Chafika, Benzaid; Taleb, Tarik; Phan, Cao Thanh; Tselios, Christos; Tsolis, George

Distributed AI-based security for massive numbers of network slices in 5G beyond mobile systems

Published in:
2021 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2021

DOI:
10.1109/EuCNC/6GSummit51104.2021.9482418

Published: 28/07/2021

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Distributed AI-based Security for Massive Numbers of Network Slices in 5G & Beyond Mobile Systems

Benzaid Chafika*, Tarik Taleb*, Cao-Thanh Phan†, Christos Tselios§, George Tsolis§
*Aalto University, †b<>com, §Citrix Systems Inc.

***Abstract*—The envisioned massive deployment of network slices in 5G and beyond mobile systems makes the shift towards zero-touch, scalable and secure slice lifecycle management a necessity. This is to harvest the benefits of network slicing in enabling profitable services. These benefits will not be attained without ensuring a high level security of the created network slices and the underlying infrastructure, above all in a zero-touch automated fashion. In this vein, this paper presents the architecture of an innovative network slicing security orchestration framework, being developed within the EU H2020 MonB5G project. The framework leverages the potential of Security as a Service (SECaaS) and Artificial Intelligence (AI) to foster fully-distributed, autonomic and fine-grained management of network slicing security from the node level to the end-to-end and inter-slice levels.**

I. Introduction

The 5G and beyond networks are envisioned to support heterogeneous and flexible deployment scenarios, whereby the same infrastructure is shared among multiple services/verticals [1]. The concept is commonly known as network slicing, which consists in creating multiple logical networks (i.e., slices) over a common shared physical infrastructure. Each slice provides tailored network capabilities to fulfil the performance needs of a particular service type [1]. As a result, network slicing holds the promise of moving mobile networks from one-size-fits-all to one-size-per-service design model, empowering differentiated service provisioning [2].

The envisioned growing interest from service providers in embracing network slicing to deliver profitable 5G and beyond services will lead to the deployment of a massive number of network slices, posing unprecedented complexity in their efficient management and orchestration. Despite the merit of existing contributions introduced by research projects (e.g., EU H2020 5G!Pagoda, 5G-EVE, 5Genesis, SliceNet, and SelfNet) and academic literature (e.g., [2], [3], [4]), there is still a long way to go before achieving scalable, proactive and secure slice lifecycle management in an autonomous way. The EU H2020 MonB5G project[2], a 5G-PPP Phase 3 project, comes to achieve this goal by providing an innovative system for autonomic deployment and management of a massive number of network slices in 5G and beyond networks. To this end, the MonB5G system will heavily leverage distribution of operations, zero-touch management across multiple technology domains (e.g., Radio Access Network, Core Network, and Cloud), and data-driven distributed AI-based mechanisms.

Given the ever-evolving attack surface of the slicing-enabled beyond 5G environment [5], automated security orchestration shall be incorporated, as an integral feature, into the envisaged network slicing management and orchestration system and that is to cope with security issues that can target network slices. In this paper, we introduce a security orchestration framework which aims at enabling faster detection and reaction to attacks, ultimately securing network slices from node-level attacks to the end-to-end and inter-slice level attacks, and that is by leveraging distributed and hierarchical autonomous closed-loops.

The rest of this paper is organized as follows. Section II summarizes related work. Section III provides a main overview on MonB5G's platform for autonomic management of 5G network slicing. Section IV presents the envisioned security orchestration framework, describing its main components and their integration in MonB5G architecture. Finally, the paper concludes in Section V.

II. Related Work

The concept of a novel, higher-level pervasive construct that leverages AI and cognitive systems to build autonomic networks, was originally introduced in [6], under the term Knowledge Plane (KP), paving the way for the design of the Generic Autonomic Networking Architecture (GANA) [3], a reference model for autonomic networking, cognition and self-management. GANA can be seen as a holistic model which incorporates, harmonizes and accommodates the main concepts and principles from well-known models of autonomic networked systems, such as IBM-MAPE, FOCALE and CONMan, for delivering an end-to-end solution.

