Zero-touch security automation mechanisms for edge NFV: the π-Edge approach

Alexandros Valantasis*, Nikos Psaromanolakis*, Vasileios Theodorou*
*Intracom Telecom, Athens, Greece
Email: {savalant, nikpsarom, theovas}@intracom-telecom.com

***Abstract*—The shift towards distributed computing architectures that push data storage and processing to the edge of the network, is resulting into a convergence of cloud-computing services and next generation mobile network technologies. In order to uniformly manage resources and services in the formed cloud/core to edge/devices continuum and to handle the diversity of multi-party underlying infrastructure technologies in a latency-aware, reliable and trustworthy fashion, management automation has become more crucial than ever. In this work, we present the security analytics mechanisms of the π-Edge platform–our edge management platform that embodies zero-touch automation features for interoperability, Quality of Service (QoS) assurance, resilience and trust. To this end, we introduce a declarative NFV MANO Information Model (IM) and methods for automatically enhancing Network Slices at the edge, with security services that i) continuously monitor user-plane traffic on the links between Virtual Network Functions (VNFs), ii) detect possible network vulnerabilities or malicious behaviour and iii) apply relevant actions to effectively observe and mitigate identified threats. The implementation of such mechanisms is evaluated through experimentation on a use case of DDoS attacking scenarios, showcasing the usability and the benefits of our proposed solution.**

***Keywords*—Edge Computing, Network slice security automation, Platform as a Service, Edge lifecycle management**

I. Introduction

Next generation mobile network technologies are aiming towards pervasive and ubiquitous communication capabilities that will enable a multitude of human-centric and human-empowering services, spanning a diverse range of domains. From immersive applications offering unparalleled end-user experience, to industrial use cases and critical scenarios, the requirements for improvements of network quality of service (QoS) by orders of magnitude, as well as the increased demand for reliability, trustworthiness and explainability of complex, intertwined communication and application services to support such heterogeneous scenarios, are posing extreme challenges to their effective operation and lifecycle management (LCM).

At the same time, we are witnessing the verge of the openness of telecom and cloud resource and service ecosystems, in order to allow for the synthesis of end-to-end federated infrastructures and composite services, to share the large investment costs necessary for network coverage and scalability. This transition is fostering the emergence of both horizontal and vertical marketplaces, extending from core/cloud level to Edge Computing infrastructure and Edge/Internet of Things (IoT) devices. In particular, the latency-sensitivity and privacy-preservation benefits of pushing data storage and processing at the edge of the network, instead of transfering large datasets from their data generation environments all the way towards centralized datacenters, is further catalyzing the inclusion of third party edge resources to the pool of available infrastructure.

Nevertheless, despite the huge potential of such distributed and interoperable schemes, they can easily result in a mosaic of multi-vendor hardware, software and virtualization technologies, which is immensely hard to homogeneously manage in a trusted, robust and efficient manner. In such environments, automation appears as the only viable solution for network management and operation, alleviating human-operators from extremely complex tasks and streamlining service LCM, while respecting their intricate quality requirements. Moreover, automation can aid in bridging the skills gaps that arise from the convergence of various different disciplines during this multi-party evolution of network systems, e.g. Cloud Computing, Artificial Intelligence, 5G/6G Networking, Cyber-security etc.

In this work, we focus on the automated management of security mechanisms for edge Network Function Virtualization (NFV) environments, aiming towards the enrichment of Network Slices with custom security services in a zero-touch manner. To this end, we define an extension of NFV Management and Orchestration (NFV MANO) Information Model (IM) to capture automation features that can be defined by end-users in a declarative manner. The latter includes both the inclusion of desired security services that tackle a subset of well-known security vulnerability and threats, as well as their custom behavior with observability and actuation primitives. Moreover, we describe the design of an architecture and the implementation of a platform that handles the translation of declaratively-defined automation services, into instantiation, configuration and LCM of VNFs and supporting services that realise end-to-end the defined behavior, without manual intervention. Our approach is evaluated through a distributed denial-of-service (DDOS) attack scenario, where we show both the attack detection and the mitigation automatically applied.

