Demo: Closed-Loop Security Orchestration in the Telco Cloud for Moving Target Defense

Wissem Soussi[1,2], Maria Christopoulou[3], George Xilouris[3], Edgardo Montes de Oca[4],
Vincent Lefebvre[5], Gürkan Gür[1], Burkhard Stiller[2]
[1]Zurich University of Applied Sciences (ZHAW), Switzerland
[2]University of Zurich, Switzerland
[3]National Center for Scientific Research Demokritos (NCSRD), Greece
[4]Montimage, France
[5]Solidshield, France
E-mails: [1]name.lastname@zhaw.ch, [2][soussi|stiller]@ifi.uzh.ch, [3]maria.christopoulou@iit.demokritos.gr,
[4]edgardo.montesdeoca@montimage.com, [5]vincent@solidshield.com

***Abstract*—This work presents a Moving Target Defense (MTD) framework for the protection of network slices and virtual resources in a telco cloud environment. The preliminary implementation provides a closed-loop security management of services with proactive MTD operations to reduce the success probability of attacks, and reactive MTD operations, empowered by a tampering detection and a traffic-based anomaly detection system. MTD strategies are adaptive and optimized with deep reinforcement learning (deep-RL) for balancing costs, security, and availability goals defined in a Multi-Objective Markov Decision Process (MOMDP).**

***Keywords*—Moving Target Defense, TelcoCloud Security, management and orchestration.**

I. Context and Motivation

Network softwarization [1] enables dynamic and flexible telco cloud environments that can be adapted based on the clients' requirements using virtualization of services (in containers or virtual machines) and software defined networking (SDN). In this setting, traditional network and system security methods, like cryptography, authentication, and vulnerability patches, inherently help to reduce the system's attack surface. However, since the attack surface is generally a static target, attackers can gain insightful information before launching an attack campaign, using a multitude of reconnaissance techniques and scanning tools.

From this perspective, Moving Target Defense (MTD) becomes crucial as it alters the technological stack, the configuration, and the topology of a networked system to reduce the asymmetrical advantage of attackers over blue teams. In a telco cloud, MTD leverages the flexibility and reconfigurability of that environment, allowing not only to perform proactive movements and to reduce the risks of threats and Attack Success Probability (ASP), but also reactive movements to mitigate detected attacks. Within this scope a telco cloud MTD Framework was developed in the INSPIRE-5Gplus project [2]. It performs near-real time monitoring of networking resources and makes decisions on MTD operations in a closed-loop fashion for cost-effective proactive and reactive security against various attacks.

Various research efforts are dealing with MTD in the literature [3], using shuffle, diversity, and redundancy approaches. MTD has been applied in the mitigation of DDoS attacks [4], [5], while proactive MTD operations leveraging SDN and Network Function Virtualization (NFV) have been explored in [5]. Game theory based MTD optimization strategies have been adopted to optimize MTD strategies against various attack models to enable a cost-efficient protection. These models range from general-sum Markov Games [6] to partially observable Markov Decision Process (POMDP) [7]. In this regard, this work is a continuation in this research direction and presents a multi-Objective Markov Decision Process (MOMDP) for representing the network state and enabling machine learning (ML) based continuous optimization and adaptation of sequential MTD actions.

The MTD framework here monitors the telco cloud in various underlying networks (*i.e.*, the Radio Access, Core, Data Plane, and virtualization layers) to control performance and availability of the protected services to user equipments (UEs). Vulnerability scanning and risk assessment are performed to elaborate a proactive MTD strategy. Such strategy is learned via deep-RL (Reinforcement Learning) and tackles a multi-objective optimization problem, where the goals are to maximize security (*i.e.,* minimize threats), to minimize the operational cost, and to alleviate the impact on availability and Quality-of-Service (QoS). Ultimately, the MTD framework reveals to be decisive in countering Advanced Persistent Threats (APT) originating from undetected intrusions and malware infections. The MTD framework also includes an anomaly detection framework (ADF) and an anti-dumping system, Solidshield Systemic, both sending attack alerts to showcase MTD mitigations against tampering, malware infection, and intrusion.

