HTTP protocol, where the characters sequence \r\n\r\n represent the end of the request: SlowComm never sends such characters, hence forcing the server to an endless wait. Additionally, during a SlowComm the request payload is sent abnormally slowly. Similar behaviour could be adopted for other protocols as well (SMTP, FTP, etc.). As a consequence, by applying this behaviour to a large amount of connections with the victim, a DoS may be reached. In particular, SlowComm works by creating a set of predefined connections with the victim host. For each connection, a specific payload message is sent

(the payload is typically endless), one character at time (one single character per packet), by making use of the Wait Timeout [9] to delay the sending. In this way, once the connection is established with the server (at the transport layer), a single character is sent (hence, establishing/seizing the connection at the application layer, hence, with the listening daemon). At this point, the Wait Timeout is triggered, to delay the sending of the remaining payload, and to prevent server-side connection closures. During our work we proved how the attack may successfully lead a DoS to different popular TCP based services [4], hence proving that the attack is particularly dangerous.

To protect from SlowComm and Slow DoS Attacks in general, it is important to consider the following fact: *it is trivial to detect and mitigate a single attacking host, while it is extremely difficult to identify a distributed attack*. This fact derives from the fact that IP address filtering may be applied to detect and mitigate a SlowComm attack (see, for instance, our tests on mod-security [4]), while in case of a distributed attack this concept may not be adopted with ease. Moreover, from the stealth perspective, the proposed attack is particularly difficult to detect while it is active, since log files on the server are often updated only when a complete request is received or a connection is closed: being our requests typically endless, during the attack log files do not contain any trace of attack. Therefore, different approaches should be adopted, for instance based on statistic [10], machine learning [6, 11, 12], or spectral analysis [13]. A possible approach to adopt combines the algorithm proposed in [10] and the methodology proposed in [14] to detect running SlowComm attacks. Early version of the algorithms has been tested in laboratory, while testing on relevant environments has not been accomplished to date. Concerning the ANASTACIA platform, further work on the topic will be focused on evaluating a possible implementation of such approach, aimed to provide protection from Slow DoS Attacks by embedding innovative anomaly-based intrusion detection algorithms in a relevant environment and providing additional capabilities to the ANASTACIA framework, in the context of cyber-security applied to counter last generation threats.

2.3.3 Trusted Security Orchestration in SDN/NFV-enabled IOT Scenarios

In the ANASTACIA architecture, the security orchestrator oversees orchestrating the security enablers according to the defined security policies. The later would be generated either by the end-user or received from the

monitoring and reaction plane. The security orchestration plane, through its components security orchestrator, security resource planning and policy interpreter, is able to coordinate the policies and security enables to cover the security configuration needed for different communications happen in the network. The security orchestration plane takes into account the policies requirements and the available resources in the underlying infrastructure to mitigate the different attacks while reducing the expected mitigation cost and without affecting the QoS requirements of different verticals. The resources in the underlying infrastructure refer to the available amount of resources in terms of CPU, RAM, and storage in different cloud providers, as well as the bandwidth communication between these network clouds.

Figure 2.3 depicts the main architecture of the security orchestration and enforcement plane suggested in ANASTACIA. Using SDN network, the IoT domain is connected to the cloud domain, whereby different IoT services are running. The user accesses the IoT devices, first, through the cloud domain, then the SDN enabled network and the IoT router. In fact, in ANASTACIA, the communication between a user and an IoT device happens through a chain of virtual network functions (VNFs) named service function chaining (SFC). The latter consists of three parts:

(i) The ingress point, which is the first VNF in the SFC. The user initially attaches to the ingress point;
(ii) The intermediate VNFs;
(iii) The egress point, which is the last VNF in the SFC. The egress point should be connected to the IoT controller. As depicted in Figure 2.3, the order of the communications between the VNFs is defined according to the different SDN rules enforced thanks to the SDN controller. The nature and the size of the SFC would be defined according to the nature of the user (a normal or a suspicious).

Figure 2.4 depicts the different steps of the orchestration and enforcement plane suggested in ANASTACIA. The attack is detected thanks to the Mitigation Action Service (MAS) component. The later sends a mitigation request (MSPL file) to the security orchestrator (Figure 2.4, Step 3). To mitigate the attacks, the security orchestrator interacts with three main actors, which are (Figure 2.4):

IoT controller: It provides IoT command and control at high-level of abstraction in independent way of the underlying technologies. That is, it is able to carry out the IoT management requests through

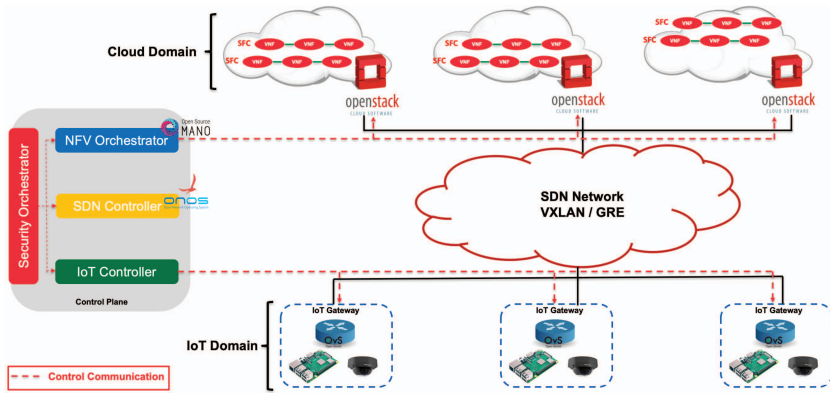

Figure 2.3 Security orchestration plane.