Our main contribution is two-fold. On one hand, we intro-

978-3-903176-51-5

duce a novel architecture and mechanisms for the translation of high-level declarative descriptions into automated VNF LCM and network slicing. Our approach allows for granular management of the security-related behavior of network slices, whereby instead of a "take-it-or-leave-it" security enablement, we advocate expressiveness of automation behavior at an abstraction level that allows end users to define the "what" of their intensions and leave out the "how" of the deployment and operation to the platform functionality. In this direction, we introduce the security features of π-Edge Platform–our edge management platform for edge automation and interoperability. On the other hand, we describe a practical implementation of a threat mitigation scenario, involving the threat detection and the event-based actuation triggered by a DDOS attack–one of the most popular cyber-attacks that has yet to be examined thoroughly and faced effectively in NFV environments.

The rest of the paper is structured as follows: Section II introduces the π-Edge platform and its components of interest for security automation. Consequently, Section III introduces the security automation mechanisms of our approach and describes the processes for the end-to-end translation of declarative IM, into management actions of π-Edge platform components and the setting-up of security-automation-enabled network slices. Section IV presents results from concrete implementation of our methodology for a DDOS attack scenario and finally, after referencing related work in Section V, we provide concluding remarks and discussion in Section VI.

II. π-Edge Platform for Edge Automation

π-Edge platform is an edge management platform that offers a plethora of services for efficiently managing and ulitizing edge resources. It adopts a Platform-as-a-Service (PaaS) service delivery model that was first introduced in [1], for increased automation, maintainability and interoperability with centralized orchestrators (e.g., NFV MANO), resulting to significantly minimizing the management overhead of the latter. Moreover, as analyzed in Section III, it offers network slicing declarative security services for multi-tenant and multi-party edge ecosystems in order to ensure trusted and reliable slices across the infrastructure, without human-involvement.

A. High Level Architecture

As depicted in Fig. 1, π-Edge platform provides a variety of services, including QoS Monitoring, Machine Learning Operations (MLOps) automation, Software Defined Networking (SDN) Controller features, IoT platform and 5G Core integration services, Multi-access Edge Computing (MEC) and IoT Services, and the *Intelligent Agent*, which is responsible for lifecycle management (LCM) of Edge Services (e.g. auto-scaling and auto-healing). In this work, emphasis is put on the *Edge Catalogue* and *Security Services* components, offering zero-touch security automation mechanisms across the entire deployed services on the edge infrastructure.

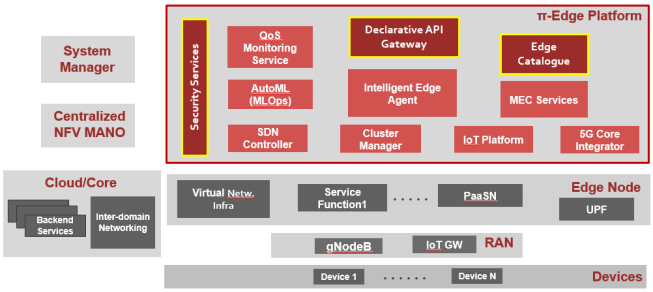

Fig. 1: High Level Architecture of π-Edge platform.

1) Edge Catalogue: The Edge Catalogue contains three types of entries, i.e. *Service Functions*, *PaaS Services* and *Edge Nodes*. Service Function is the smallest unit of deployment. It contains information necessary for the instantiation and LCM of deployment units, such as container/ Virtual Machine (VM) image names, application ports, volume dependencies, auto-scaling policies, etc. Regarding PaaS Service, it is the abstraction that models self-contained, modular and integrateable platform services. Each PaaS Service consists of a chain of Service Functions, i.e. one or more deployment units towards the realization of application logic, adopting the PaaS delivery model of the π-Edge platform. Lastly, the Edge Node represents the supported edge infrastructure nodes of an edge cluster, on which a PaaS service can be deployed and hosted, for instance virtual/ physical compute environments and Edge/ IoT devices.

III. Security Automation Mechanisms

In this section, an overview of the overall design of our security automation mechanism is provided, in conjunction with the methodology used in the implementation process. In this respect, we introduce our end-to-end zero-touch security automation mechanism, which bases on a declarative NFV MANO Information Model [2], to automate the provisioning of security services–provided by π-Edge, as well as security services that are seamlessly attached to Network Slices at the level of VNFs.

```
nst.yaml
  ...
  automation-service:
  - id: sas-42
    type: security
    name: sas-automation-service
    security-policy:
    - threat-type: DDOS
      on-detection: monitor_zoom-in
  ...
```

Fig. 2: NFV IM extension example for declarative automation services support.

