NFV-based network protection: the SHIELD approach

A. Lioy
Politecnico di Torino
Torino (Italy)

G. Gardikis
Space Hellas
Athens (Greece)

B. Gaston
Fundació I2CAT
Barcelona (Spain)

L. Jacquin
Hewlett Packard Labs
Bristol (United Kingdom)

M. De Benedictis
Politecnico di Torino
Torino (Italy)

Y. Angelopoulos
National Center for Scientific Research Demokritos
Athens (Greece)

C. Xylouris
Orion Innovations PC
Athens (Greece)

***Abstract*—This demo showcases some of the capabilities foreseen for the security infrastructure designed by the H2020 SHIELD project. SHIELD exploits NFV for adaptive monitoring of an IT infrastructure and for feeding the data to an analytics engine to detect attacks in real time. An intelligent reaction system is then activated to reconfigure the SDN/NFV infrastructure so that the attacks are thwarted. The SDN/NFV infrastructure itself is protected from attacks thanks to trusted computing techniques, that permit to quickly identify misbehaving nodes. The proposed demo will present detection and reaction to a DDoS attack (by on-the-fly deployment of new virtual network security functions and/or change of network paths), as well as detection of software attacks against virtual network functions (executed in Docker containers) and unauthorized modification of the SDN switching tables and NFV configurations.**

I. Introduction

SDN and NFV offer new capabilities in several respects. With regards to network security, it is very important their ability to easily reconfigure network paths and to change built-in network functionality through the deployment of *Virtual Network Functions (VNF)* in specific network locations as needed.

SHIELD (Securing against intruders and other threats through an NFV-enabled environment) is a H2020 project [1] that aims to exploit SDN/NFV capabilities for creating a protection layer for an IT infrastructure [2] . To this aim, security-specialized network functions (named *virtual Network Security Functions, vNSF*) are developed and exploited. These can be *monitoring vNSF* (to collect data for the analytics engine) or *reactive vNSF* (to implement the reaction to an attack).

The ideas behind SHIELD were driven by three main use cases: (UC1) an *Internet Service Provider (ISP)* or a corporation willing to protect its own infrastructure (while reducing costs and management complexity with respect to a traditional appliance-based design); (UC2) an ISP willing to offer *Security-as-a-Service (SECaaS)* to its customers through its own NFV infrastructure; (UC3) a duly empowered entity, such as an externally appointed *Security Information and Event Management (SIEM)* provider, needing to monitor a network.

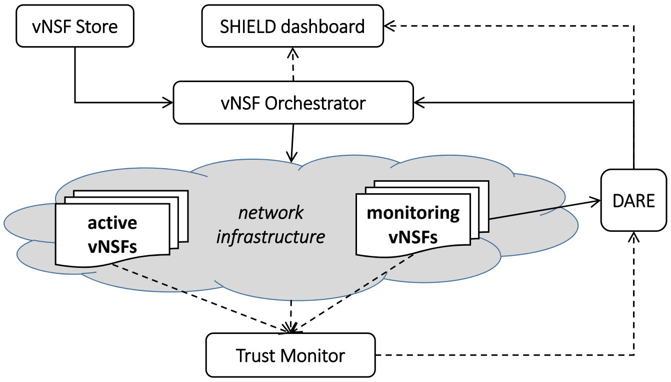

Figure 1. Schema of the SHIELD architecture.

The architecture of SHIELD is depicted in Figure 1 and it is composed of the following main elements:

- a vNSF orchestrator, to manage the deployment and operation of the vNSFs in coordination with other network-oriented operations over the SDN/NFV infrastructure;
- a vNSF store, providing the virtual components used in creating the protection layer;
- the monitoring and acting vNSFs actually deployed into the to-be-protected IT infrastructure;
- the Trust Monitor, in charge to monitor the state of the running vNSFs as well as that of the infrastructure itself (to know which nodes can be trusted to receive the deployment of a new vNSF);
- DARE, the Data Analysis and Remediation Engine, which executes two main tasks: (A) detect attacks based on the information received from the monitoring vNSFs and its own knowledge base, and (B) exploit a rule-based engine to decide which is the appropriate reaction to an attack and request appropriate reconfiguration of the protection infrastructure.
- a dashboard to interact with the relevant users (e.g. network/security managers, duly empowered third-parties).

All these elements are aligned with ETSI-NFV architecture [3] and built on the basic functionalities and prototype components developed in the former FP7 projects T-NOVA [4] and SECURED [5].

II. Demo part I – NFV-based detection and reaction

To demonstrate the capabilities of SHIELD, we designed a demo aiming to detect and react to a *Distributed Denial-of-Service (DDoS)* attack. This permits to showcase several features of SHIELD:

- availability and use of various kinds of vNSFs, namely those for monitoring net-flow traffic and layer 7 filtering (a.k.a. application-level firewall);
- detection of the attack through data collected by the monitoring vNSFs and fed to the DARE, which marks the traffic as suspicious and invokes the actions associated to this kind of threat;
- the DARE defines the "recipes" associated to the specific attack and presents them to the user via the dashboard;
- the user is notified about the incident and applies the mitigation via the dashboard;
- the vNSF orchestrator is requested to block the offending traffic by deploying or activating appropriate firewall vNSFs;
- the orchestrator deploys reaction vNSFs in suitable nodes, blocking the attack.