The GANA reference architecture uses KP to autonomously support the various management and control systems, including the Network Function Virtualization (NFV) Orchestrator, the Software Defined Network (SDN) controller, the End-to-End (E2E) service orchestrator and the Operation Support Systems / Business Support Systems (OSS/BSS). Those systems represent the data/events sources for the KP. Recently, a proof-of-concept for applying the GANA reference model to empower E2E autonomic (closed-loop) security management and control for 5G slices was proposed [7]. The specific framework defined two complementary Decision-making Elements (DEs) and levels for autonomic security management and control operations, namely the Network Element/Network Function (NE/NF)-level security management DE and the KP-plane (also called Network-Level) security management DE. This inspiring framework remains a hard mapping between

[1]3GPP TS 23.501. System Architecture for the 5G System (5GS); Stage 2 (Release 16). Dec. 2020

[2]https://www.monb5g.eu

[3]ETSI White Paper No. 16. GANA -Generic Autonomic Networking Architecture. Oct. 2016

GANA and a multi-domain 5G system, which simply results in centralized DEs and node-level DEs without reflecting the in-between levels of a 5G system, i.e. slices that need to be isolated and are divided further into sub-slices per technology/administrative domain.

The security as a service (SECaaS) concept has emerged as an effective business model wherein cybersecurity services are made available on-demand via the cloud [8]. Cloud Security Alliance (CSA)[4] defined the guidelines for implementing the security as a service (SECaaS) model in a cloud environment. Consequently, SECaaS has been widely adopted in different research projects targeting 5G network security, such as Anastacia[5] and INSPIRE-5Gplus[6]. The project Anastacia devised a framework for protecting IoT infrastructures by leveraging SDN/NFV-based security features in Multi-Access Edge Computing (MEC) and smart building management. The Anastacia framework aims to manage security policies and define relevant security controls to be orchestrated. Its architecture [9] includes (i) a control plane encompassing NFV Management and Orchestration (MANO) modules, SDN controllers and IoT controllers to supervise the usage of resources and real-time operations of security enablers; (ii) an autonomic plane for enforcing security measures and real-time reconfiguration and adaptation of services; and (iii) a seal management plane which combines security and privacy standards with real-time monitoring. Anastacia may have paved the way to the implementation of SECaaS, however, it did not target 5G environments and was only limited to the MEC domain. 5G-Ensure[7] defined a security architecture for 5G and developed security VNFs to go with it, yet the project did not consider any autonomic or AI-based solutions.

Another promising approach comes from INSPIRE-5Gplus, an ongoing project aiming to revolutionize the security in 5G and beyond networks by implementing a fully automated E2E smart network and service security management framework. To meet this goal, INSPIRE-5Gplus leverages a set of emerging trends and technologies, including Zero-touch network and Service Management (ZSM), SECaaS, Software-Defined Security (SD-SEC) and AI/ML techniques. Nevertheless, the current INSPIRE-5Gplus architecture [10] appears to remain centralized in a per domain level, lacking slice-specific security management and isolation.

Lastly, ETSI ENI (Experiential Network Intelligence) ISG (Industry Specification Group) is defining a Cognitive Network Management architecture using closed-loop AI mechanisms [8]. To enable policy-based network security, the ENI system architecture includes a Policy Management Functional Block. This block ensures that consistent and scalable decisions are made governing the behaviour of a system, while supporting all policy types (i.e., imperative, declarative and intent), including context-aware policies [9].

To tackle most of the abovementioned limitations, MonB5G purposes the development of a security orchestration architecture that exploits the potential of SECaaS model and AI techniques [11] to foster scalable and autonomic management of network slicing security in 5G and beyond networks and that is in a distributed fashion. To this aim, the security management closed-loops are distributed cross domains from the network node level to end-to-end and inter-slices levels. This architecture allows service-tailored and on-demand specification and deployment of virtual security functions (VSF) and risk management strategies. In the subsequent sections, we present the envisioned MonB5G security orchestration framework.

III. MonB5G Architecture and Main Overview

MonB5G aims to design a novel framework for accommodating the provisioning, deployment and lifecycle management (LCM) of large numbers of network slices, in alignment with the vision of 5G and beyond. For achieving a high level of efficiency and scalability, it adopts the MAPE (Monitor-Analyze-Plan-Execute) paradigm and relies on distributed closed feedback loops, facilitated by AI-driven operations, and that is to ensure a certain degree of autonomic network operation. Such an approach facilitates local data processing, and consequently allows rapid data-driven decisions which are crucial for handling time-critical issues. Network components become much more scalable and agile, since they are now operating without the overhead of transferring large datasets of information, thus reducing the delay and optimizing the usage of valuable system resources.

