2018-00434 - PhD Position/ Compressed and Verifiable Filtering Rules in Software-defined Networking [S]

Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

Contexte et atouts du poste

The proposed PhD is a CIFRE thesis that will take place at Inria Nancy Grand Est laboratory in collaboration with the industrial partner Cynapsys Technologies (www.cynapsys.de).

The contacts at Inria for information and application are
Dr Abdelkader Lahmadi (Team Madynes) abdelkader.lahmadi@loria.fr
Dr Michael Rusinowitch (Team Pesto) michael.rusinowitch@loria.fr

The Inria research team Pesto (https://www.inria.fr/en/teams/pesto) relies on formal models and techniques, for computer-aided analysis and design of security protocols (in a broad sense). The Inria research team Madynes (https://www.inria.fr/en/teams/madynes) develops applied and experimental research dedicated to the management (monitoring, security and configuration) of the Future Internet.

Mission confiée

SDN (Software Defined Networking) is a recent networking paradigm which enables networks to be programmable by separating data and control planes [1]. The control plane is managed by the controller to configure various network services including firewalls, IPS and IDS security functions. These functions are mainly chained by means of network policies that are translated to flow forwarding rules to be applied by the switches. In SDN environments these functions, and in particular firewalls, are implemented as network functions with dedicated hardware or in virtualized environments to inspect and filter traffic or they are implemented as a built-in controller application which takes decisions and deploys the filtering rules over the switches, as proposed in [2]. SDN is an approach to computer networking that allows network administrators to manage network services through the abstraction of higher level functionality. Most of these security functionalities rely on filtering techniques applied on flow and packet properties including addresses (IP or MAC) and ports to accept or drop travelling packets. However, making such filtering distributed over SDN switches and dynamic to be able to cope with network updates and to mitigate multiple types of attacks (DDoS, botnet infections, etc) carried out by external and insider attackers is a challenging task. It is important to aggregate [3], distribute and process these filtering rules in an efficient manner since they will be processed and stored inside SDN switches which are resource constrained devices. In addition, the filtering rules may be conflicting between them or with flow policies provided by the controller to realise network services thus it is also important to verify their consistency and conflicts.

Principales activités

In this PhD, we will rely on a new filtering technique using double-masked IP blocks [4] for IP exact, prefix and arbitrary matching instead of using classical single masks [5]. The multi-masked technique is able to aggregate IP blocks even not numerically adjacent and it helps compacting the filtering policy, optimising the memory usage and speeding up the controlling process: any packet coming into the network is examined by the control plane...
and a decision is taken to drop or to accept the packet based on a predefined list of rules that needs to be compacted and well ordered to guarantee an optimized processing time and less memory usage. The goal of this PhD is to design, implement and evaluate multi-masked techniques for building a compressed and verifiable filtering rules in Software Defined Networks with the possibility of distributing the workload processing among several packet filtering devices operating in parallel. The first axis of the work consists of designing efficient algorithms and models that can be implemented to compress the filtering lists in Software-defined Networks using the multi-masked compression techniques. The proposed solutions have to be implemented, tested and their performance evaluated within an SDN environment (OpenFlow switches) and also compared with traditional IP filtering mechanisms in networking environments (Netfilter/iptables). The second axis of the work is dedicated to the formal verification of the resulting filtering rules and their consistence to detect and resolve conflicts, anomalies and non-compliance with the original filtering policies. On one hand, the multi-masked compression techniques to be used may limit the expressivity and the readability of the configuration as it changes the original rules spaces. On the other hand, the network topology continuously evolves and the users always request new services for any new development. Therefore, the filtering policies become increasingly complex and the resulting lists of rules are susceptible to be non-optimal after each modification performed by the network administrator or SDN controllers.


Compétences
Applicant for this position must have an MSc or equivalent in computer science or Telecommunications. The PhD candidate should have these skills:

- Solid background and interest in networking with a knowledge about network security
- Solid background and interest in algorithms and data structures (some knowledge about formal methods is welcome, too)

Applicant have to send a detailed CV to:

abdelkader.lahmadi@loria.fr
michael.rusinowitch@loria.fr

Avantages sociaux
- Subsidised catering service
- Partially-reimbursed public transport

Rémunération

Monthly salary after taxes : around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd