Towards Automating Security Enhancement for Cloud Services

Mohamed Oulaaffart, Remi Badonnel, Olivier Festor

Towards Automating Security Enhancement for Cloud Services

Mohamed Oulaaffart
RESIST Research Team
LORIA/INRIA Nancy Grand Est
54600 Villers-les-Nancy, France
mohamed.oulaaffart@loria.fr

Remi Badonnel
RESIST Research Team
LORIA/INRIA Nancy Grand Est
54600 Villers-les-Nancy, France
remi.badonnel@loria.fr

Olivier Festor
RESIST Research Team
LORIA/INRIA Nancy Grand Est
54600 Villers-les-Nancy, France
olivier.festor@loria.fr

***Abstract*—Cloud infrastructures provide new facilities (elasticity, load balancing, easy integration) to build and maintain elaborated services built from multiple resources in a flexible manner. The changes that continuously affect these services, in particular the migration of resources amongst such cloud infrastructures, induce configuration changes. These latter may generate new vulnerabilities that can compromise the confidentiality, integrity and availability of services. Our approach aims at automating the security enhancement of cloud composite services during the migration of their elementary resources. In that context, it first relies on investigating to what extent orchestration languages can be extended to support such automation. It then requires the design of a framework enabling security automation, in order to adapt and complement the configuration of these elementary resources. This includes specifying dedicated algorithms for selecting adequate security mechanisms before, during and after the migration of one or several resources composing an elaborated service. Finally, it should exploit the complementary of endogenous and exogenous mechanisms for supporting such security enhancement.**

***Index Terms*—Cloud Security, Orchestration Languages, Resource Migration, Automation, Composite Services**

I. Introduction

Cloud infrastructures contribute to the building of elaborated services based on multiple computing resources by composing and configuring a large variety of resources, such as virtual machines, network devices, software components [1]. These resources may be deployed across different infrastructures owned by one or several cloud provider(s), and are subject to changes over time. This increases the complexity of management tasks and the probability of vulnerability occurrences. Such security concerns may compromise the entire cloud service. In particular, the migration of cloud resources, which consists of transferring some components of a cloud application from a given provider (or a given infrastructure) to another one, poses key security challenges. This process is often motivated by performance and cost objectives, such as workload balancing, resource collocation, fault tolerance and maintenance of cloud resources. Despite these benefits, the changes induced by migration activities may directly impact the security of cloud services and their resources exposing them to potential attacks. Indeed, the modification of resource and service configurations during the migration process may involuntarily generate vulnerable states and increase their security exposure. In addition, the contextual changes may also contribute to potential vulnerabilities that might cause important damages, such as disclosure of information, data loss and data tampering [2], [3].

Supported by the project CONCORDIA that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927

In that context, our approach consists in automating security enhancement for cloud services and their resources in order to maintain safe configurations. We consider exploiting orchestration language extensibility to enable the specification of security enhancements for cloud composite services, according to different orchestrated security levels. The objective is to integrate into such specification the security mechanisms that may be activated or not, depending on contextual threats, in order to protect the cloud services. We then propose to design a dedicated framework with specific algorithms for supporting the security of cloud services during the migration phase, by taking into account configuration changes and dependencies amongst resources. We are also considering the complementarity of endogenous and exogenous security mechanisms with that respect.

The remainder of this paper will be organized as follows. Section II describes existing work related to orchestration languages and cloud security automation. Section III highlights the proposed approach for automating security enhancement for cloud composite services, and details the three main underlying axes in terms of specification, architecture and security mechanisms. Section IV shows to what extent risk management algorithms could support the automated selection of security mechanisms through different illustrative examples. Finally, Section V gives the conclusions of the paper and points out future research perspectives.

II. Related work

In this section, we give an overview of existing work related to our cloud security automation approach, with a focus on orchestration languages for cloud services, as well as on exogenous and endogenous methods for securing cloud resources, in particular during migration activities. We will look especially at solutions exploiting orchestration languages to support security management.