The AI-based MAPE management loops are implemented using four components, namely: the Monitoring System (MS), Analytics Engine (AE), Decision Engine (DE) and the actuation functions (ACT). The AEs and DEs leverage modern distributed AI (DAI) techniques, including federated learning and multi-agent deep reinforcement learning, to empower autonomous distributed slice LCM capabilities. The DAI techniques allow distributed learning and decision making while sharing the learned knowledge between agents, hence significantly reducing the learning overheads while increasing the accuracy [12].

To deliver the highest value possible while maintaining an inherent system simplicity, the MonB5G framework is designed based on specific principles. Particularly, the architecture: (i) maintains a strong distinction of components, having domain-grade slice LCM and resource management, both handled by entities which remain agnostic to the slices per se, while each slice integrates its own management platform as dictated by the In-Slice Management (ISM) paradigm [13], (ii) delivers hierarchical, end-to-end slice orchestration capabilities together with scalable and programmable slice management, by fully integrating ISM implemented as a set of VNFs which are then responsible for the fault, configuration,

[4]https://bit.ly/2NckOGS
[5]http://www.anastacia-h2020.eu/
[6]https://www.inspire-5gplus.eu/
[7]https://www.5gensure.eu/
[8]ETSI GS ENI 005 V2.0.21. System Architecture. Dec. 2020
[9]ETSI GR ENI 003 V1.1.1. Context-Aware Policy Management Gap Analysis. May 2018

accounting, performance, and security management (FCAPS) of the specific slice, (iii) supports distributed, AI-driven management operations, (iv) incorporates programmable, energy-aware infrastructure management, (v) boosts slice security through the slice management isolation delivered by ISM, and (vi) allows the creation of a dedicated "management slice" which can be used for run-time management of multiple slice instances, in alignment with the Management as a Service (MaaS) paradigm. An overview of static components and business actors of the MonB5G architecture is presented in Fig. 1.

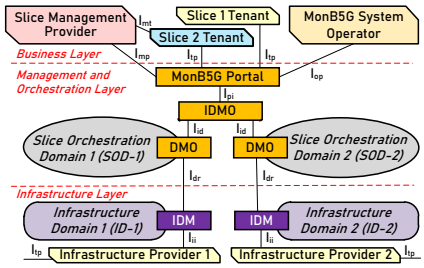

Fig. 1. MonB5G Architecture: Static components and Business Actors.

From a programming perspective, the distributed closed-loops are the entities responsible for implementing MaaS, covering the smart cognitive deployment, LCM and FCAPS, while being cost-effective and energy-efficient. The management services are decomposed into distributed, interacting components executed at the OSS/BSS level, inside the virtual domains, and embedded in slices. In the architecture, the static management components are separated from the dynamic and functional components in the Inter-domain Manager and Orchestrator (IDMO), and the Domain Manager and Orchestrator (DMO).

DMO is responsible for orchestration and management of the slices within the Slice Orchestration Domain (SOD). The DMO can be seen as a combination of OSS/BSS and MANO orchestrator controlling the SOD. In MonB5G, it has been decided to keep the orchestration part agnostic to slices. Therefore, the runtime management of slices is not performed by the orchestrator, but by dedicated components. Hence, the proposed architecture assumes that the domain orchestrator deals with the software dimension of slices only (i.e., LCM, resource scaling). Slice runtime management, as it cannot be generic, is handled by management components embedded in the slices. Between the SODs, there exists IDMO. The IDMO is used by the operator and its customers in order to deploy multi-domain network slices. It collects information from all DMOs that are owned by the operator, and selects SODs and DMOs to be used to host and orchestrate a specific sub-network slice. IDMO is responsible for providing sub-slice stitching and the correlation of events and KPIs from different domains. It can be seen as an E2E orchestrator and manager (umbrella orchestrator according to ETSI NFV). More details on MonB5G architecture can be found in [14].

