Security and Communication Networks

Special Issue on
Automated Management of Security in Software Networks

WILEY | Hindawi

CALL FOR PAPERS

Enforcing network security requirements is a crucial task that companies, organizations, and private citizens have to deal with in order to preserve privacy, guarantee critical infrastructure resilience, protect intellectual property, and comply with both international regulations and business contracts.

Several studies have reported that human errors in configuring the security controls are, by a large margin, the most significant cause of security breaches and breakdowns. In the past years, approaches have been proposed that aim to automate security enforcement, but have not been widely adopted in the current practice. For instance, policy-based management proposed an approach where the functional behavior and the security of a network are defined by means of policies, which are sets of technology independent rules. Policy-based management aims at increasing the self-managing abilities of network components to reach a more autonomic behavior. Nonetheless, policy-based management relies on policy refinement to translate high-level technology independent goals into concrete configuration settings that can be actually enforced on the managed system by the Network Security Functions available in the network to protect. However, if simple or very specific cases are excluded, translating policies into configuration settings that can be actually enforced by the security controls is still an open issue. Intent-based networking leverages the security of a network on AI methods. Intent-based networking requires the definition of desired functional and security state at high level, the intents, and uses machine learning techniques to automatically translate intents into actual security enforcement rules for the available security controls. Both these techniques have not yet reached their maturity.

Meanwhile, Network "Softwarization" looks promising and in some respects is already delivering flexible management of computer networks. Two technologies are currently driving this progress: Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). NFV and SDN foster flexible and programmable network function deployment and ease of scaling, simplify operational tasks, reduce response times and total cost of ownership, and act as essential components of management automation.

However, the flexibility does not extend to security controls. While networking elements and protocols are designed to automatically adapt to changes, adaptation is not a design principle for security controls, whose configurations require careful adaptation and human intervention at every change. This issue is not only slowing down the adoption of network automation but also reducing the potential adoption of cognitive methods for security management. However, a large amount of data is available at the Management and Orchestration (MANO) level that could be used for automatic security enforcement.This special issue aims to attract both theoretical and practical works that deal with the automatic management of security in Software Networks that rely on NFV and SDN. Its focus is on the construction of modern network software-intensive systems at the modelling, implementation, and runtime stages, with a special focus on reuse at postdeployment and runtime.

We welcome submissions covering the different aspects of security management in network automation mechanisms and virtualized environments.

Potential topics include but are not limited to the following:

- Automated deployment of security configurations in Software Networks
- Intent-based networking
- Integration of security-related operations in NFV MANO
- Automated analysis of security properties in Software Networks (SN)
- *AI algorithms for automatic threats and attacks identification
- Methods for automatic threats analysis in SN
- Models of capabilities for automatic management of Network Security Functions (NSF)
- Seamless adaptation of security policy enforcement rules after policy changes
- Models for dynamic adaptation of security policy enforcement rules
- *Management and control interfaces of NSF in NFV
- Autonomic management of virtualized networks
- Security policy-aware SDN configuration
- Security policy-aware MANO
- Optimal NSF allocation for security policy enforcement
- Automatic privacy policy enforcement
- Policy-based security management frameworks
- Security policy refinement in Software Networks
- AI algorithms for policy identification
- AI methods for checking correctness of security policy enforcement
- Auditability and verifiability of security policies in Software Networks

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/smsn/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Cataldo Basile, Politecnico di Torino, Turin, Italy
cataldo.basile@polito.it

Guest Editors
Diego López, Telefonica I+D, Madrid, Spain
diego.r.lopez@telefonica.com

John C. Strassner, Huawei Technologies, Santa Clara, USA
john.sc.strassner@huawei.com

Submission Deadline
Friday, 19 April 2019

Publication Date
September 2019