II. System Architecture

The telco cloud operator is the main stakeholder of this Proof-of-Concept (PoC) demonstration, whose objective is to improve the protection of network slices created for clients. The MTD framework architecture is depicted in Figure 1. It is designed to be compatible with the closed-loop management of the ETSI Zero touch network and Service Management (ETSI ZSM) [8] and ETSI NFV architecture that defines the NFV Management and Orchestration (MANO), network slices, Network Services (NS), and Virtual Network Functions (VNF).

 DOI: 10.1109/NOMS56928.2023.10154420

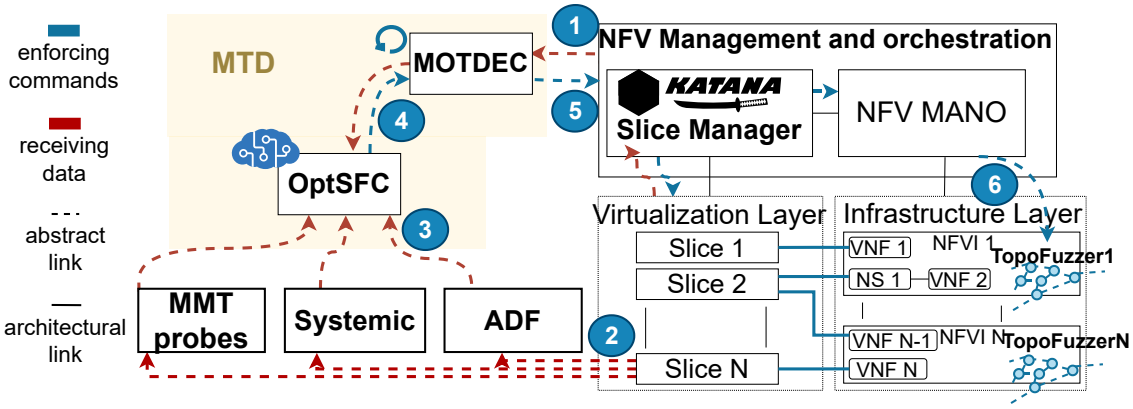

Fig. 1. System Block Diagram for the Demo Environment

A. Core Components of the MTD framework

Katana Network Slice Manager: Katana [9] is responsible for the creation of network slices following pre-defined slice templates, which describe the NSes and VNFs composing the slice. Katana interacts with the NFV MANO and the Virtual Infrastructure Manager (VIM) to deploy the slice as described in the template and monitor its life cycle.

MMT monitoring probes: Montimage monitoring probes capture in near-real time network traffic and evaluate various metrics, such as round-trip-time, throughput, packets in/out, and retransmission rate for further traffic analysis.

Anomaly Detection Framework (ADF): ADF is an open source software framework that uses Machine Learning (ML) to detect known and unknown network attacks by analyzing the traffic behavior.

Solidshield Systemic: Solidshield Systemic defines a SECaaS (Security-as-a-Service) platform for executable rewriting. It ingests executable files and generates automatically a modified version, hardened and monitored at runtime. Systemic is able to detect the tampering of one software's memory page.

Optimizer of Security Function (OptSFC): OptSFC [10] is a decision-making agent that deploys a deep RL to train and obtain a model for optimized MTD strategies. It collects network metrics and security alerts to build the MOMDP model representing the telco cloud state in near-real time, using OpenAI Gym[11]. The OpenAI Gym environment interacts with the deep RL algorithm during training and inference.

MTD controller (MOTDEC): MOTDEC [10] is the controller that enforces MTD actions decided by OptSFC. It is implemented in Python and categorizes MTD actions into two categories: Soft MTD actions and Hard MTD actions, based on the resource allocation and the impact on the QoS of protected services.

Network Topology Fuzzer (TopoFuzzer): TopoFuzzer [12] is a network gateway and a modular extension of MOTDEC. It uses Linux Kernel's iptables to enable Hard MTD actions, such as service re-instantiation and service migration. TopoFuzzer also uses a virtual network built with Mininet to provide Soft MTD actions enabled with SDN, such as topology fuzzing and data plane path shifting.