IV. Security Architecture

In this section, we present the envisioned security orchestration framework. We start with the integration of its components into the overall MonB5G's network slicing management and orchestration architecture described in Section III. We then detail the main adopted security enablers and approaches. Fig. 2 depicts the security related components of the architecture. For the sake of simplicity, most of the management details are deliberately hidden, thus focusing only on the main security elements. In alignment with the distributed and hierarchical management philosophy adopted by MonB5G, global security is managed through the end-to-end security orchestrator (E2E SO) located in the IDMO, while the security at the domain level is handled by a local security orchestrator (local SO) hosted in the DMO. The local SO manages the security closed-loops together with the security enablers, i.e., Virtual Security Functions (VSFs), that need to be deployed to enforce security within its respective domain.

A. Security objectives

The SO must have a modular architecture to be considered as a management and orchestration environment distributed across multiple administrative domains. When a domain manages network slice subnets, the OSS or more precisely the Network Slice Subnet Management Function (NSSMF) delegates the management of security goals to the domain SO. The scope of the SO is subnetwork protection, following useful guidelines issued by international bodies such as ENISA and NIST for properly responding to cybersecurity incidents. These guidelines lead to a convergent approach for building cybersecurity capabilities, which are divided into three phases: Preparation, Reaction and Improvement.

During the Preparation phase, which starts prior to any actual incident, the SO must capture the security needs during the design of the network slices, understand the network slice structure and analyze potential vulnerabilities, threats and risks in an attempt to finally characterize the security objectives which need to be achieved. Appropriate protective measures must then be tailored and deployed along with the network slice, followed by an effectiveness evaluation process.

The second phase, namely the Reaction, starts when the incident occurs or when a security breach is identified through raised flags or anomaly/artifact-based detection techniques monitored by dedicated cyber threat intelligence entities. Corrective actions, such as updating security policies or network modifications, must be carried out in a timely manner to contain the security incident. This specific phase is considered complete after the eradication of the incident's root cause and the restoration of systems to normal operation.

The last phase, the Improvement, begins with the post incident activities. It consists in conducting a more extensive investigation and root cause analysis, learning lessons from the incidents to understand emerging vulnerabilities, threats and risks and reinforcing future defensive measures.

These three phases represent the lifecycle of security management. In each of these phases, the use of intelligent tools, implemented through the combination of MS, AE and DE components, allows to create either partially or fully automated processes. These processes can provide human experts with

a better vision at each phase, leading to better and faster decisions. Ultimately, closed feedbacks may fully remove human supervision.

B. Security orchestration

The security is distributed with the slice instances by implementing the required security management closed loops following SECaaS paradigm. The closed loops and the security enablers used to enforce the security policies are managed by the SOs at the domain and E2E levels through the "Security Service Manager" component.

1) E2E Security Orchestrator: The E2E SO has a global view and is responsible of the security of all slices from the E2E perspective. At the slice creation phase, the E2E SO checks (via communicating with local SOs) whether the slice can be deployed at the agreed SSLA requirements depending on the security capabilities provided by the respective technological domains where the slice will be deployed. If feasible, the E2E SO identifies the security policy to enforce and the corresponding enablers to deploy based on the slice blueprint, the received SSLA and the performed risk assessment. During the slice runtime, the E2E SO is responsible of enforcing cross-domain security decision policies coming from IDMO closed loops, such as migrating a sub-slice to a new domain to avoid a security threat in the original domain.

2) Local Security Orchestrator: Local to every domain, it ensures the local security management, by instantiating and managing the appropriate closed loops using a SECaaS approach when deploying a sub-slice instance. The closed loops can be deployed at the sub-slice instance level or at the VNF level. The adoption of SECaaS model allows the reusability of the deployed closed loops or some of their components (i.e., MS, AE, DE and ACT) between subslices. The SO ensures that the reusability is performed according to the isolation level of slices. The security policies issued by the DEs and their enforcement status are stored and managed by the "Conflict Management" component, providing the SO an overall view of all security policies enforced within the domain's sub-slices and allowing to avoid any conflict between policies. Once issued, the security policy is saved with "Enforcing" status. Its status is changed to "Success" if the ACT component can correctly execute the policy's actions, otherwise it is set to "Failure". The SO ensures the successful enforcement by adjusting the security policy and executing the necessary corrective operations. If the mitigation of the security issue is not possible at the domain level, the local SO escalates the problem towards the E2E SO, which assess the problem and generates the mitigation actions in E2E scope.