Cloud orchestration refers to the process of managing the whole lifecycle phases of cloud composite services. This process covers selecting, describing, configuring, deploying, monitoring, and controlling such cloud applications. In order to perform and automate this lifecycle, we typically rely on orchestration languages for describing them and detailing their elementary resources. They allow automating the deployment of cloud services across distributed cloud providers regardless of the underlying platforms or infrastructures, and provide multiple extension facilities to cope with management operations. Amongst these orchestration languages, we can highlight the Heat Orchestration Template (HOT) [4], the Topology and Orchestration Specification for Cloud Applications (TOSCA) [5], [6], and the AWS CloudFormation language [7], [8]. The first one has been introduced by the HEAT project from the OpenStack cloud foundation, and is interpretable by an orchestration engine to build and deploy different composite cloud services at the IaaS layer. The TOSCA open-source language, proposed by OASIS, introduces complementary features to cover additional service layers (IaaS, PaaS, SaaS), and supports the specification of different orchestration levels. It also permits the definition of relationships, capabilities and requirements with respect to cloud resources. AWS Cloud Formation proposes similar features to orchestrate Amazon cloud web services, but corresponds to a proprietary solution. The extensibility of such orchestration languages constitutes an opportunity for specifying security levels and constraints to be taken into account during the migration of resources [9].

Solutions to protect cloud resources include endogenous security mechanisms that directly impact the cloud resources, such as generating specific cloud resources with low attack surfaces, modifying the internal parametrization to prevent vulnerable configurations, and exploiting certification techniques for guaranteeing cloud resource behaviours. For instance, the authors of [10] propose to extend an orchestration language to drive the generation of protected unikernels, corresponding to lightweight virtual machines composed only of the strict necessary packages and libraries. In this case, any configuration changes imply the re-generation of a new virtual machine. Vulnerability management methods, such as developed in [11], consists of assessing the configuration of cloud resources by comparing them to known vulnerability description datasets. This permits the identification of potential unsafe configuration states, and select corrective operations, if available, to modify the configuration of the concerned cloud resources before their migration. Furthermore, certification solutions, such as [12], [13], enable the elaboration of a trusted ecosystem for cloud resources. They consist in exploiting certificates to guarantee the resource behaviours. These approaches are initiated with the certification of cloud resources in a controlled environment. After the deployment of cloud services, the resources are continuously tested in order to control their behaviours and maintain the validity of certificates. Alternatively, exogenous security mechanisms aim at protecting the cloud resources by exploiting external security functions [14], [15]. For instance, the authors of [16] propose a security orchestrator built from the NFV MANO orchestrator. The solution is centered on access control rules that are enforced on resources and are specified using an orchestration language extension. Furthermore, audit approaches such as [17], [18] aim at evaluating cloud service providers before the migration of resources, and then during the operation of resources. Evidence may typically be collected from the cloud service providers to determine the level of trust with respect to the infrastructure of a given provider, and its capability to comply with the expected security policy.

III. Proposed approach

We propose an automated approach for supporting security enhancement in cloud composite services, with a particular focus on issues related to resource migration. Figure 1 illustrates a composite cloud service composed of more than ten components (orange nodes), distributed over three different cloud providers. These components are linked to each other by horizontal dependencies when the components belong to the same layer and vertical ones when the components are in different layers. The migration of a cloud component (symbolized by the black narrow) from one cloud provider (or infrastructure) to another one modifies the configuration of the composite service and requires security enhancement methods to maintain its security level. Our approach relies on three pillars: the extension of an orchestration language for specifying security requirements, the specification of a dedicated framework with adequate security algorithms for selecting protection mechanisms, and the evaluation of the complementary of exogenous and endogenous techniques.

The first pillar concerns the extension of a cloud orchestration language, such as the TOSCA language, in order to evaluate its exploitability for supporting security enhancement automation. The purpose is to take into account the horizontal and vertical dependencies that are specified by the language in the composite service description, in order to drive the security enhancement. For instance, the horizontal dependencies depend on the relationship that may exist between two interconnected resources located on different nodes, while the vertical dependencies concern a given software product with respect to the running operating system. The extended language may serve as support for defining different orchestrated security levels, and expressing alternative configurations that permit to maintain security during migration activities. These alternatives should include the parametrization of security mechanisms (filtering rules, attack signatures, access control lists), and prevent vulnerable configurations (depending on their criticality) by taking into account known vulnerability descriptions. They should also consider the capabilities of providers and resources to comply with expected modifications.

