Scientific Report: Short Term Scientific Mission

COST Action CA15127

Sandra Scott-Hayward

1. STSM Details

STSM Title: SDN-based anomaly detection of network failures and misconfigurations

STSM Applicant: Dr. Sandra Scott-Hayward, Queen's University Belfast, Belfast, U.K.

Host: Prof. Stefano Secci, CNAM, Paris, France

Period: January 5-13, 2019

Working Group: WG3

2. Purpose of the STSM

The purpose of the STSM was two-fold:

- To develop a collaboration between the Network Security research group at Queen's University Belfast (QUB) and the networking research group at Cnam, Paris.
- To define the scope of a research activity building on anomaly detection research in progress in the research group of Stefano Secci, and in particular of the PhD student Agathe Blaise, which we identified closely aligns to QUB Software-Defined Network (SDN) security research directions.

3. Description of the work carried out during the STSM and main research results obtained

Seminar

During the STSM visit, Sandra delivered a seminar to introduce QUB Centre for Secure Information Technologies (CSIT) and to present QUB SDN security research. The title of the seminar was "Scalable Network Security with SDNFV". A detailed presentation of the motivation and functionality of TENNISON [1], a distributed SDN framework for scalable network security, was presented. The objective of TENNISON has been to develop a distributed SDN security framework that combines the efficiency of SDN control and monitoring with the resilience and scalability of a distributed system. The provision of multi-level monitoring and distributed control to enable efficient network attack remediation was

described. A second element of the presentation was OFMTL-SEC [2], which provides network security protection at the data plane, again enabling efficient network protection. This is particularly relevant to the RECODIS COST Action with the focus on the resilience of communications in existing and future communication network architectures. A lively discussion was had during the seminar regarding the motivation for the design of TENNISON and the challenges to implementation based on the state-of-the-art in open-source and commercial SDN equipment.

Research Collaboration

Over the course of the STSM visit, Sandra worked with Agathe Blaise, a PhD student with Stefano Secci, discussing Agathe's work on early detection of unknown botnets. In the research discussion, information was shared regarding anomaly detection techniques, data sets for experimentation and evaluation, and appropriate attack remediation mechanisms with SDN. A scope of work has been defined for a follow-on STSM visit by Agathe to QUB. The objective of the work will be to implement the early detection of unknown botnets anomaly detection algorithm at the SDN switch-level. This will enable an efficient mitigation of botnet-enabled network attacks.

Book Chapter

A planned outcome of the STSM was a contribution to the RECODIS book on SDN-based anomaly detection of network failures and misconfigurations. Based on discussion during the STSM, the proposed topic for the book chapter is a review of existing scalable and collaborative security monitoring and attack detection/protection methods in SDN, and a comparison of these proposed frameworks with respect to their practicality/feasibility for deployment. We believe that this topic aligns well with RECODIS and will provide a useful source of information regarding scalable and collaborative SDN-based anomaly detection. Work has already begun on developing the content of the book chapter.

Research Discussions

In addition to the anomaly detection and SDN discussions described above, a number of valuable discussions took place with local and visiting researchers:

- With Prof. Otto Duarte (Federal University of Rio de Janeiro), we discussed the challenges of practical implementation of scalable SDNFV solutions.
- With Dr. Marco Fiore (researcher at the Italian National Research Council, CNR-IEIIT), we discussed mobile traffic analysis and the ability to leverage mobile traffic for anomaly detection linked to both general network functionality and, potentially, security issues.
- With Dr. Thi-Mai Trang Nguyen (LIP6), we discussed recent performance comparison measurements between two widely-used SDN controllers; Open Network Operating

System (ONOS) and OpenDaylight (ODL) and security vulnerabilities related to the topology discovery functionality within SDN.

- With PhD and Masters students, we discussed the requirements for multiple controllers in SDN to support network resilience, and the mechanisms of clustering with specific SDN controllers such as ONOS and ODL.

4. Future collaboration with the Host institution

As anticipated, the groups of Dr. Sandra Scott-Hayward and Prof. Stefano Secci share many research interests. We plan to continue collaboration beyond the scope of the STSM, initially with the proposed visit by Agathe Blaise to Queen's University Belfast in Spring 2019. A number of other potential topics for collaboration will be explored based on the research discussions described in the previous section.

[1] Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A. and Race, N. "TENNISON: A distributed SDN framework for scalable network security", IEEE Journal on Selected Areas in Communications, Dec. 2018.

[2] Scott-Hayward, S. and Arumugam, T. "OFMTL-SEC: State-based Security for Software Defined Networks" In Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE Conference on. IEEE, 2018.