Similarly to the E2E SO, the local SO has a SSLA manager which translates the SSLA requirements into security actions and KPIs while deploying a sub-slice to monitor and ensure that the tenant security requirements are met. The security manager is responsible for instantiating and deploying MS, AE and DE that shall autonomously operate within the specific domain to provision SECaaS within the domain.

C. Slice security identification from the template

The network slice can be tailored based on the NEtwork Slice Type (NEST) [10] which is a Generic network Slice Template (GST) filled with values. These properties reflect the customer's use case for the network slice and define the inputs for the network slice management function (NSMF). At the preparation phase, the network slice is designed according to the requirements of the Service Level Agreement (SLA) and SSLA agreed between the customer and the network slice provider. In addition to the inputs from the customer, the network slice provider may include other security requirements associated to its internal policies. GSMA has defined some security properties for the GST such as the availability and the isolation level. However, other security properties such as the confidentiality and integrity protection, as well as the traceability may be considered according to the customer's vertical. The E2E SO captures all security needs and translates them into minimum acceptable security objectives for each domain managing a subnet component of the network slice. During the operational phase, defensive, threat detection and response measures are deployed and enabled in each network slice subnet.

D. Security as a service components

As aforementioned, the MonB5G architecture is strongly based on the triplet components MS, AE, and DE. At the low levels, ACT is added. These components are providing SECaaS and can be shared between multiple slices. The SO relies on on-demand security services (i.e., SECaaS) to protect the network slice in all aspects of its lifecycle. During the design phase, SECaaS helps the SO to identify all security needs derived from the customer's requirements, the provider's internal policies, and the structure of services and networks. Protective measures are then derived and implemented as an internal SECaaS to the network slice instance. This aims at limiting the risk exposure of the slice assets (network service instances) when the slice instance is in an operational phase. Security services include security functions that contribute to the realization of security standard guidelines and are offered through a Platform as a Service (PaaS) model as defined in IFA029 [11]. The PaaS is deployed as a network service (NS), the security functions appear as VNFs connected to the customer's VNFs, the configuration of security policies is handled via the element managers (EM), the security function lifecycle management is performed by the VNFM, and the SO relies on the NFVO for the orchestration of the NS and the resources. Thus, due to its architecture, the SO is modular and adaptive, as the security platform can be used to secure both the slices (inter-slice) and their network services (intra-slice) and the offered security services can be differentiated to cope with the particularities of a customer or a vertical. Hereunder, we introduce the high level roles of the envisioned components

[10]GSMA. Generic Network Slice Template. 2020

[11]TSI GR NFV-IFA029 - Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS". 2019

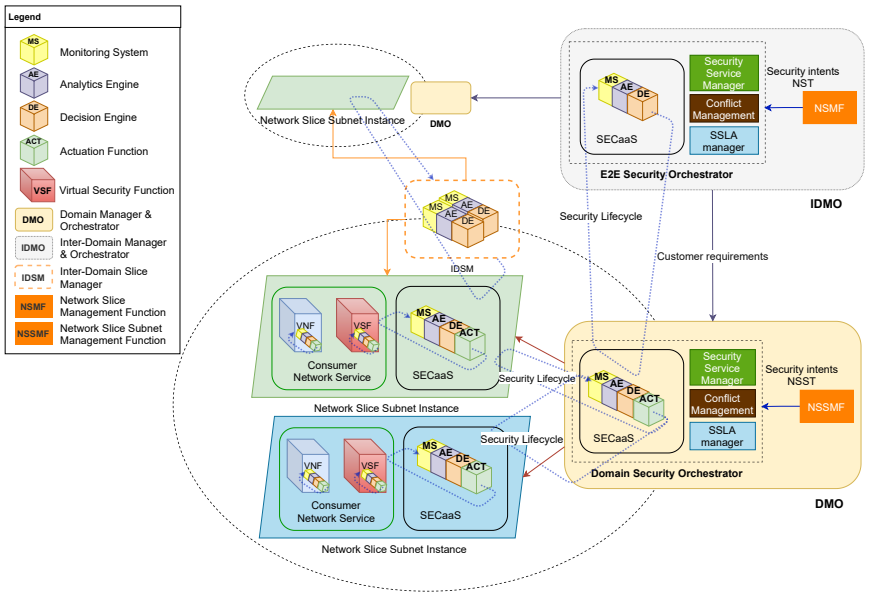

Fig. 2. Security Orchestration Architecture.

for implementing SECaaS closed loops, namely MS, AE, DE and ACT.

