Network Security Automation

Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer and Control Engineering (35^{th}cycle)

Network Security Automation

Abstract

By

Daniele Bringhenti

******

Supervisor(s):
Prof. Riccardo Sisto, Supervisor
Dr. Fulvio Valenza, Co-Supervisor

Politecnico di Torino
2022

Network Security Automation

Daniele Bringhenti

In the latest years, softwarization paradigms such as Network Functions Virtualization and Software-Defined Networking shook the traditional vision of networking. The recent evolution of computer networks reflects the main driving force of these paradigms, based on high flexibility and dynamism. Network sizes and complexity are constantly increasing, because enriching a networked service with a new function only requires the deployment of a virtualized or containerized software function. To this regard, the advent of the Internet of Things paradigm led to a pervasive presence of computer and network communications in everyday activities, thus also increasing heterogeneity of applications that are connected to the network. Specifically considering cyber security, the characteristics of modern virtualized networks are no longer compliant with the traditional ways to enforce security. Traditionally, network security management was performed manually by human operators, with trial-and-error approaches where the security status was updated whenever a cyber attack was able to overcome the defenses provided by the previous status. However, such an approach can work only with small-sized and almost static networks, where everything is under the direct control of a human user. Continuing with a manual approach in modern virtualized networks would likely lead human operators to introduce vulnerabilities, which could be exploited to breach into the network, and sub-optimizations, which would reduce network efficiency.

A possible solution to limit this issue is to leverage automation in the approaches pursued for network security management. First of all, automation can contribute to minimizing the number of human interventions, as automatic approaches commonly require only input specifications and human assistance during their independent work. Moreover, automation favors the introduction of two important features, i.e., formal verification and optimization. On the one hand, formal verification can provide correctness assurance of the automatically computed management decisions, thus increasing human confidence in automatic approaches, where many tasks are not under human control. On the other hand, optimization can improve the quality of management decisions. For example, for the task of configuring a network security function such as a firewall, if the configuration rule set is minimized, usually the function requires less time to process packets.

Unfortunately, despite all such benefits that automation could bring over to network security management, currently in the literature it has been successfully applied only to solve networking issues, and rarely to manage security ones.

Therefore, this dissertation aims to fill this literature gap by proposing novel approaches to improve the state of the art about network security automation. The main contributions of this dissertation are related to two main research areas: automatic security configuration and automatic security orchestration. For what concerns automatic security configuration, this dissertation proposes the VEREFOO approach, which solves the configuration problem of network security functions (e.g., firewalls and VPN gateways), by combining automation, formal verification, and optimization. VEREFOO follows the policy-based management paradigm: starting from a user-provided network topology with related security policies, VEREFOO computes the allocation of security functions in the network topology and their configuration rules. This result is computed in a fully automated way, it is formally guaranteed to satisfy all security policies, and it is optimized, including the minimum numbers of allocated functions and configuration rules. This result is achieved by formulating the configuration problem as a Maximum Satisfiability Modulo Theories problem, which enables pursuing correctness by construction and optimization. An extensive experimental evaluation shows not only that the proposed approach is feasible, but also that it scales to networks of significant size and that it provides better optimization than traditional configuration strategies. For what concerns automatic security orchestration, this dissertation addresses some of the open problems that should be solved in order to make this kind of orchestration reliable and efficient. First, an automatic methodology to optimize distributed firewall reconfiguration transients is proposed, in order to limit, as much as possible, the traversal of insecure transient states when new firewall allocation and configuration rules have to be deployed. Second, a novel approach is proposed for network security function selection in the orchestration workflow, based on a novel security function abstraction, which enables more optimized choices. Finally, the integration of the VEREFOO approach within state-of-the-art network orchestrators is discussed, also showing concrete integration examples. Experimental evaluation shows that these proposals can cooperate in close synergy with orchestrators oriented to solve networking problems, thus representing an important step ahead towards full autonomy in network security.