B. Description of the Workflow

The blue circles numbered in Figure 1 denote the steps of the closed-loop workflow of the MTD framework:

(1) It starts by configuring MOTDEC and the Katana slice manager to integrate MTD operations into the NFV management and orchestration (MANO) of the Telco Cloud. This includes discovering virtual resources (*i.e.,* slices, NSs, VNFs, and VDUs) and their interdependencies, as well as the hosting infrastructure and its resource capability.

(2) The security modules, namely the MMT probes, Systemic, and the ADF, collect raw monitoring data, analyzes them, and generates meta-data or security alerts.

(3) All meta-data and security incident alerts are sent to OptSFC through its REST API. OptSFC creates the MOMDP state, including additional threat and risk assessments.

(4) Proactively, based on the risk assessment formulated in the MOMDP, and reactively, based on the security alerts received in Step (3), OptSFC proposes the MTD operation to be enforced by MOTDEC.

(5) The Katana slice manager orchestrates Hard MTD actions using the APIs of the NFV MANO and the VIM.

(6) The TopoFuzzer completes these operations requiring a handover of clients' connections without disrupting them and performs the Soft MTD actions on the middle virtual network.

III. 5G Testbed and PoC Setup

The demonstration setup includes a 5G testbed as illustrated within Figure 2. This involves two separate OpenStack deployments for the Edge, Radio Access, and Core network domains. The Edge Openstack NFVI includes the simulated 5G UEs, the Next Generation NodeB (gNB) base station, the Edge User Plane Function (UPF), and a generic VNF that provides an application service to the connected users. The Core Openstack includes the control plane of the 5G Core Network, the subscribers' database, and a generic video-processing VNF for service provisioning. The Core Openstack also provides the MTD framework modules, except those that are located in the edge nodes: the MMT probe, Systemic (at the application layer in the VNF), and TopoFuzzer. The NFVO MANO is implemented by Open-Source MANO (OSM) [13]. The core 5G network is implemented with Open5GS [14], a 3GPP Release-16 compliant implementation of the 5G core, while the Radio Access Network (RAN) and the mobile UEs are implemented by UERANSIM [15]. All tools used in this Standalone (5G SA) testbed are open-source implementations.

 DOI: 10.1109/NOMS56928.2023.10154420

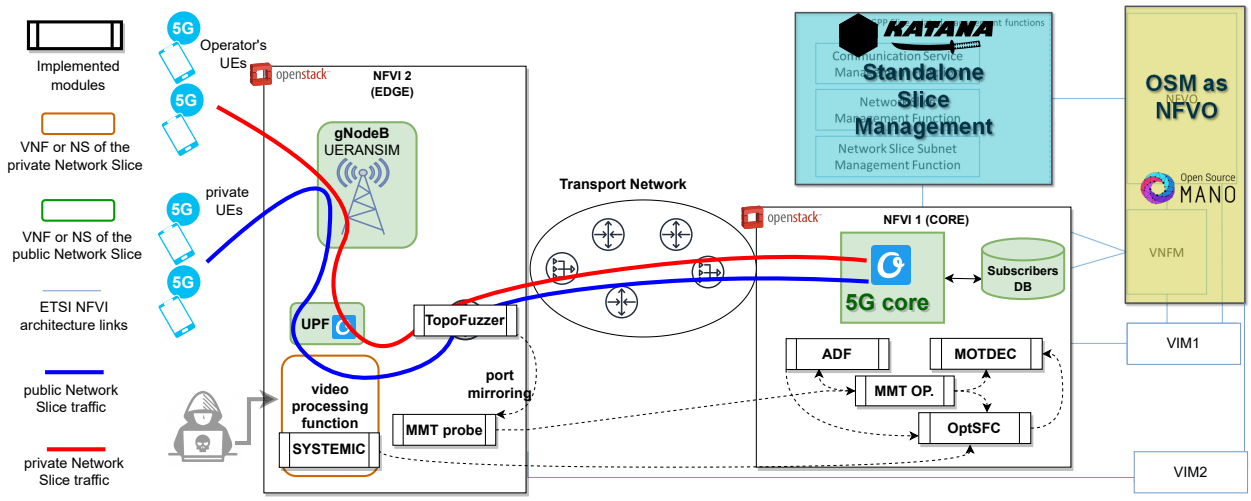

Fig. 2. 5G Testbed with the Integrated MTD Framework

IV. Demonstration Scenarios

Two carefully crafted scenarios have been selected to demonstrate the advantages of the closed-loop orchestration.