- MS collects real-time security-relevant data and provides information to AE. The data sources are identified depending on the hierarchical level and the final objective of DE. MS pre-processes the collected data.
- AE processes the monitoring data in order to extract high-level security information and events. Analyzing the collected KPIs, network flows and resources status will help in diagnosing the node and the network to detect or predict attacks and security issues.
- DE is the mastermind that has the ability to tell the system what to do as a reaction or prevention to protect the network against imminent security threats. The Security DEs' role is crucial in deciding on the reaction and the dynamic security policy per slice and attack episode. The decision can configure an existing security enabler in the slice or deploy a new one. However, these decisions are described in an abstract model rather than vendor-specific. DEs can be distributed horizontally and vertically, and each can relate to a specific application/VNF, sub-slice, or a slice scope. DEs are atomic elements that have a specific autonomic security function. For instance, at the VNF level, the DE embedded is responsible only for a unique security threats set that may target its hosting VNF. In this case, the risks and their remediation must be identified at the preparation phase based on the understanding of the network structure and security needs. For instance, in a VNF, the inner running application and the exposed protocols are known before the deployment which permits to extract the potential risks and select the proper DEs. At the higher level, the sub-slice's attached DEs depend on the sub-slice threats and characteristics. The same applies for slice DEs deployed in the IDSM. This distribution will greatly simplify the autonomic threat detection and may facilitate a fast response to local security threats.
- The ACT component is in charge of executing security policies determined by DEs and that is by performing a translation from the high-level decision into vendor-specific configuration according to the targeted enablers. ACT can trigger deploying a specific VSF through MANO or update the configuration of an existing VNF/VSF.

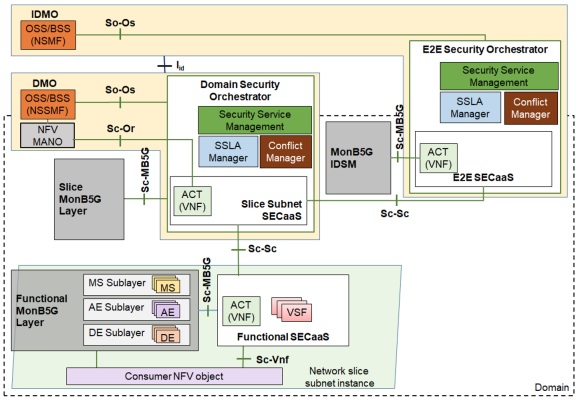

Fig. 3. Reference points of the security orchestrator.

E. Security orchestrator interfaces

The following reference points are defined for the SO and the security platform SECaaS at the inter-domain, domain and functional layers:

- **So-Os**: The reference point between the SO and the OSS is used by the OSS to delegate the management of the security goals of network slice to the SO.
- **Sc-MB5G**: The reference point between the security services and the MonB5G sublayer components is used to interact with MonB5G components to create closed loops for security process.
- **Sc-Sc**: The reference point is used for the control communications between two security services. The E2E security

service has a global view over the activities of slice subnet security platforms and manages the E2E security requirements. In turn, the slice subnet security service controls the functional security platforms to ensure that each slice subnet instance is well protected.

- **Sc-Or**: The reference point between the security platform and the NFVO. It is used to monitor the health of NFV objects and perform management operations on them. It is related to the reference point Sc-Or as defined in ETSI GS NFV-IFA 033 [12].
- **Sc-Vnf**: The reference point between the security platform and the consumer NFV object. The functional security platform offers VSFs such as firewall, Intrusion Detection System (IDS), access management as protection measures to improve the security of the slice subnet instance.

F. Policy management

To outline how the MonB5G security architecture approaches management of security policies, it is useful to map the components above to the roles defined by Zero Trust Architecture [13] and similar frameworks:

- MS and AE collectively map to the Policy Information Point (PIP). MS collects security-relevant events from various data sources, crucial for implementing threat and attack detection techniques in AE, and for maintaining the security context of all actors or entities involved.
- DE, as well as the Security Service Manager of the SO are a distributed and hierarchical implementation of a Policy Decision Point (PDP). DE performs policy evaluation in decentralized fashion, based on events and context from AE and localized policy configurations. However, the Security Service Manager orchestrates policy decisions within and across slice and domain boundaries, to implement the security intents configured by NSMF/NSSMF, which thus maps to the Policy Administration Point (PAP).
- ACT, typically in conjunction with VSFs that run continuously, or are instantiated on demand, maps to the Policy Enforcement Point (PEP). ACT translates policy decisions to specific actions that establish a perimeter of network security defenses, which continuously protect the services that reside in the slice, or execute remediations, which address or mitigate attacks to security.