A. Declarative NFV MANO Information Model and System Manager

A pivotal concept that we introduce in our work is the automated translation of a declarative NFV MANO IM, which is close to user intent level, into concrete technical implementation, configuration and (inter-)operation of VNFs. To this need, we provide the opportunity to the end-user not only to describe the Network Slice that needs to be deployed but also to declare in a high-level manner the security automation mechanisms that shall enrich the trustworthy operation of the Network Slice. In fact, the user can provide information about the type of the threat that shall be tracked for a particular Network Slice, as well as the actuation policy to be applied when this kind of threat is detected. According to our architecture, the management of the mapping between user high level intent and the materialized runtime services and configurations is performed by the *System Manager* component. The System Manager is responsible for combining the initial Network Slice of the user with the additional information about the security mechanisms it provides into an extended Network Slice that includes the corresponding dedicated security services. The extended Network Slice IM, an example of which is illustrated in Fig. 2 is an extension of the ETSI NFV-SOL006 model [2] with optional declarative automation fields and is thus backwards compatible with NFV MANO centralized orchestrators such the ETSI-hosted OpenSource MANO(OSM) [3].

B. Security Services of π-Edge Platform

The Security Services provided by π-Edge Platform can automatically configure and enable, in a zero touch manner, the complete end-to-end security pipeline. In fact, Security Services are divided into two main categories, namely the *Core Security Services* and the *Support Security Services*. The former are integral components of the π-Edge Platform while the latter are acting as agents deployed on the edge host, being shared across different network slices instantiated on the same host.

The Core Security Services are the core components of the platform regarding the security automation functionality. They are categorized into the *Declarative Security API GW* and the *Security Actuator and Observer*. The former is responsible for receiving a request from the System Manager about the instantiation of a network slice in order to start the activation of the security mechanisms to the specific slice. In addition, it informs the Security Actuator and Observer which has the main responsibility of configuring the slice VNFs, by applying the appropriate routing rules to the VNFs of the slice, as well as to enable the security traffic analysis mechanism on the Security Analysis Service VNF of the extended slice. On the other hand, the PaaS Support Security Services instantiated by π-Edge are two connected Service Functions, as presented in section II, that emulate the functionality of a search and analytics engine and a monitoring and interactive visualization application.

C. Security Services per Slice

A core component of the security automation mechanism is the dedicated Security Services that are automatically attached as additional VNFs to the initial Network Slice requested by the user. The presented Security Services, namely the *Security Analysis Service* and the *Virtual Router*, are deployed as VNFs in order to support any type of virtualized infrastructure.

1) Security Analysis Service: The Security Analysis Service (SAS) is the module that is in charge of performing network diagnostics in order not only to detect possible network vulnerabilities, attacks or threats of the extended Network Slice, but also to apply the required countermeasures for the mitigation of these adverse events. In fact, SAS continuously analyzes (e.g., every 30 seconds) the user plane traffic exchanged between the users' VNFs of the Slice in order to detect potentially weird or malicious behaviour. In addition, when a suspicious traffic pattern is identified, SAS declares the slice as "under inspection" and informs the "Security Actuator & Observer" service of π-Edge about this suspicious behaviour. SAS encapsulates the network security monitoring functionality for the live analysis of network events, as well as data transformation features for the aggregated and usable view of captured events in form of summarized statistics. These statistics are further sent to Support Security Services of π-Edge and especially to the Search and Analytics Engine in order to be stored centrally.

In essence, SAS fully automates locally the implementation and configuration of security monitoring rules for a particular network slice, mitigation policies and actuation upon detected threats, on a per-security-threat-type basis. To achieve this, as shown in Fig. 3, it bases on predefined templates that describe low level packet capturing behavior, the filtering of information of interest for each threat type, the granularity level of log monitoring, the aggregation level and desired presentation view of extracted information. Such templates can be used as-is, customized or enriched, allowing different levels of control on the declarative translation from the high level security-related mandates provided by end users.