A. Proactive Security Scenario

This scenario does not see any active attack, since it is a proactive security situation. Firstly, running network slices and virtual resources are shown using the OSM GUI. Vulnerability scans are performed in OpenVAS, and risk assessment metrics derived from Common Vulnerability Enumerations (CVE) and Common Vulnerability Scoring System (CVSS) are shown. Secondly, network metrics are collected by the network probe every 15 s to measure the network performances. The various metrics aggregated in the MOMDP state are presented, which triggers an MTD operation. Finally, the demonstration displays the enforcement of the MTD operation on the targetted VNF.

B. Reactive Security Scenario

Two types of attacks are triggered: *(1)* tampering attacks on the VNF binary application and *(2)* Command and Control (C&C) botnet traffic. For step (2), attack alerts of Systemic are shown when detecting the first attack, and of ADF, when detecting the second. For the C&C attack, a PoC malware is installed on the edge VNF, sending traffic to the botnet master. The MTD framework neutralizes both attacks by re-initiating or migrating the VNF using a verified non-infected image.

C. Three Demonstrated Aspects

- A technical overview of the developed system.
- Scenarios to illustrate how the PoC system operates.
- MTD framework actions to explain the prevention and mitigation of certain threats.

Acknowledgment

The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

References

[1] ETSI ISG NFV, "Network Function Virtualization (NFV)," European Telecommunications Standards Institute (ETSI), Nice, FR, Standard, Mar. 2012, [Online; accessed 21-October-2022]. [Online]. Available: https://www.etsi.org/technologies/nfv

[2] J. Ortiz *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*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020.

[3] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020.

[4] X. Chai, Y. Wang, C. Yan, Y. Zhao, W. Chen, and X. Wang, "DQ-MOTAG: Deep reinforcement learning-based moving target defense against DDoS attacks," in *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*. IEEE, Aug 2020.

[5] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for ISP networks using SDN and NFV," *Future Generation Computer Systems*, vol. 94, pp. 496–509, may 2019.

[6] S. Sengupta, A. Chowdhary, D. Huang, and S. Kambhampati, "General sum markov games for strategic detection of advanced persistent threats using moving target defense in cloud networks," in *Decision and Game Theory for Security*, T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán, Eds. Cham: Springer International Publishing, 2019, pp. 492–512.

[7] A. Mcabee, M. Tummala, and J. Mceachen, "The use of partially observable markov decision processes to optimally implement moving target defense," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, p. 6986.

[8] G. Chollon *et al.*, "ETSI ZSM Driven Security Management in Future Networks," in *IEEE Future Networks World Forum 2022*. IEEE, 2022.

[9] Themis Anagnostopoulos, "Katana network slice manager," [Online; accessed 21-October-2022]. [Online]. Available: https://github.com/medianetlab/katana-slice_manager

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

[11] G. Brockman, V. Cheung, L. Pettersson, J. Schneider, J. Schulman, J. Tang, and W. Zaremba, "OpenAI Gym," *arXiv e-prints*, p. arXiv:1606.01540, Jun. 2016.

[12] Wissem Soussi, "Topofuzzer - a network topology fuzzer," [Online; accessed 21-October-2022]. [Online]. Available: https://github.com/wsoussi/TopoFuzzer

[13] ETSI, "Open Source MANO." [Online]. Available: https://osm.etsi.org/

[14] S. Lee, "Open5GS." [Online]. Available: https://open5gs.org/

[15] A. Güngör, "UERANSIM." [Online]. Available: https://github.com/aligungr/UERANSIM

 DOI: 10.1109/NOMS56928.2023.10154420