Based on evaluating technology choices so far, we are looking at adopting the ONAP's APEX PDP Engine to implement the Policy Engine of the MonB5G's Security Service Manager. The engine is able to handle adaptive policies, i.e. policies that can modify their behaviour based on the current system and network conditions, allowing to support automated decision making.

V. Conclusion

This paper introduced a novel security orchestration framework that can efficiently and timely cope with the ever-evolving and diverse security threats targeting slicing-enabled beyond 5G mobile systems. The framework is designed in a way to enable distributed, autonomous, and fine-grained policy-based security orchestration of massive slice instances cross multiple domains by leveraging SECaaS and closed-loop AI mechanisms. Although the design of the framework is considered stable from the perspective of the main functional blocks and their role, some aspects still need in-depth exploration, such as (i) a clear definition of the interfaces between SECaaS to delegate a security task or escalate a security issue and (ii) how the ACT component can discover and be authorized to use the API exposed by the touch point.

The MonB5G project is currently developing the key framework's components, which will be integrated and tested in the overall MonB5G's network slicing management and orchestration architecture. The effectiveness the proposed framework will be evaluated according to different KPI, including the capacity to detect, contain and eradicate attacks, the deployment time, its scalability and the impact on service performance.

[12]ETSI GS NFV-IFA 033 - Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification. Aug. 2020

[13]https://www.nist.gov/publications/zero-trust-architecture

Acknowledgment

This work has been supported by the EU project MonB5G (under the Grant Agreement No. 871780). The views and opinions are those of the authors and do not necessary reflect the official position of Citrix Systems Inc.

References

[1] C. Benzaid and T. taleb and M. Z. Farooqi, "Trust in 5G and Beyond Networks," *IEEE Network Magazine*, To appear.

[2] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[3] T. Taleb et al., "CDN Slicing over a Multi-Domain Edge Cloud," *IEEE/ACM TMC*, vol. 19, no. 9, pp. 2010 – 2027, Sept. 2020.

[4] T. Taleb and I. Afolabi and K. Samdanis and F. Z. Yousaf, "On Multi-domain Network Slicing Orchestration Architecture & Federated Resource Control," *IEEE Network Magazine*, vol. 33, no. 5, pp. 242 – 252, Sept. 2019.

[5] ENISA, "ENISA Threat Landscape for 5G Networks; Updated Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)," , Dec. 2020.

[6] D. D. Clark et al., "A knowledge plane for the internet," in *Proc. of the 2003 conf. on Applications, technologies, architectures, and protocols for computer communications*, 2003, pp. 3–10.

[7] TSI GANA, "White Paper No. 6: Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management & Control for 5G Slices," , June 2020.

[8] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Transactions on network and Service management*, vol. 11, no. 1, pp. 60–75, 2014.

[9] I. Farris et al., "Towards provisioning of sdn/nfv-based security enablers for integrated protection of iot systems," in *2017 IEEE CSCN*. IEEE, 2017, pp. 169–174.

[10] C. Benzaid et al., "White paper: Intelligent security architecture for 5g and beyond networks," *INSPIRE-5Gplus*, Nov. 2020.

[11] C. Benzaid and T. taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" *IEEE Network Magazine*, vol. 34, no. 6, pp. 140–147, Nov. 2020.

[12] ——, "AI-driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions," *IEEE Network Magazine*, vol. 34, no. 2, pp. 186–194, Mar. 2020.

[13] S. Kukliński and L. Tomaszewski, "DASMO: A Scalable Approach to Network Slices Management and Orchestration," in *NOMS 2018 - 2018 IEEE/IFIP Net. Operations and Management Symposium*, 2018, pp. 1–6.

[14] "D2.1. 1st Release of the MonB5G Zero Touch Slice management and Orchestration Architecture," Tech. Rep., 2021.