2) Virtual Router: The Virtual Router component is in charge of connecting the users VNF and also mirroring/forwarding specified traffic to the Security Analysis Service for the traffic analysis.

D. Architectural Design and Workflow

In this subsection, we present the interaction of system components towards the instantiation of a security-automation-enabled Network Slice. First, the user requests from the System Manager, through a Network Slice Template (NST)

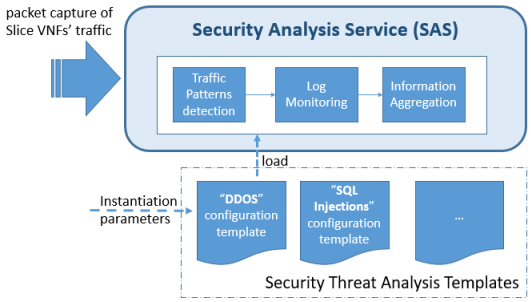

Fig. 3: Security Analysis Service implementation behaviour.

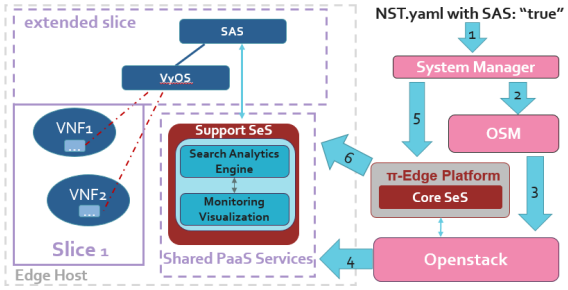

Fig. 4: Workflow Diagram for instantiation of security-enabled Network Slice.

the instantiation of a Network Slice which includes one or more VNFs. In addition to typical NST IM fields, the user describes through declarative automation extended fields, as shown in the example of Fig. 2, whether the specific Network Slice shall support security automation mechanisms, and if so, provides high-level information about the type of the security threats to be watched and the actuation policy to be applied upon detection of relevant threats.

Consequently, the initial NST is automatically transformed by the System Manager into an updated NST', including 2 additional VNFs, namely the Security Analysis Service and the Virtual Router. This extended slice template is then passed on to the NFV MANO entity for instantiation of the slice. Consequently, relevant requests are received by the VIM in order to deploy the VNFs of the extended slice to the edge host. When the extended slice has been successfully deployed, the System Manager informs the π-Edge in order to make the appropriate configurations to the VNFs of the slice. In fact, the "Security Actuator & Observer" component 1) configures the routing rules of the users VNF in order to use the Virtual Router VNF as gateway and 2) activates the security traffic analysis and enables a specific threat identification behavior on the Security Analysis Service VNF. Last but not least, the "Security Actuator & Observer" connects the Security Analysis Service VNF to the Support Security Services that are already deployed by the π-Edge platform on the same edge host. The aforementioned procedure is shown in Fig. 4.

IV. Evaluation

In this section, we present the different technologies and the selected tools used in the implementation process and we present in detail the use case attacking scenario in order to evaluate our security mechanism. In addition, we provide our experimental results and findings.

As mentioned above, the PaaS Support Security Services of π-Edge platform perform the functionality of a search and analytics engine and a monitoring and interactive visualization application. For the former, an Elasticsearch RESTful engine [4] for search and analytics has been used, as it gives the opportunity of not only storing the data centrally but also performing detailed analysis and complex analytics. For the visualization of these statistics, a Kibana analytics and visualization platform [5] has been implemented as it performs advanced data analysis while also visualizing the data received from Elasticsearch in a variety of interactive tables, charts, and maps. The aforementioned Service Functions are deployed by the π-Edge platform as a PaaS Service that consists of two Docker containers.

In addition, regarding the implementation of the Security Services per Slice, the Security Analysis Service (SAS) is developed as an extension of the Zeek platform [6] integrated with a Filebeat[7] instance for data collection. Zeek is used as the network security monitoring tool which is responsible for the live analysis of network events that consequently are passed to Filebeat, which is responsible for the data transformation. Both Zeek and Filebeat components have been deployed as Docker containers in a well-defined Docker network configuration. In addition the other components of the Security Services per Slice, namely the virtual Router is implemented using the VyOS [8] software for routing.

