PERFORMANCE STUDY OF MAKING IDSS SELF-ADAPTABLE IN IAAS CLOUDS

CHRISTINE MORIN, ANNA GIANNAKOU, LOUIS RILLING
MYRIADS TEAM

Infrastructure as a Service (IaaS) clouds use virtualisation to allow tenants to outsource their information systems in the operator's cloud. Key characteristics of IaaS clouds include scalability, multi-tenancy and resource sharing. Tenants can also automate the creation, destruction or reconfiguration of virtual machines (VM) and networks. However, the same characteristics that make IaaS clouds agile and dynamic, also affect the ability of a security monitoring framework to successfully detect attacks [1]. Traditional security monitoring frameworks are not designed to automatically cope with reconfigurations of the virtual environment, and the potentially high rate of such reconfigurations makes it impossible for a security administrator to reconfigure the security monitoring framework accordingly. For these reasons, a successful cloud-tailored security monitoring framework should automatically adapt its components whenever the information system is reconfigured or relocated in the cloud.

A security monitoring framework is based on probes in the information system, like Intrusion Detection Systems (IDS). In particular, Network-based IDSs (NIDS) analyse the network traffic to detect attack attempts and abnormal behaviour.

The purpose of this internship is to extend a self-adaptable cloud security framework called SAIDS [2], in order to understand the requirements of different kinds of IDSs, and study the performance impacts and benefits of using adaptation in the security monitoring framework. The student should:

(1) write SAIDS drivers for Suricata and Bro NIDSs (SAIDS already features a driver for Snort);
(2) study the performance impact of NIDS adaptation on cloud configuration changes (VM creation, deletion, migration as well as addition or removal of services in VMs);
(3) study how self-adaptation can help making NIDSs scale with the monitored network traffic.

References

[1] N. Shirazi et al. Assessing the impact of intra-cloud live migration on anomaly detection. In *Proc. CloudNet*, 2014.

[2] A.Giannakou et al. Towards Self Adaptable Security Monitoring in IaaS Clouds. In *Proc. CCGrid*, 2015.