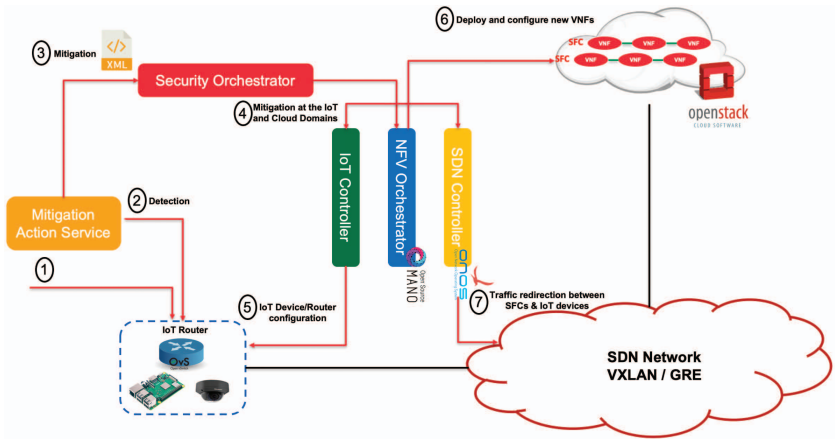

Figure 2.4 Security orchestration and enforcement in case of a reactive scenario.

different IoT constrain protocols like CoAP or MQTT. It also maintains a registry of relevant information of the deployed IoT devices like the IoT device properties and available operations. Since it knows the IoT devices status, it could be able to perform an effective communication to avoid the IoT network saturation when it is required a high-scale command and control operation. In "Security Management Architecture for NFV/SDN-aware IoT Systems" (Under review) can be found an example and performance of IoT management as part of a building management system. To mitigate different attacks, the security orchestrator interacts with the IoT controller to mitigate the attacks at

the level of the IoT domain and prevent the propagation of the attack to other networks (Figure 2.4: 4). The IoT controller enforce different security rules at the IoT router (data plane) to mitigate the attack (Figure 2.4: 5).

NFV orchestrator: In ANASTACIA, to ensure efficient management of SFC, we have integrated SDN controller (ONOS) with the used Virtual Infrastructure Manager (VIM), in our case OpenStack. The integration of SDN with the VIM enable the smooth communication between different VNFs that form the same SFC. After receiving the MSPL message from the MAS, the security orchestrator identifies the right mitigation plane should be implemented. If the mitigation plan requires the instantiation of new VNFs, the security orchestrator instructs the NFV orchestrator to instantiate and configure the required VNFs. To instantiate the required VNFs, the NFV orchestrator interacts with the VIM (Figure 2.4: 6). Also, the security orchestrator interacts with the policy interpreter to translate the received MSPL to the low configuration (LSPL) needed for different VNFs. After the successful instantiation of a security VNF, the security orchestrator configures that VNF with the received LSPL (Figure 2.4: 6).

In ANASTACIA, we have also developed different virtual security enablers that should be instantiated to mitigate the different attacks. For instance, we have developed a new VNF firewall based on SDN-enabled switch and OpenFlow. OVS-Firewall is a newly developed solution that relies on OpenFlow protocol to create a sophisticated firewalling system. We have also proposed and developed a new security VNF, named virtual IoT-honeynet, that allows to replicate a real IoT environment in a virtual one by simulating the IoT devices with their real deployed firmware, as well as the physical location. The IoT-honeynet can be represented by an IoT-honeynet security policy, and the final configuration can be deployed transparently on demand with the support of the SDN network. "Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks" (Under review) shows the potential and performance of this approach.

SDN controller: This component helps in rerouting the traffic between the VNFs in different SFCs. As depicted in Figure 2.4, when the mitigation action service notifies the orchestrator about an attack, the SFC would be updated by adding/inserting new security VNFs in the SFCs. The security orchestrator

should push the adequate SDN rules to reroute the traffic between different VNFs in the SFC and the IoT domain (Figure 2.4: 7). Also, according to the different situations, the security orchestrator can choose the SDN as security enabler. In this case, it can be the attack mitigated by pushing exploring the strength of the SDN technology. If so, the security orchestrator can instruct the SDN controller to push some SDN rules to prevent, allow or limit the communication on specified protocols and ports between different communication peers (Figure 2.4: 7).

By relying in the aforementioned orchestration properties and features, as well as the SDN and IoT controllers, the ANASTACIA framework aims to cope with the research challenges related with Orchestration of SDN/NFV-based security solutions for IoT environments and currently several experiments have been carried out in different security areas.

For instance, several experiments have been carried out regarding **virtual IoT-honeynets**. This kind of VNF allows to replicate a real IoT environment in a virtual one by simulating the IoT devices with their real deployed firmware, as well as the physical location. The IoT-honeynet can be represented by an IoThoneynet security policy, and the final configuration can be deployed transparently on demand with the support of the SDN network. "Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks" (paper under review) shows the potential and performance of this approach.