In the proposed architecture design, OSM [3] is playing the role of the NFV MANO orchestrator. OSM is connected to a Cloud provider responsible for deploying the virtualized resources, which in our case is an OpenStack IaaS [9].

Regarding the use case attacking scenario in order to evaluate our security mechanism, we performed a DDoS TCP SYN attack to one of the initial VNFs requested for instantiation by the user. In our case, the user requests an initial Network Slice that includes 2 VNFs while also declaring not only the type of the threat that shall be identified, which is a DDoS attack, but also the actuation policies to be applied. To this need, a plethora of different mitigation actions are offered from the security automation mechanism, namely 1) to increase the monitoring granularity of the security traffic analysis or 2) to apply traffic firewall rules to the attacked VNF in order to blacklist the attackers IP. Regarding the procedure that the

attack was performed, in VNF-1, a simple http web server at a specific port was enabled. The aforementioned port will be attacked concurrently, using 1, 5 and 10 spoof IPs. With the proposed attacking behaviour, we were trying to deceive the attacked VNF by spoofing the IPs of familiar devices inside the same network in order to bypass the default firewall policies of the system.

In a TCP SYN flood, the attacker sends a high volume of SYN packets to the open port of the attacked VNF using spoofed IP addresses. This behavior causes the attacked VNF to send a reply (SYN-ACK) to the fake source address and leave its ports half-open, waiting for a reply from a host that doesn't exist, leading to the exhaustion of its resources (CPU and RAM). In order to perform a TCP SYN Flood Attack we used the hping3 network tool with the proper arguments. First of all, we set a different number of packets transmitted per second in order to emulate different attacking load scenarios. In addition, we specified the port of the attacked VNF, the SYN flag for TCP SYN connections, while also a plethora of different fake IPs addresses, in order to disguise the real source and avoid detection, are determined.

Once the the Security Analysis Service VNF detects the TCP SYN Flood attack, as it has been configured by the declarations of the user to search and detect this type of malicious behaviour, informs the Security Actuator and Observer service of π-Edge about this "under-inspection" slice. Moreover, the Security Analysis Service VNF also applies a set of actions according to the declarations of the user, namely 1) to set the monitoring granularity for the security traffic analysis component to be equal to 30 seconds or 2) to prevent the communication between the attacker and the attacked VNF by blacklisting the attackers fake IPs. Specifically, the former action will result the security traffic analysis to obtain and report statistics every 30 seconds in order to "zoom-in" to these malicious activity. For this reason, the Security Analysis Service VNF re-configures the monitoring behaviour of its internal traffic analysis component, namely the ZEEK [6]. The aforementioned mitigation action can be evaluated by the Kibana [5] dashboard as it visualizes the statistics obtained from the Security Analysis Service VNF at the same time interval as the monitoring granularity that has been applied.

Regarding our experimental findings, we performed a set of trials in order to evaluate the resource impact of the proposed security automation mechanism. In fact, as shown in Fig.5 we measured the instantiation time for a different number of initials VNFs requested by the user, and also provided a comparison with the end-to-end overall time needed (instantiation and configuration), when the same Network Slice is enriched with the two additional VNFs, namely the dedicated security services. As we range the number of the VNFs requested by the user, the enrichment of the slice with the security services, adds a constant overhead of approximately 2 minutes to the

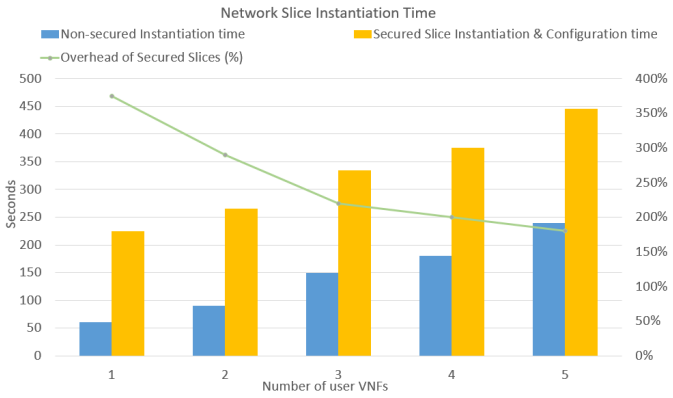

Fig. 5: Security Slice configuration time for an increasing number of user VNFs.

initial slice, for any case number of VNFs, respecting only the instantiation time. Referring to the configuration time needed to configure the routing rules and to enable the security traffic analysis, security services of π-Edge add another 45 seconds to the overhead of 2 minutes in the case of 1 user application VNF, while in the case of 5 user applications VNFs this time increases to 85 seconds. The presented measurements reinforce our belief that the π-Edge platform requires a minimum of time to set up the security pipeline which appears to increase in a linear fashion with the increasing number of user's VNFs.

