SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127
STSM title: SDN-based anomaly detection of network failures and misconfigurations
STSM start and end date: 25/02/2019 to 08/03/2018
Grantee name: Agathe Blaise

PURPOSE OF THE STSM:

The first motivation for this STSM was to pursue the collaboration between the Network Security research group at Queen's University Belfast (QUB) and the networking research group at Cnam. Secondly, we wanted to discuss and continue the ongoing work between both institutions, in terms of SDN anomaly detection research. Indeed, the research at Cnam on anomaly detection, closely aligns to QUB Software-Defined Network (SDN) security research directions. During the first visit, a conceptual outline of this work had been discussed to establish a work plan for the next few months, including this visit. Also, the relevant content for the RECODIS book chapter given our collaboration had been discussed, leading to the table of contents.

As a result of the first STSM, we anticipated the following outcomes for this one:

1. Consolidation of the collaboration between QUB and Cnam, to follow up the visit of Sandra Scott-Hayward in January 2019.
2. Review of ongoing work on the implementation of a real-time anomaly detection system in SDN for early identification of network failures, since the visit of Sandra Scott-Hayward.
3. Experimentation of the solution on QUB equipment.
4. Follow-up contribution to the RECODIS book on SDN-based anomaly detection of network failures and misconfigurations.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

The STSM was the opportunity to pursue the collaboration between both institutions, in the field of anomaly detection using benefits of programmable networks. In particular, we carried on our work on the implementation of a real-time anomaly detection system in SDN for early identification of network failures. First we discussed the work achieved between the two visits. During that time, we developed an experimentation/evaluation plan, and began to implement the algorithm with simulation tools. Then, the STSM was the time to merge our ideas, in order to establish a proper work program and to define objectives. We also got the opportunity to test our first pieces of work using QUB equipment and test bed, as it owns smart NICs from Netronome, enabling development of P4 algorithms. Performing some tests on a specific equipment helped us in designing a realistic algorithm, having a better knowledge of the possibilities and limitations of a programmable switch.

We also discussed our research findings on SDN monitoring and anomaly detection, in order to continue the ongoing work on the RECODIS book chapter. More specifically, we highlighted some important parts, such as (i) the need for collaboration between several detection agents, to balance the workload and be able to detect large-scale anomalies in Cloud environments, and (ii) existing SDN-based intrusion detection systems taking advantage of SDN and NFV. Finally, we propose a solution for a scalable and collaborative intrusion detection system, that benefits from programmable networks using technologies such as P4. This is in line with our algorithm that detects anomalies in a SDN environment.

I also met with the staff and students in the networking research group. This was very interesting to discover another environment and to discuss with researchers working on related topics. I met with Sandra's PhD student who works on the same area as me, using eBPF which is a technology similar to P4. I also attended presentations by several PhD students. From this experience, I really liked the opportunity to ask them questions, to share ideas, and to discuss some important topics in networking.

Finally, I attended the RISE spring school that was hosted at QUB for two days. It brought together the hardware security community, both academic and industry. This was a great opportunity to hear from experts in that field, and to learn about an important subject related to security.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The STSM was successful, as we have been able to fulfill the objectives that we had defined. First, the STSM was the opportunity to consolidate the collaboration between QUB and Cnam, to follow up the visit of Sandra Scott-Hayward in January 2019.

Second, we produced the RECODIS book chapter, as we planned during the first visit. It now contains significant content about scalable and collaborative anomaly detection in an SDN context. In the last part we proposed our solution for an efficient network anomaly detection, taking advantage of the configurable data plane in SDN, and the collaboration between several controllers, also eased by SDN and NFV. This introduces our work on the implementation of an anomaly detection algorithm in such networks.

Finally, we completed the theoretical design to implement our algorithm, dividing it into several main steps, and determining whether each step is best implemented at the switch level (no overhead but limited operations) or externally. We also discussed the experimental testbed and the relevant metrics for the evaluation. Then, we directly programmed the programmable switches, so that now we have some important pieces of code for our anomaly detection algorithm. Given these first experiments, we have been able to establish a plan of the remaining work to do on the algorithm.

FUTURE COLLABORATIONS (if applicable)

During this visit, we continued our work on anomaly detection of network failures and misconfigurations in an SDN environment. We made significant progress on that part during the STSM, as we were able to program and test our algorithms directly on QUB equipment. Now we have a clearer view about what it is possible to do, and we plan to finish it in the next few months. Ultimately, we would like to write an article about the implementation of the detection algorithm, as a result of our collaboration.

Also, we plan to pursue our work on the RECODIS book chapter. In particular, we have to make some final adjustments to the chapter before it goes to review. Following review, we will make any necessary amendments.