Furthermore, the security orchestration of ANASTACIA enables continuous and dynamic management of Authentication, Authorization, Accounting (AAA) as well as Channel Protection virtual security functions in IoT networks enabled with SDN/NFV controllers. Our scientific paper [1] shows how a virtual AAA is deployed as VNF dynamically at the edge, to enable scalable device's bootstrapping and managing the access control of IoT devices to the network. Besides, our solution allows distributing dynamically the necessary crypto-keys for IoT M2M communications and deploy virtual Channel-protection proxies as VNFs, with the aim of establishing secure tunnels (e.g. through DTLs) among IoT devices and services, according to the contextual decisions inferred by the cognitive framework. The solution was implemented and evaluated, demonstrating its feasibility to manage dynamically AAA and channel protection in SDN/NFV-enabled IoT scenarios.

A telco cloud environment may consist of multiple VNFs that can be shipped and provided, in the form virtual machine (VM) images, from different vendors. These VNF images will contain highly sensitive data

that should not be manipulated by unauthorized users. Moreover, the manipulation of these VNF images by unauthorized users can be a threat that can affect the whole system setup. In ANASTACIA, we have designed and developed different tools to prevent the manipulation of different VNF images should run on top of different network clouds. In ANASTACIA, we have devised efficient methods that verify the integrity of physical machines before using them and also the integrity of virtual machine and virtual network function images before launching them [15–17]. For this purpose, different technologies have been investigated, such as i) Trusted Platform Module (TPM); ii) Linux Volume Management (LVM); iii) Linux Unified Key Setup (LUKS). For instance, in [16], we have provided a trusted cloud platform that consists of the following components:

- TPM module that is used to store passwords, cryptographic keys, certificates, and other sensitive information. TPM contains platform configuration registers (PCRs) which can be used to store cryptographic hash measurements of the system's critical components. There are in total 24 platform configuration registers (PCRs) in most TPM modules starting from 0 till 23.
- Trusted boot module, which is an open source tool, uses Intel's trusted execution technology (TXT) to perform the measured boot of the system. Trusted boot process starts when trust boot is launched as an executable and measures all the binaries of the system components (i.e., firmware code, BIOS, OS kernel and hypervisor code). Trust boot then writes these hash measurements in TPM's secure storage.
- Remote attestation service, which is the process of verifying the boot time integrity of the remote hosts. It is a software mechanism integrated with TPM, to securely attest the trust state of the remote hosts. It uses boot time measurements of the system components such as BIOS, OS, and hypervisor, and stores the known good configuration of the host machine in its white list database. It then queries the remote host's TPM module to fetch its current PCR measurements. After receiving the current PCR values, it compares them against its white list values to derive the final trust state of the remote host.
- OpenStack Resource Selection Filters component that should be integrated with the nova scheduler. In OpenStack, when a VNF is launched, the nova-scheduler filters pass through each host and select the number of hosts that satisfy the given criteria. Each filter passes the list of selected hosts to the proceeding filter. When the last filter

is processed, OpenStack's default filter scheduler performs a weighing mechanism. It assigns weight to each of the selected hosts depending on the RAM, CPU and any other custom criteria to select a host which is most suitable to launch the VM instance.

2.3.4 Dynamic Orchestration of Resources Planning in Security-oriented SDN and NFV Synergies

Network operators are facing different type of attacks that introduce new set of challenges to detect and to defend from the attack. However, the hardware appliances for defence or detection are neither flexible nor elastic and they are expensive. To extend the NFV MANO framework, ANASTACIA incorporates a set of intelligent and dynamic security policies that can be updated seamlessly to constantly reflect security concerns in the VNF placement through the resource planning module while still ensuring acceptable QoE. Moreover, we have defined and implement synergies between SDN controllers and NFV MANO for the purpose of coordinating security to have an effective impact by defining adequate SDN rules or the adequate virtual security appliances (VNF) to be enforced through the Security Enabler Provider module. In the following section the resource planning and the security enabler provider modules will be defined.

2.3.4.1 Resource planning module

During the first phase of ANASTACIA, we have done two main works. The first one focused on the selection of best service (Virtual Network Function (VNF)), called "The security enablers selection", among the list of enablers selected previously by the selected Security Enabler Provider, to cope with a security attack, and a second work focus "Mobile Edge Computing Resources Optimization". In fact, one of our two main use cases focuses on Mobile Edge Computing, as an example, to secure protection of a company perimeter, based on several buildings with different usage situated in different areas using distributed resource as MEC; an emerging technology that aims at pushing applications and content close to the users (e.g. at base stations, access points, and aggregation networks), reduces the latency, improves the quality of experience, and ensures highly efficient network operation and service delivery.

During the second phase of the project, we aim to extend the resource planning module to include a dynamic Service Function Chain (SFC) requests placement that aim to reduce the routing overhead in case of an attack happen

as an example. In fact, it is challenging to allocate multiple SFC requests on an NFV Infrastructure, especially in a cost-driven objective. VNFs have to be chained in a specific order. Moreover, depending on their type and isolation considerations, VNFs can be potentially shared among several SFCs. Finally, VNFs must not be placed far from the shortest path to avoid increasing SFC delay and network usage.