Hence, the overall end-to-end instantiation and configuration time of the secured Network Slice, is calculated at 225 seconds in the case of 1 user application VNF, while in the case of 5 user applications VNFs this time increases to 445 seconds. As we can observe, the percentage of the additional overhead regarding the instantiation time of the initial slice is gradually decreasing as we scale the number of user's applications VNFs that are participated in the initial slice. As a result, the proposed security mechanism is not affected by larger-scale scenarios and it presents lesser performance overhead, as we scale the number of user's VNFs.

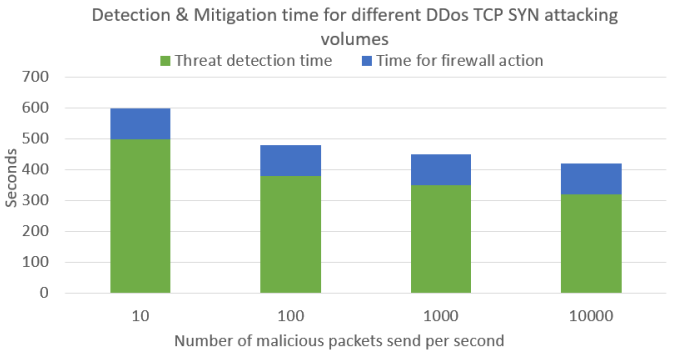

Fig. 6: Threat detection and firewalling time for different DDos TCP SYN attacking volumes using 10 spoof IPs.

In addition, to further evaluate the effectiveness of the security mechanism, we measured the time needed for detecting the DDoS SYN attack, while also actuating the necessary firewall policies, which in our scenario is to blacklist the attacker's IP. To this need, we experimented with three different scenarios by using 1, 5 and 10 spoof IPs, attacking concurrently. In fact, as we can observe from Fig.6, where we used 10 spoof IPs, the security automation mechanism requires 500 seconds in order to detect a low-volume DDoS attack, while also needs an additional time of 10 seconds in order to apply firewalling, with a transmission rate of 10 packets per second. As we range the transmission rate of the malicious packets in order to achieve more intensive DDoS attacks, the security mechanism requires less time and notably, an average of 330 seconds to detect this malicious activity, while for the mitigation actions, this time remains the same (10 seconds). This constant behaviour for the time of the firewalling action is a result of the security automation mechanism's functionality, where in every iteration aims to detect and block only one spoof IP at a time, while afterward starts another one for every new spoof IPs. This behaviour transforms our mechanism into a highly response system, every time that threat is detected. Similarly, for the cases of 5 and 1 spoof attacking IPs, the time required for detecting the threat, is 5 and 10 times accordingly lower than before, while the chronological pattern, regarding the different attacking transmission rate, remains the same for both cases.

Moreover, we experimented with the same attacking scenario but using a different mitigation action, which is the adjustment of the default monitoring granularity of the security traffic analysis component. As we can observe from Fig.7, the security automation mechanism demands to find only one malicious attacking spoof IP in order to actuate the Monitoring "Zoom-in" action. As a result, the security mechanism requires 50 seconds, which is significantly less time than before, in order to detect a malicious spoof IP for a low-volume DDoS attack with a transmission rate of 10 packets per second. As we range the transmission rate of the malicious packets, the mechanism requires an average of 33 seconds to detect this malicious activity. For every different case of attacking intensity, the security mechanism needs an additional time of 8 seconds to apply the monitoring "Zoom-in" action.

The presented results showcase the usefulness of the mechanism for detecting and preventing, in a minimum of time, DDoS attacks with a) high intensity and b) with low transmission rate that otherwise would be unnoticed by the default system's firewall policies.