III. Demo part II – trusted infrastructure

Since SHIELD uses SDN/NFV for protecting a target, the SDN/NFV infrastructure itself must be protected to avoid being subverted by an attacker and not performing its expected protection actions.

Besides standard hardening and protection techniques commonly used to protect NFV and cloud platforms, we place special emphasis on trust and integrity of the virtualised infrastructure. We want to know if the network nodes are in a "good" state, that is if they are running only the provided software (and no other possibly malicious or wrong components) and if the deployed configurations are coherent with those planned at the management and control layers. If the answers to these questions are positive, then we conclude that the infrastructure is in a trusted state and can be used to deploy the required monitoring and acting vNSFs.

Figure 2 depicts the architecture and flows used in SHIELD to monitor the integrity of the infrastructure.

The Trust Monitor periodically polls the nodes in the network to get their integrity reports (via the well-known secure Remote Attestation protocol) and compares the results with those present in a white-list database. This database is populated by the network and security managers that insert information about the acceptable vNSFs, their expected current configurations, and the software components of *NFV Infrastructure (NFVI)* itself.

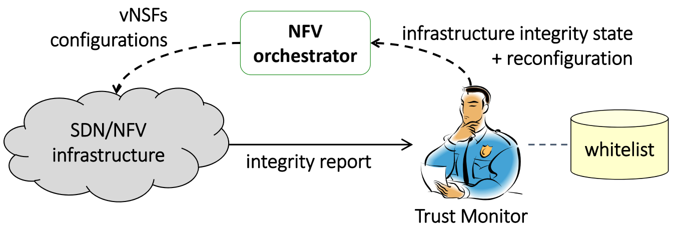

Figure 2. Trust monitoring in SHIELD.

If a miss or a misalignment is detected, the Trust Monitor informs the DARE and the orchestrator, requesting to isolate the offending component and to reconfigure the infrastructure to still provide the expected functionality with other good components. Of course, an investigation by an auditor is also required to understand the source of the problem and prevent bit in the future.

The technology used to implement the Trust Monitor and the integrity attestation framework was developed in SECURED [6] as an extension of the Open Attestation (OAT) framework.

The proposed demo will touch the following points:

- the Trust Monitor verifies the integrity state of the NFVI and reports its good state (including the deployed vNSFs and related configurations);
- an attack is performed on the NFVI (e.g. due to an improperly configured access control on a node) and the attacker deploys a new malicious software component at the node and changes the SDN flow table;
- the Trust Monitor gets the integrity report from the node and detects both a miss and a misalignment with respect to the information in the white-list;
- the Trust Monitor requests the orchestrator to stop the offending vNSF and restore the original SDN flow table;
- the Trust Monitor verifies at the next poll that the NFVI has returned to its original integrity state.

Acknowledgment

The research described here is part of the SHIELD project, co-funded by the European Commission (H2020 grant agreement no. 700199).

References

[1] "The SHIELD project." [Online]. Available: https://www.shield-h2020.eu/

[2] G. Gardikis, K. Tzoulas, K. Tripolitis, A. Bartzas, S. Costicoglou, B. Gastn, C. Fernndez, C. Dvila, L. Jacquin, H. Attak, D. Katsianis, I. Neokosmidis, T. Batista, R. Preto, A. Lioy, A. Litke, N. Papadakis, D. Papadopoulos, A. Pastor, J. Nuez, N. Davri, G. Xylouris, M. Kafetzakis, M. Terranova, C. Giustozzi, E. Trouva, Y. Angelopoulos, and A. Kourtis, "SHIELD: A Novel NFV-based Cybersecurity Framework," in *NetSoft-2017: 3rd IEEE Conference on Network Softwarization*, Bologna (Italy), July 3-7 2017.

[3] ETSI NFV Industry Standardisation Group, "ETSI GS NFV 002 (v1.2.1) – Network Functions Virtualisation (NFV); Architectural Framework," Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf

[4] The T-NOVA project – Network functions as-a-service over virtualised infrastructures. [Online]. Available: http://www.t-nova.eu/

[5] The SECURED project – SECURity at the network EDge. [Online]. Available: https://www.secured-fp7.eu/

[6] L. Jacquin, A. Lioy, D. R. Lopez, A. L. Shaw, and T. Su, "The trust problem in modern network infrastructures," in *Cyber Security and Privacy: 4th Cyber Security and Privacy Innovation Forum, Brussels (Belgium), April 28-29, 2015, Revised Selected Papers*, F. Cleary and M. Felici, Eds. Springer International Publishing, 2015, pp. 116–127.