2.3.4.2 The security enablers selection

The aim of the model is to select the best service (Virtual Network Function (VNF)) among the list of enablers selected previously by the selected Security Enabler Provider, to cope with a security attack and that minimize the maximum load nodes (CPU, RAM, bandwidth) of the topology, provided by the system model. Indeed, the system information will provide relevant data about the whole infrastructure, server capacity (CPU, RAM, etc.), and VNF flavours (CPU, RAM, etc.). On the other hand, the Security Enablers information will provide the data regarding the available Security Enablers capable to enforce specific capabilities. The goal of the model is minimizing the maximum load nodes to improve provider cost revenue (provider energy efficiency goal). For more details please refer to the Anastacia deliverable D3.3.

2.3.4.3 Mobile edge computing resources optimization

Mobile edge computing (MEC) is an emerging technology that aims at pushing applications and content close to the users (e.g. at base stations, access points, aggregation networks) to reduce latency, improve quality of experience, and ensure highly efficient network operation and service delivery. It principally relies on virtualization-enabled MEC servers with limited capacity at the edge of the network. One key issue is to dimension such systems in terms of server size, server number and server operation area to meet MEC goals. In this work, we have proposed a graph-based algorithm that, taking into account a maximum MEC server capacity, provides a partition of MEC clusters, which consolidates as many communications as possible at the edge. We evaluate our proposal and show that, despite the spatio-temporal dynamics of the traffic; our algorithm provides well-balanced MEC areas that serve a large part of the communications.

This work has been published in a Sigcomm [18] workshop and extended for a TNSM journal [19].

2.3.4.4 Security enabler provider

The Security Enabler Provider is a component of the Security Orchestration Plane, as defined in the Anastacia architecture. This component is able to identify the security enablers which can provide specific security capabilities, to meet the security policies requirements. Moreover, when the Security Resource Planning, a sub-component of the security orchestrator, defined before, selects the security enabler, the Security Enabler Provider is also responsible for providing the corresponding plugin.

The Security Enabler Provider primarily interacts with the Policy Interpreter. Specifically, two different interactions have been contemplated:

- The first one will provide to the Policy Interpreter a list of security enabler candidates from the main identified capabilities.
- The second one will provide to the Policy Interpreter the specific Security Enabler Plugin to perform the policy translation. This policy translation process was defined in Anastacia D3.1 [20], and also published in journal paper [2].

The first role is implemented as a piece of software that from the specific capabilities given as an input it will provide the more accurate enablers. The second role is also implemented as piece of software capable to translate MSPL policies into specific configuration/tasks rules according to a concrete security enabler. For more details please refer to the Anastacia deliverable D3.3 [21].

2.3.5 Security Monitoring to Threat Detection in SDN/NFV-enabled IOT Deployments

Security threat levels change dynamically as the attackers discover new breaches and try to exploit them. To cope with this challenge, the ANASTACIA project relies on SDN and NFV techniques to embed the developed security products and provide a dynamic way to deploy them when needed. In this way, the ANASTACIA project delivers a set of scientific and technological innovations, grouped in two principal key innovation areas.

2.3.5.1 Security monitoring and reaction infrastructure

Saedgi et al. identify the principal challenges when securing IoT-based Cyber Physical Systems, highlighting as one of the principal challenges the development of a "*a holistic cybersecurity framework covering all abstraction layers of heterogeneous IoT systems and across platform*

boundaries" [22]. The ANASTACIA project fulfils this challenge by proposing a state-of-the-art security infrastructure composed by three principal modules:

- ***Monitoring Agents***: These are the components in charge of extracting the security data from the monitored network. The ANASTACIA framework has been designed flexible enough to support both physical and virtual monitoring agents, as well as to extract data from data networks (both IP and IoT networks) and from analogue CPS devices. This make the ANASTACIA framework a multilevel security platform, and therefore suitable for physical sensor networks, emulated environments and hybrid networks. In this direction, the ANASTACIA partners have worked in the implementation of monitoring agents adapted for 6LowPan and ZigBee IoT networks, as well as the development of agents capable of extracting temperature information from analogue sources. These agents have been tested using the case studies of the project, aiming to be applied in wider scenarios for its final validation. Following this path, the project partners are extending even further these monitoring agents with virtualization characteristics. By means of using NFV and SDN technologies on the monitoring agents, it will be possible to deploy and (re)configure them on demand, allowing to deploy new agents on the network as a reaction to ongoing attacks. In this sense, the ANASTACIA partners are also extending the security policy language (MSPL) to correctly specify such type of countermeasures, allowing the deployment of new monitoring agents on the network in a complete autonomous manner.
- ***Monitoring Module***: This component contains the logic of the detection of security incidents. The heterogeneous monitoring agents (IoT networks and analogue agents) use a shared communication channel to publish the extracted security data. This information is then analysed by the incident detectors (for well-known attacks) and behaviour analysis modules (for zero-days attacks), emitting verdicts about the detected incidents. As stated in [22], detecting zero-days attacks does not ensure a high security level, since well-known attacks are still used by malicious users to gain control of the systems. ANASTACIA does not only provide both types of analysis (well-known attacks and behaviour analysis) but it will also use all this information to provide a deeper analysis and found correlations between already-known attacks and they behavioural analysis result, detecting hidden relationships between events coming from

different sources. The ANASTACIA partners are developing such correlation engines to enhance both security analyses and provide enriched information to the reaction module.

