PhD Topic
Reactive Security Monitoring in Clouds

Place of work: IRISA / Inria Rennes Bretagne Atlantique, Rennes, France

Team: Myriads team (`https://team.inria.fr/myriads`)

Advisors: Christine Morin (Inria) and Louis Rilling (DGA-MI)

Start date: October 2017

Funding: position funded for 3 years (typical duration of a PhD thesis in France)

Requirements

- Master of Computer Science degree or equivalent diploma
- A previous experience or internship in security, cloud computing or distributed systems is desirable.
- Fluent in English (French speaking not necessary)
- Strong team-working abilities

Application file (to be sent to the two advisors in a single pdf file):

- Cover letter
- Detailed curriculum vitae
- Two reference persons including the Master internship advisor (provide their email addresses)
- Transcripts for Bachelor and Master studies
- Links to master's and internship's thesis/reports, and publications if applicable

Deadline for application: April 10th, 2017

Contact: advisors (firstname.lastname@inria.fr)

Detailed description

Context With cloud computing, client organizations outsource part of their information system (IS) in virtualized infrastructures (set of virtual machines (VM) interconnected through virtual networks), hosted in the physical infrastructure of a cloud provider. A Service-Level Agreement (SLA) is a contract signed by cloud customers with their cloud providers that defines guarantees on the provided service [1, 2, 3]. The provided services usually relate to performance, availability, and security. For each of these categories of service, Service Level Objectives (SLOs) define quantitatively (using metrics) or qualitatively (using operational modes) the performance that the provider commits to deliver.

Motivation Compared to an information system implemented on a bare-metal physical infrastructure, an outsourced information system exhibits a very dynamic configuration and is exposed to additional threats, especially due to multi-tenancy.

We are interested in security monitoring. In an IS implemented on a bare-metal physical infrastructure, the security monitoring system is implemented in the same infrastructure and is entirely controlled by its owner organization. In clouds, the security monitoring of an outsourced IS cannot entirely be controlled by the cloud client organization and benefits from being partially implemented externally to the virtualized infrastructure, for instance in the hypervisor running on cloud servers [4, 5]. Reasons include robustness against threats, threat coverage, and cost.

In this thesis we propose to study how to automatically reconfigure the security monitoring in reaction to a broad range of causes, especially the evolution of vulnerabilities and threats. Two properties of clouds support this proposal. First, the programmable-reconfiguration features offered by clouds can help to reconfigure the security monitoring automatically. Second, from the client's point-of-view, the SLA is a convenient interface to define a high-level quality of security monitoring service while letting the provider monitor the evolution of common vulnerabilities and threats.

Challenges In order to make cloud security monitoring reactive to context changes, two main challenges must be solved. First, in the SLA, the SLOs should take into account the possibility of reaction and its causes, because reaction may change the security level required in different aspects. For instance, the emergence of new types of attacks on a given service requires that new detection rules should be added in an intrusion detection system, whereas the upgrade of a vulnerable service fixes some known vulnerabilities and make related intrusion detection rules useless. This first challenge raises two sub-challenges. (i) A classification of context changes that require a reconfiguration reaction should be built, in order to identify the classes of context changes that are relevant to deal with automatically, and, for each of these identified classes, to study the required flexibility in SLOs. (ii) For each of these context changes classes, common reaction strategies and the required infrastructure support should be studied. Reaction strategies should especially aim at combining SLOs with a context change in order to derive a new security monitoring setup.

To address this first challenge we propose to introduce an upper level of SLO that we call *reaction-aware SLO*, which formalizes the overall objective that reaction should target. The classification of context changes should help to find an adequate level of abstraction for this objective formalization (for instance "To detect the ten most probable attacks on my web application"). Translation strategies to infer a concrete SLO (for instance "Add NIDS rules for the known SQL injection attacks on WordPress v4.4.5 + Custom Contact Form v5.1.0.2") from a previous concrete SLO and a context change will then be studied.

The second challenge is to find strategies to automatically reconfigure a whole security monitoring setup. The main objectives are to keep respecting security monitoring SLOs during the reconfiguration and to apply the reaction strategy for an actual context change. Three sub-challenges should especially be addressed. (i) The security monitoring components involved may depend on each other regarding their configuration (for instance an intrusion detection probe must be connected to a log collector to send alerts), and these dependencies must be taken into account during the reconfig-

uration. (ii) The provider may use a same security monitoring component for several clients, and thus the reconfiguration must take into account the SLOs of every clients, even if only one client is concerned by a given context change. (iii) On a context change, the reconfiguration must organize the transition from a previous security monitoring setup to a new setup that has different monitoring rules, while keeping respecting the SLOs. For instance, the transition should not, even temporarily, lower the detection level and let some detectable attacks run undetected.

To address this second challenge, we propose to proceed incrementally. First coordinated reconfiguration algorithms could be studied without reaction to context changes, that is with constant concrete SLOs. Second, the studied reconfiguration algorithms could be adapted with transition strategies from a previous set of concrete SLOs to a new set of concrete SLOs.

Evaluation The studied strategies and algorithms will be implemented in prototypes in order to evaluate experimentally on the Grid'5000 experimentation platform (`http://www.grid5000.fr/`) the feasibility and the tradeoffs between security, performance, and cost.

References

[1] Roberto G. Cascella, Lorenzo Blasi, Yvon Jegou, Massimo Coppola, and Christine Morin. Contrail: Distributed Application Deployment under SLA in Federated Heterogeneous Clouds. In *The Future Internet*, pages 91–103. Springer, Berlin, Heidelberg, May 2013. DOI: 10.1007/978-3-642-38082-2_8.

[2] Stefania Victoria Costache, Nikos Parlavantzas, Christine Morin, and Samuel Kortas. Merkat: A Market-based SLO-driven Cloud Platform. In *5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013)*, Bristol, United Kingdom, December 2013.

[3] Djawida Dib, Nikos Parlavantzas, and Christine Morin. SLA-based Profit Optimization in Cloud Bursting PaaS. In *14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Chicago, United States, May 2014.

[4] Tal Garfinkel and Mendel Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *10th ISOC Annual Symposium on Network and Distributed Systems Security Symposium (NDSS'03)*, February 2003.

[5] Sylvie Laniepce, Marc Lacoste, Mohammed Kassi-Lahlou, Fabien Bignon, Kahina Lazri, and Aurelien Wailly. Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor. In *Proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, SOSE '13, pages 25–36, Washington, DC, USA, 2013. IEEE Computer Society.