Security in Softwarized Networks: Prospects and Challenges

1st Nicholas Gray
University of Würzburg
Würzburg, Germany
nicholas.gray@informatik.uni-wuerzburg.de

2nd Thomas Zinner
University of Würzburg
Würzburg, Germany
zinner@informatik.uni-wuerzburg.de

3rd Phuoc Tran-Gia
University of Würzburg
Würzburg, Germany
trangia@informatik.uni-wuerzburg.de

I. Abstract

Today, network security in enterprises is mainly enforced by firewalls guarding the perimeter of the network against an ever increasing number of cyber threats. While inspecting and enforcing security policies on every flow entering or leaving the network, Perimeter Gateway Firewalls (PGF) provide hardly any defense once the perimeter is breached, which allows attackers and malware to easily compromise additional hosts as we have seen in the recent outbreak of the WannaCry worm.

To mitigate such outbreaks, enterprises usually rely on costly Intrusion Prevention Systems (IPS) and a centralized update management to install security updates in a timely manner. Both systems aim to minimize the window, in which the enterprise network is susceptible to attacks. Yet, this is a tedious process as the IPS requires an attack signature and changes to the software stack demands thorough testing. Furthermore, in the case of ZeroDay attacks no signatures and updates are available. Hence, this often results in a widened window in which the network remains vulnerable and an increased risk.

A complimentary approach to alleviate these threats is to quarantine malicious hosts on a network level, as this can be deployed immediately and is independent from the update procedure. To accomplish this, a fine-grained flow selection and security control is needed. Whereas architectures such as Ethane and more recent technologies like Software-defined Networking (SDN) and Network Function Virtualization (NFV) provide this required granularity, the adaptation of these technologies in enterprise networks remains limited. This is due to the fact, that the integration of new technologies into an existing network infrastructure is a highly complex task, as the compatibility with systems such as network management and cloud management has to be assured for production environments. In addition, SDN also broadens the attack surface as novel networking devices and protocols are deployed, which needs to be taken into account during the risk assessment. Especially due to their critical role within the softwarized management of the network, these devices and protocols are high ranked targets for potential attackers and thus require extensive testing and hardening.

In this work, we demonstrate the prospects of seamlessly integrating SDN and NFV based security operations into the existing enterprise network infrastructure to provide state-of-the-art stateful firewalling for advanced packet filtering as well as on-demand fine-grained flow separation and isolation for the exterior and interior network. This is achieved by levering an omnipresent firewall, which is based on cloud principles enabling enhanced scalability and resilience. To proactively ensure the robustness of deployed physical and virtual devices, we present FlowFuzz a fuzzing framework for SDN-enabled software and hardware switches. Here, we focus on the OpenFlow protocol which handles the communication between SDN-enabled switches and the central controlling instance. Whereas the framework utilizes the output of conventional tools such as AddressSanitizer for investigating software switches, it also evaluates data obtained from side channels, i.e., processing times and power consumption to identify unique code execution paths within hardware switches to optimize the fuzzing process. We use our framework implementation to perform a first evaluation of the OpenVSwitch and a total of four SDN-enabled hardware switches. We conclude by presenting our findings and outline future extensions of the fuzzing framework.

References

[1] Lorenz, C., Hock, D., Scherer, J., Durner, R., Kellerer, W., Gebert, S., Gray, N., Zinner, T., Tran-Gia, P., An SDN/NFV-enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement. IEEE Communications Magazine. 55, 217 - 223 (2017).

[2] Pfaff B., Scherer J., Hock D., Gray N., Zinner T., Tran-Gia P., Durner R., Kellerer R., Lorenz C., SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise, ACM SIGCOMM Computer Communication Review, 2017

[3] Gray N., Sommer M., Zinner T., Tran-Gia P., FlowFuzz - A Framework for Fuzzing OpenFlow-enabled Software and Hardware Switches, Black Hat Briefings USA, 2017