V. Related Work

The implementation of security mechanisms in context of the Zero-touch network and Service Management (ZSM) paradigm has gained a lot of attention in relevant literature,

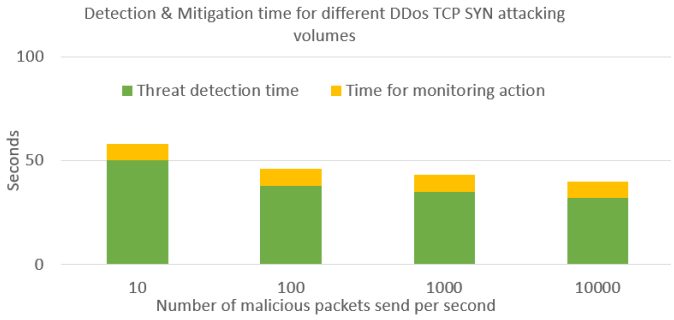

Fig. 7: Threat detection and monitoring "Zoom-in" time for different DDos TCP SYN attacking volumes.

as the provided security functionalities aim to transform the traditional network to an autonomous system, capable of self-healing based on service-level metrics without human intervention. The promise of this direction is the continuous assurance of security protection for the network components in a zero-touch and agnostic to the user manner. In [10], the authors presents their work on how Machine Learning (ML) and especially Deep Learning (DL) can assurance better security and performance for Zero-touch network and Service Management (ZSM) systems. In fact, they used a DL-based channel state information (CSI) to show the consequences and the negative effect of a white-box attack on a DL-based communication system, by analyzing the performance of deep learning-based CSI and especially the normalized mean square error.

Towards the concept of ZSM, in [11], the authors present ZSM as an enabler towards enrichment of 5G networks with security and trust. To achieve this, they used Artificial Intelligent (AI) mechanisms and Machine Learning (ML) algorithms for the management and configuration of the network in conjunction with minimal human configurations. In addition, they used distributed ledger technologies through the concept of smart contracts in order to accomplish security amongst multi-tenant environments. In [12], the authors present a smart platform that guarantees end-to-end security management based on a zero-touch model in 5G and Beyond 5G networks using state of the art techniques such as Machine Learning (ML), Artificial Intelligence (AI) and Trusted Execution Environment (TEE) in order to provide security according to pre-declared service level agreements (SLAs). In [13], the authors provide a new mechanism enriched with auto-scaling policies and functionalities for dynamically orchestration of applications across multiple infrastructures. In [14],[15], the authors present possible security risks and vulnerabilities that might be arise from the Automation of Network and service Management and Operation concept, and they provide several mitigation actions to prevent the possible threats and risks with traditional security solutions while also they introduce new security

research ideas by applying SDN/NFV technologies along with Artificial Intelligence. In [16], the authors present a pioneer framework in order to accomplish secured network slices in 5G & Beyond Mobile Systems by applying and combining two novel approaches, namely the Security as a Service (SECaaS) and closed-loop AI mechanisms.

Moreover, a lot of research efforts have been introduced on the mitigation of security attacks. In [17], the authors developed a novel query-flooding parameter duplication (QPD) attack by inferring the machine learning information model. In order to mitigate this kind of attack, the authors proposed a defence mechanism that uses the differential privacy (DP), namely the monitoring-based differential privacy (MDP). In [18], the authors proposed framework, based on the traffic analysis, which can efficiently identify SQL injection attacks and notify users while assisting in real-time threat evaluation of data loss.

To the best of our knowledge, our work is the first to allow end users to define security attacks of interest and automation behavior for Network Slices in a declarative fashion, allocating the translation to tedious and complex implementation, configuration and integration tasks to platform components, while at the same time allowing end-user visibility and control over slices at the appropriate abstraction level.

