HOW TO EVALUATE THE COMPLIANCE OF A SECURITY EVENT FLOW SETUP TO SLAS

CHRISTINE MORIN, AMIR TESHOME, LOUIS RILLING
MYRIADS TEAM

Key words: IaaS cloud, security monitoring, SLA
Contacts: Christine.Morin@inria.fr, amir-teshome.wonjiga@inria.fr, louis.rilling@irisa.fr
Location: IRISA/Inria Rennes - Bretagne Atlantique (Rennes), Myriads team (`https://team.inria.fr/myriads`)

Infrastructure as a Service (IaaS) clouds use virtualisation to allow tenants to outsource their information systems in the provider's cloud. Key characteristics of IaaS clouds include scalability, multi-tenancy and resource sharing.

One of the risks of moving to a public cloud is losing full control of the information system infrastructure. The provider will be in charge of monitoring the physical infrastructure and providing the required service to clients. This pushes clients to have trust on providers. Providers give assurance on some aspects of the service but, as of today, security monitoring is not one of them. In our work, we aim to allow providers to provide customers with guarantees on security monitoring of their outsourced information system.

We focus our work on security monitoring in clouds. *Security Monitoring* is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. By monitoring a system it is possible to detect suspicious behaviors and take action before severe damage.

A security monitoring framework is based on probes in the information system, like Intrusion Detection Systems (IDS). Probes generate security logs that are processed by several tiers until they reach the security operator [1]. The intermediate tiers are composed of log collectors and aggregators, which configurations, numbers, and locations in the network must be carefully chosen to achieve required properties like timeliness and reliability [2].

In an IaaS cloud, the security monitoring frameworks of the tenants are partly implemented by the provider outside of the virtualized information systems, so that components like IDSes and log collectors may be less vulnerable to attacks and can be shared between tenants. Thus the provider has to automatically configure security monitoring components for the tenants.

A Service Level Agreement (SLA) is a contract between clients and service providers. SLAs describe the provided service, the rights and obligations of both

parties and state penalties for when the specified terms are not respected. Hence, SLAs help providers to build more trust.

To include security monitoring terms into an IaaS cloud SLA, the following tasks are required:

(1) a way for providers/clients to specify their security monitoring parameters/requirements,
(2) mechanisms to enforce these requirements in a cloud infrastructure,
(3) a verification method to check if the requirements are respected at any given time.

The purpose of this internship is to study IaaS cloud SLA security monitoring terms related to the intermediate tiers of security log management. This should extend the work in progress about security monitoring terms related to a network IDS [3]. The student's objectives are:

(1) to find relevant metrics to describe the compliance to SLAs of a setup of the log collection and aggregation tiers in the provider part of the security monitoring frameworks;
(2) to design methods for a tenant to verify online that the provider has setup the collection and aggregation tiers correctly according to the SLA terms;
(3) to implement and evaluate a selection of the verification methods designed.

References

[1] Karen Kent and Murugiah Souppaya. Guide to Computer Security Log Management. Special Publication 800-92, National Institute of Standards and Technology (NIST), 2006.

[2] Roland Rieke, Luigi Coppolino, Andrew Hutchison, Elsa Prieto, and Chrystel Gaber. Security and Reliability Requirements for Advanced Security Event Management. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pages 171–180. Springer, 2012.

[3] Amir Teshome, Louis Rilling, and Christine Morin. Including Security Monitoring in Cloud Service Level Agreements. In *Symposium on Reliable Distributed Systems (SRDS)*, Budapest, Hungary, September 2016.