The second pillar is centered on the elaboration of a framework with selection algorithms that exploit the extended orchestration language. The algorithms will enable to automatically determine the operations to be performed, depending on the current configuration and the resource (or set of resources)

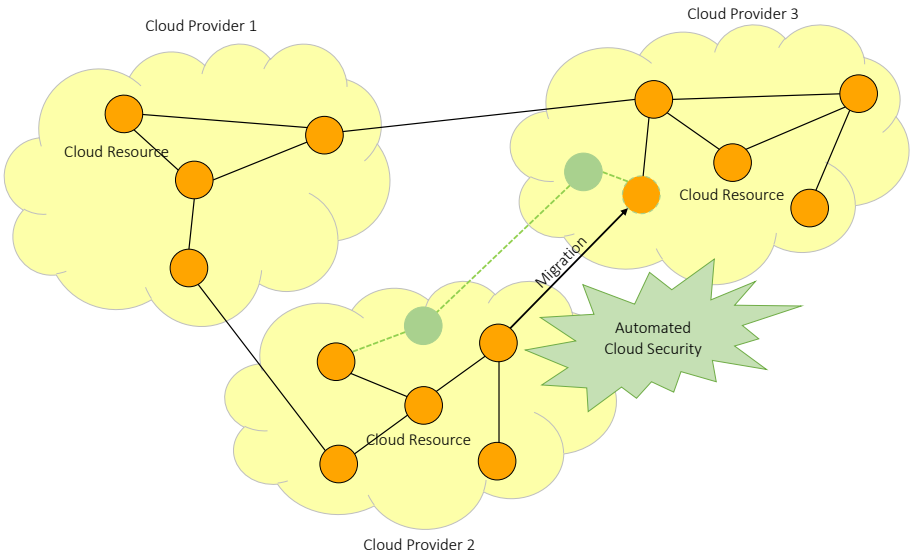

Fig. 1. Automated security enhancement during the migration of cloud resources

to be migrated. These operations may involve the resource itself or external resources that may come from the initial cloud provider (or initial infrastructure) or from the new cloud provider (or new infrastructure). Let us consider the scenario that is described in Figure 1. We can observe that the cloud composite service is composed of elementary resources (represented by orange nodes with continuous border), including one migration node, that are distributed over three different cloud providers (represented by yellow-coloured clouds). A resource from a cloud provider is migrated to a second cloud provider (on the right part of the figure). The migrating node is represented after migration by an orange node with a dotted border. It corresponds to an elementary resource of the cloud service, such as a web server or a virtualized network device. The migration impacts the configuration of the cloud service and may introduce new configuration vulnerabilities on the resource and on the service on which the resource is built, requiring to operate corrective or proactive operations.

The third pillar focuses on exploiting the complementarity of endogenous and exogenous mechanisms to support migration activities. In order to enforce security, we can operate on the migrated resource (new orange node with dotted border) by modifying its configuration or deploying new internal security controls. We can also rely on external resources to protect the new resource. This is represented by green nodes, and may be done from the initial and/or the new cloud providers. Let consider that the resource corresponds to a web server, and that the migration introduces a new vulnerability due to the contextual change induced by the cloud provider. In some cases, we can consider a security patch to be executed on the resource itself before the migration. In other cases, a patch may not be available to address the vulnerability, and will require the activation of security functions (such as a firewall instance with specific filtering rules).

IV. Preliminary Results

In order to automate the selection of the right security mechanism to be activated during the migration of a given cloud resource, we propose to exploit risk management algorithms. The objective is to dynamically adapt the exposure of the cloud resource with respect to the potentiality of security attacks, when changes are triggered by the resource migration. This adaptation relies on the selection of endogenous and exogenous security mechanisms that permit to protect the cloud resource. Let us consider a security attack a and a cloud resource r. The risk level $R(a,r)$ can typically be defined as the combination of the threat potentiality $P(a,r)$ related to the attack, the exposure of the cloud resource $E(a,r)$, and the consequence $C(a,r)$ of the attack on the cloud resource when this attack succeeds [19], as shown on Equation 1.