- ***Reaction Module***: Using the information provided by the monitoring module (namely incidents verdicts and behavioural analysis results), the reaction module has the responsibility of determining the best mitigation plan for the detected incidents. The ANASTACIA framework provides a simple yet powerful design for this component, which uses not only the incidents verdicts provided by the monitoring module, but also system model and the capabilities deployed in the network. All this information is enhanced with a risk analysis to determine the best set of countermeasures to cope with the ongoing attack. Further information about how this analysis is performed can be found in the following sections.

2.3.5.2 Novel products for IoT- and cloud-based SDN/NFV systems

The security infrastructure described above represents one of the principal outcomes of the project, however the partners are also working on a concrete implementation of this design. To implement this monitoring infrastructure, the partners have developed a set of technologies that fulfil the functionalities of the ANASTACIA infrastructure, generating a set of novel products ready to be deployed on IoT- and cloudbased systems. For example, partner Montimage has developed a 6LowPan network sniffer in coordination with the MMT tool to detect anomalies in IoT networks. UTRC (in collaboration with OdinS) has developed analogue temperature agents and a machine learning-based behavioural analysis for data sensors, allowing them to detect zero-days attacks on temperature sensor networks. ATOS has extended its XL-SIEM tool to perform the risk analysis when computing the reaction and the inclusion of the system model when computing the countermeasures to be taken. Despite the development of such products is not finished yet, the partners have managed to integrate PoC version of such technologies on a shared platform, allowing to perform initial tests and validation of the technologies. Moreover, it is envisaged to further extend this tools with a correlation engine, aiming to reveal hidden relationships between security events coming from different sources (monitoring agents) and, therefore, raising the awareness level of the whole security platform.

To further extend the offer of products, the ANASTACIA partners are preparing the solutions to be NFV- and SDN-ready, by means of adapting

the solutions (especially network agents) to work as single, self-contained NFV modules. In this sense, the ANASTACIA outcomes will have the potential to be deployed in virtualized environments, be dynamically deployed as a reaction to an ongoing attack and, capable of being reconfigured if required. In this scenario, the ANASTACIA platform will have the ability to momentarily harden the security of the portions of the network are under attack, by means of deploying new agents, load new security rules on the monitoring agents/module, analyse new protocols or reconfigure the existing instances. All these actions are to be maintained until the security level has returned to normal values or the network administrator has intervened to solve the security breach.

All these novel products will have a high impact on the security market, opening business possibilities in the IoT-based CPS area.

Despite the ambition of the project is high, the ANASTACIA partners have already established the bases of the further innovations. The ANASTACIA partners will continue its efforts to fully integrate the security innovations with the SDN and NFV technologies, as well as developing a correlation engine for security events. This direction aims to provide the market with a highly-dynamic security solution, capable of not only detecting current cyber threats, but also capable of reacting against them and also deploy new security instances to adapt to the always-evolving security levels of IoT networks.

2.3.6 Cyber Threats Automated and Cognitive Reaction and Mitigation Components

The monitoring information and the incident detected are evaluated for automatic mitigation. Security policies are used to determine the security enablers supported by the IoT infrastructure. This is also used to know the mitigations that the IoT infrastructure supports. Obviously, not all mitigations work with all possible threats, and not all mitigations have the same cost. Cost is not considered here just in terms of economic impact, but also in terms of time to mitigate, computational resources required or complexity of the mitigation. ANASTACIA automatically analyses these factors and, along with the incidents detected, evaluates and decides on the most convenient mitigation in each case. To this end several data are considered in the analysis:

- severity of the incidents, which is received by the correlation engine at the monitoring module and takes into account the type of incident and the duration of the incident among others,

- importance of the assets affected, which depends on the criticality of the IoT devices affected, their location or the importance of the data they manage,
- the cost of the mitigation, obtained either from the orchestrator in charge of enforce the available security enablers, or from the system admin in case specific expert knowledge is required.

The global risk of the incident is obtained from (1) and (2), which is used together with (3) to decide on the most convenient mitigation. A decision support service (DSS) is used to compute that information, providing with a score for each mitigation, which represents the suitability of the mitigation for the ongoing incident. The mitigation with the higher suitability score represents the most suitable mitigation, which is passed to the orchestrator for its enforcement. To this end a Mitigation Action Service (MAS) is used to translate the output of the DSS to a format that is understandable by the orchestrator. The MAS is then in charge of generating the reaction in the MSPL format. This language was selected since its XML-based structure allows specifying the type of base capability to deploy (e.g. filtering, monitoring), and the configurations of such action (e.g. involved IPs, port numbers, number of agents to deploy). The MSPL format also allows the MAS to directly send the mitigation plan to the Security Orchestrator, which will use it to deploy the computed plan.