VI. Conclusion

In this work we present the security automation mechanisms for edge NFV environments provided by the π-Edge platform that encapsulates zero-touch automation features for interoperability, resilience and trust. In this context, a novel framework is introduced, which is capable of translating high-level declarative descriptions into VNF LCM configurations, as well as of enabling the security automation mechanisms responsible for detecting possible network vulnerabilities or security threats and applying the required countermeasures for the mitigation of such adverse events. In order to evaluate the introduced security automation mechanisms, a use case scenario of a DDoS attack along with the mitigation actions that apply were implemented and presented in detail. In addition, a set of experiments measuring both the resource utilization overhead of the proposed security automation mechanism and the time required in order for the security mechanism to identify and mitigate the attack, were illustrated. The obtained results showcase that for practical scenarios, the security automation mechanisms provided by π-Edge platform, require bounded time to set up, which is proportional to the size of network slices, while the overall overhead to enable security features to a network slice is comparative to slice instantiation time, presenting a declining trend as the number of VNFs in the slice increases. The latter, combined with the demonstrated ability of our mechanisms to detect and mitigate concrete security threats, indicates the usefulness of security automation mechanisms offered by π-Edge platform, compared to the overhead that it creates, especially at large scale scenarios.

Acknowledgment

This work has received funding from the European Union's Horizon 2020 project 5GZORRO (Grant Agreement No. 871533).

References

[1] Alexios Lekidis; Vasileios Theodorou; Nikolaos Psaromanolakis; Carmen Guerrero; Diego R. Lopez, "PiEdge: An Edge-Driven PaaS Model for Network Slicing Automation," *EuCNC/6G Summit*, 2021.

[2] ETSI, "ETSI GS NFV-MAN 001 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); Management and Orchestration," 2014.

[3] ETSI, OSM, "Open Source Mano," *https://osm.etsi.org/*, 2016.

[4] "Elasticsearch," *https://www.elastic.co/elasticsearch/*.

[5] Elastic NV, "Kibana," *https://www.elastic.co/kibana/*.

[6] BSD licenses, "Zeek," *https://osm.etsi.org/*, 1994.

[7] Elastic NV, "Filebeat," *https://www.elastic.co/beats/filebeat*.

[8] The VyOS Project, "VyOS," *https://vyos.io/*.

[9] T. Rosado and J. Bernardino, "An overview of openstack architecture," in *Proceedings of the 18th International Database Engineering & Applications Symposium*, 2014, pp. 366–367.

[10] Qing Liu; Jiajia Guo; Chao-Kai Wen; Shi Jin, "Adversarial Attack on DL-based Massive MIMO CSI Feedback," in *Journal of Communications and Networks*, 2020.

[11] Gino Carrozzo; M. Shuaib Siddiqui; August Betzler; José Bonnet; Gregorio Martinez Perez; Aurora Ramos; Tejas Subramanya, "AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture," in *European Conference on Networks and Communications (EuCNC)*, 2020.

[12] Ortiz J., Sanchez-Iborra R., Bernabe J.B., Skarmeta A., Benzaid C., Taleb T., Alemany P., Muñoz R., Vilalta R., Gaber C., et al., "INSPIRE-5Gplus: intelligent security and pervasive trust for 5G and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020.

[13] Young Lee; Ricard Vilalta; Ramon Casellas; Ricardo Martínez; Raul Muñoz, "Auto-Scaling Mechanism in the ICT Converged Cross Stratum Orchestration Architecture for Zero-Touch Service and Network Management," in *20th International Conference on Transparent Optical Networks (ICTON)*, 2018.

[14] Chafika Benzaid; Tarik Taleb, "AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions," in *IEEE NEtwork*, 2020.

[15] Chafika Benzaïd; Tarik Taleb; Muhammad Zubair Farooqi, "Trust in 5G and Beyond Networks," in *IEEE Network*, 2021.

[16] Benzaid Chafika; Tarik Taleb; Cao-Thanh Phan; Christos Tselios; George Tsolis, "Distributed AI-based Security for Massive Numbers of Network Slices in 5G Beyond Mobile Systems," in *Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2021.

[17] Haonan Yan and Xiaoguang Li and Hui Li and Jiamin Li and Wenhai Sun and Fenghua Li, "Monitoring-based differential privacy mechanism against query-flooding parameter duplication attack," vol. abs/2011.00418, 2020.

[18] H. Gu, J. Zhang, T. Liu, M. Hu, J. Zhou, T. Wei, and M. Chen, "Diava: A traffic-based framework for detection of sql injection attacks and vulnerability analysis of leaked data," *IEEE Transactions on Reliability*, vol. 69, no. 1, pp. 188–202, 2020.