In order to generate the MSPL file, the MAS analyses the response of the DSS by performing the following processes: (1) it identifies the countermeasure computed by the DSS; (2) it identifies the network capabilities able to execute the countermeasure; (3) it retrieves the information of the capabilities from the System Model Analysis module; (4) it builds the MSPL file to express the countermeasure, specifying the capability to use and the configurations of that capability used to apply the countermeasure.

Every incident handled by the reaction (including risk evaluation, decision support activities), the information associated to it (such as type of incident or IoT devices affected) and all the indicators that characterize the incident (such as severity, importance of assets affected, global risk of the incident or suitability of the mitigation) are passed to the Dynamic Security and Privacy Seal to update the seal status.

Currently we are developing the quantitative model that supports the assessment of incidents and mitigations for deciding on the most convenient reaction based on incident severity, criticality of the assets affected, possible mitigations and cost of mitigating them.

2.3.7 Behaviour Analysis, Anomaly Detection and Automated Testing for the Detection of Known and Unknown Vulnerabilities in both Physical and Virtual Environments

Our behavioural framework automatically identifies cyber-security attacks in a given IoT environment. It uses system design and operational data to discover dependencies between cyber systems and operations of HVAC in a cyber-physical domain. We predict potential security consequences of interacting operations among subsystems and generate threat alarms. Specifically, our behavioural engine is empowering ANASTACIA's use case scenario using the "best" practices to implement security in terms of (1) adding network security (in forms of IDS/IPS), and (2) using threat intelligence to detect evasions or hidden attacks. Our developed platform can detect:

- Known attacks such as DDoS and MiTM attacks,
- IoT zero-days attacks and slow DoS attacks that might pass undetected by normal IDS/IPS [9].

Our framework developed a monitoring component that is composed of messaging wrappers, Constraint Programming (CP) models and buffered sensor data from IoT networks. Primarily, CP model is the core component of our behavioural analysis engine. First the information is gathered and analysed for learning a CP model and then it is deployed to identify any intrusion. Moreover, CP model built on continuous stream of data (i.e. time-series) where the time interval between successive updates could vary from milliseconds to minutes. CP model consists of network of relations between building sensor data. Using this CP model, we aggregate the different types of sensor data to truly model the normal behaviour of the system that is being supervised. This model is built for monitoring at system level, but it does not prevent from including in the model information about network performance if that is exposed to it. For an example, CPU consumption of a device can be included along its actual sensor data. The variety of data that we can aggregate allows the model to be as generic or as specific as the end-user required it to be. Since the model is built on relations, we can leverage from the fact that what data effects what other data type (features).

We developed an approach to learn a CP-based decision model consisting of a set of relations to detect misbehaviour of the system. More specifically, the idea is to learn a set of relations which together when satisfied defines the normal behaviour of the system. After learning important relations, the approach discards un-important relations, and consequently creates a model with best possible relations and features of sensor nodes. In each iteration,

the relation between the sensor features and all other network features further verified. Also, we identify the sensors are involved in breaking the relation and what are the set of relations are broken Following this fashion, the model is further tuned. The developed 'Monitoring' component enables continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. This monitoring component also evaluates the security situation against known policies, models, threat signatures to detect abnormalities and outliers, e.g. high data download, external database or port accesses during an emergency. Such situations will be analysed by the 'Reaction' component which will evaluate the severity of the situation. Isolation and predictive mechanisms are activated to ensure that the rest of the building operations system continues as normal. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component, e.g. a building emergency will lock-down the non-essential database accesses, and escalation of the emergency to the city fire brigade should be performed by any of the authorized personnel. To this end, our behavioural engine's innovation is summarized as the following key points:

- Learning constraint programming model for capturing the normal behaviour of a given cyberphysical system
- CP-model provides explanation when a potential anomaly is detected by reporting which constraints fails to satisfy the model
- User-defined constraints can be easily integrated with the constraints learn from the data
- The developed behaviour engine can handle multiple attacks of different types.

2.3.8 Secured and Authenticated Dynamic Seal System as a Service

Several projects have tried to address the need to enable trustable ICT deployments. The solutions they have developed are generally focused either on enhancing trust on security or on privacy, but not both. This situation can be counterproductive if considered in the context of the obligations emerging from the recently adopted European General Data Protection Regulation (GDPR) (which considers both security and privacy controls as fundamental to the protection of personal data).

Moreover, existing solutions are usually based on two separate models:

- Either ISO standard-based certification of products and information management systems respecting ISO 17065 or ISO 17021-1 and relaying on human audit and assessment;
- Or purely system-based monitoring of security, such as anti-virus applications or intrusion detection system (IDS), which are often designed independently from any standard.

The ever-evolving normative framework for security and personal data protection calls for a holistic approach which considers technical insights alongside human and organizational controls. An organization that seeks to comply with the regulatory frameworks will finally rely on the professional advice from information security professionals (spearheaded by a Chief Information Security Officer -CISO-) and legal professionals (usually taking the token as Data Protection Officers -DPO-), which might have difficulties understanding the complex outputs of the technological enablers used to introduce the necessary controls to the systems they oversee and integrating these with the legal and managerial feedback necessary to transparently and accurately demonstrate due diligence has been carried out.

In response to this situation, ANASTACIA's Dynamic Privacy and Security Seal (DSPS) will seek to inform the end-user (DPO/CISO) on the most relevant privacy and security issues while supporting certification and compliance activities. To this end, the DSPS will:

- Introduce a privacy-by-design and by default compliant architecture, services and graphical user interface (GUI) that seek to combine the certainty and trustworthiness of conventional certification schemes with real-time certification surveillance capabilities through the real time dynamic monitoring (provided by ANASTACIA) of the certified system.
- Compile alerts and threats from ANASTACIA, compatible monitoring solutions (using the STIX 2 standard) and the end-user (CISO/DPO) and showcase them through a unified GUI, displaying IoT/CPS privacy and security information while providing decision support capabilities, and data visualization (considering accessibility/ease of use requirements).
- Empower the end-user by enabling the client's Data Protection Officer (DPO) and Chief Information Security Officer (CISO) to provide feedback to the raised alerts directly through the GUI and to enhance the information obtained from the monitoring system with technical, legal, annd organizational documentation. This data will be stored in a -privacy-by-design- distributed storage solution (powered by Shamir

Secret Sharing Scheme), which will be associated with the DSPS blockchain-based seal ledger (Hyperledger Fabric), to ensure the data is non-repudiable, immutable, and easily verifiable in direct relation to the events showcased by the DSPS both by the end-user (for internal audit and compliance purposes) and associated certification bodies (to determine the validity of relevant certifications).

The Dynamic Security and Privacy Seal (DSPS) aims to provide a holistic solution to privacy and security monitoring, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a layered process by which: 1) an initial examination by an auditor or expert determines the baseline status of the system with regards to privacy and security of both the product or system that is to be monitored, and the organizational policies and mechanisms that surround its implementation to ensure compliance with the most relevant ISO standards (particularly if linked to a certification) and regulations; 2) ANASTACIA provides constant monitoring and reaction capabilities which are then used to update the DSPS; 3) the end-user provides feedback on the effectivity of the mitigation activities and uses the DSPS enablers to enhance transparency and accountability in the monitored system.

The resulting tool will provide the end-user with a broad perspective over the state of the monitored system which will consistently track and unify the organizational/human elements considered by personal data protection regulations with the technical insights provided by ANASTACIA's monitoring and reaction services. Once implemented, this process will not only provide advanced trust-enhancing information functionalities to ANASTACIA users, but will also serve as a surveillance solution for audit/certification/legal compliance purposes. It will generate a non-repudiable historic track of system variations and potential threats (technical and organizational) to the sealed system while enhancing the contextual information available to the client, auditors or regulatory authorities.

Current work [23] has been focused towards developing the DSPS architecture as defined by ANASTACIA Deliverable 5.1; deploying and integrating the monitoring service and associated enablers; and refining the GUI elements that will inform the end-user and enable them to provide the required feedback. Upcoming research will seek out ways to simplify complex privacy and security information, so as to address the varying technical and legal knowledge of the potential end-users. Furthermore, research on integration with additional information sources (particularly through the

STIX2 format) and privacy-management tools (such as the CNIL DPIA software) will be performed to further enhance the functionalities available through the DSPS GUI.

2.4 Conclusion

This book chapter has summarized the main key innovations being devised, implemented and validated in the scope of Anastacia research project to meet the cybersecurity challenge in heterogenous IoT scenarios. Namely it has presented eight key innovations: 1) Holistic policy-based security management and orchestration in IoT, 2) Investigation on innovative cyber-threats, 3) Trusted Security orchestration in SDN/NFV-enabled IoT scenarios, 4) Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies, 5) Security monitoring to threat detection in SDN/NFV-enabled IoT deployments, 6) Cyber threats automated and cognitive reaction and mitigation components, 7) Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments, 8) Secured and Authenticated Dynamic Seal System as a Service.

These main key innovations are currently being realized and evaluated successfully in MEC and Smart-building scenarios. In this sense, important research outcomes have been already obtained and published in high impact journals, which demonstrate the feasibility and performance of ANASTACIA cybersecurity framework to dynamically handling and counter evolving kind of cyberattacks in SDN/NFV-enabled IoT deployments.

Acknowledgements

This work has been supported by the following research projects:

- Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures (ANASTACIA), funded by the European Commission (Horizon 2020, call DS-01-2016) Grant Agreement Number 731558.

The authors declare that there is no conflict of interest regarding the publication of this document.

References

[1] Alejandro Molina Zarca, Jorge Bernal Bernabe, Ruben Trapero, Diego Rivera, Jesus Villalobos y, Antonio Skarmeta, Stefano Bianchi, Anastasios Zafeiropoulos and Panagiotis Gouvas "Security Management Architecture for NFV/SDN-aware IoT Systems", IEEE IoT Journal, 2019.

[2] Molina Zarca, A.; Bernal Bernabe, J.; Farris, I.; Khettab, Y.; Taleb, T.; Skarmeta, A. Enhancing IoT 719 security through network softwarization and virtual security appliances. International Journal of Network 720 Management, 28, e2038, https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.2038.e2038, 721 doi:10.1002/nem.2038.

[3] Molina Zarca, Alejandro and Garcia-Carrillo, Dan and Bernal Bernabe, Jorge and Ortiz, Jordi and Marin-Perez, Rafael and Skarmeta, Antonio, Enabling Virtual AAA Management in SDN-Based IoT Networks, Sensors, 19, 2019, 2, 295, http://www.mdpi.com/1424-8220/19/2/295, 1424-8220, 10.3390/s19020295

[4] Cambiaso, E., Papaleo, G., and Aiello, M. (2017). Slowcomm: Design, development and performance evaluation of a new slow DoS attack. Journal of Information Security and Applications, 35, 23–31.

[5] Vaccari, I., Cambiaso, E., and Aiello, M. (2017). Remotely Exploiting AT Command Attacks on ZigBee Networks. Security and Communication Networks, 2017.

[6] Katkar, V., Zinjade, A., Dalvi, S., Bafna, T., and Mahajan, R. (2015, February). Detection of DoS/DDoS Attack against HTTP Servers Using Naive Bayesian. In Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on (pp. 280–285). IEEE.

[7] Beitollahi, H., and Deconinck, G. (2011). A dependable architecture to mitigate distributed denial of service attacks on network-based control systems. International Journal of Critical Infrastructure Protection, 4(3–4), 107–123.

[8] Cambiaso, E., Papaleo, G., and Aiello, M. (2012, October). Taxonomy of slow DoS attacks to web applications. In International Conference on Security in Computer Networks and Distributed Systems (pp. 195–204). Springer, Berlin, Heidelberg.

[9] Cambiaso, E., Papaleo, G., Chiola, G., and Aiello, M. (2013). Slow DoS attacks: definition and categorisation. International Journal of Trust Management in Computing and Communications, 1(3–4), 300–319.

[10] Aiello, M., Cambiaso, E., Scaglione, S., and Papaleo, G. (2013, July). A similarity based approach for application DoS attacks detection. In Computers and Communications (ISCC), 2013 IEEE Symposium on (pp. 000430–000435). IEEE.

[11] Duravkin, I. V., Carlsson, A., and Loktionova, A. S. (2014). Method of slow-attack detection. Системи обробки інформації, (8), 102–106.

[12] Singh, K. J., and De, T. (2015). An approach of DDOS attack detection using classifiers. In Emerging Research in Computing, Information, Communication and Applications (pp. 429–437). Springer, New Delhi.

[13] Brynielsson, J., and Sharma, R. (2015, August). Detectability of low-rate HTTP server DoS attacks using spectral analysis. In Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on (pp. 954–961). IEEE.

[14] Cambiaso, E., Papaleo, G., Chiola, G., and Aiello, M. (2016). A Network Traffic Representation Model for Detecting Application Layer Attacks. International Journal of Computing and Digital Systems, 5(01).

[15] S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, "Securing VNF Communication in NFVI," in Proc. IEEE CSCN'17, Helsinki, Finland, Sep. 2017.

[16] S. Lal, I. Oliver, S. Ravidas, T. Taleb, "Assuring Virtual Network Function Image Integrity and Host Sealing in Telco Cloud," in Proc. IEEE ICC 2017, Paris, France, May 2017.

[17] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine., Vol. 55, No. 8, May 2017, pp. 211–217.

[18] M. Bouet, V. Conana, Geo-partitioning of MEC resources, ACM MECOMM '17, August 21, 2017, Los Angeles, CA, USA.

[19] M. Bouet, V. Conana, Mobile Edge Computing Resources Optimization: A Geo-Clustering Approach, IEEE Transactions on Network and Service Management, Vol. 15, No. 2, June 2018.

[20] AM Zarca, JB Bernabe, AS, K Yacine, B Dallal, S Bianchi "Initial Security Enforcement Manager Report". 2018. H2020 Anastacia EU project deliverable D3.1.

[21] D Belabed, M Bouet, D Rivera, P Sobonski, A Molina Zarca, "Initial Security Enforcement Enablers Report" Anastacia EU project deliverable D3.3.

[22] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." Design

Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[23] Quesada Rodriguez, Adrian; Bajic, Bojana; Crettaz, Cédric; Filipponi, Matteo; Pacheco Huamani, Ana María; Perlini, Adriano, Kim, Eunah; Loup, Vincent; Ziegler, Sébastien. "Dynamic Security and Privacy Seal Monitoring Service". 2018. H2020 Anastacia EU project deliverable 5.2.

[24] Quesada Rodriguez, Adrian; Bajic, Bojana; Crettaz, Cédric; Menon, Mythili; Pacheco Huamani, Ana María; Kim, Eunah; Loup, Vincent; Ziegler, Sébastien. "Dynamic Security and Privacy Seal Model Analysis". 2018. H2020 Anastacia EU project deliverable 5.1.

[25] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on ZigBee technology," in Proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT '11), pp. 297–301, IEEE, Kanyakumari, India, April 2011.

[26] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[27] Ziegler S. et al. (2019) Privacy and Security Threats on the Internet of Things. In: Ziegler S. (eds) Internet of Things Security and Data Protection. Internet of Things (Technology, Communications and Computing). Springer, Cham, DOI: 10.1007/978-3-030-04984-3_2