$$R(a,r) = P(a,r) * E(a,r) * C(a,r) \quad (1)$$

The activation or deactivation of security mechanisms permit to reduce or respectively increase the exposure $E(a,r)$. This therefore impacts the risk level $R(a,r)$ and permits its migration. For instance, the activation of an exogenous security mechanism s_{endo} corresponding to an intrusion detection system, provided as a virtualized network function, may reduce $E(a,r)$ by protecting the cloud resource against some attacks. It may also imply a cost, noted $cost(s_{endo})$, for using the cloud resource, such as an additional delay to access this resource. The automation permits to maintain the risk level $R(a,r)$ to an acceptable level through an exposure adaptation, while minimizing the costs induced by security mechanisms.

We are considering three use cases with respect to these automation algorithms. The first one, illustrated on Figure 2 corresponds to the restriction of a cloud resource during the migration. The figure showcases the normalized values over time for the threat potentiality, the resource exposure, the risk

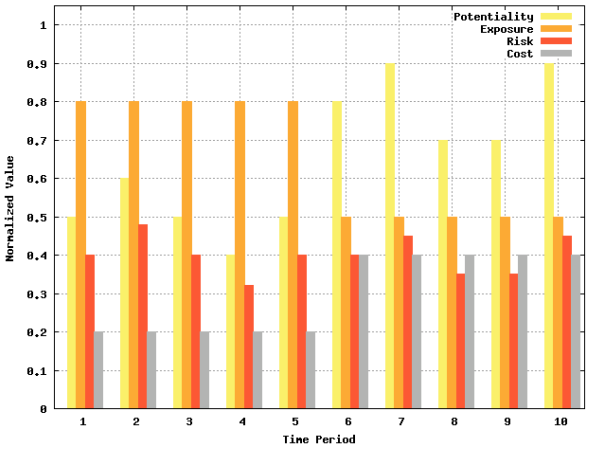

Fig. 2. Restriction example during a cloud resource migration

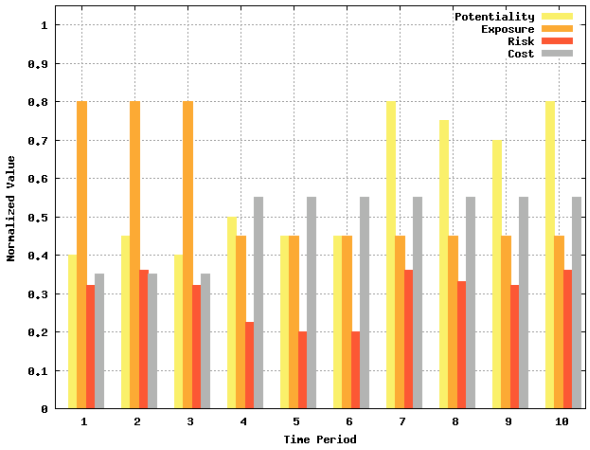

Fig. 3. Proactive restriction example during a cloud migration

level, and the cost over time. In these illustrative results, the threat potentiality is arbitrary chosen to characterize the use case, while the exposure, risk level and cost values are automatically calculated, considering pre-defined impacts and costs of individual security mechanisms. Let us consider a cloud resource migrating to an infrastructure with a higher threat potentiality at the time period 5, the automation algorithms enable the activation of security mechanisms in order to reduce the exposure of the resource and reduce the risk level. On Figure 2, the exposure is reduced from 0.8 to 0.5. This permits to keep the risk level below a given threshold, when the potentiality is increasing, but generates an additional cost of 0.2 due to the activation of a security mechanism. An alternative use case demonstrates a proactive restriction of the resource prior to its migration, as shown on Figure 3. This permits to guarantee that the risk level will stay under a value lower than a given threshold during the whole migration process. While the resource migration is effective at time period 7, a security mechanism is already activated early, at time period 4. As a consequence, the exposure is decreased to 0.45, before the potentiality increases to around 0.76 on average. The third use case is the relaxation of a cloud resource during the migration, as shown on Figure 4. The cloud resource migrates to an infrastructure that provides a lower threat potentiality (from 0.9 to 0.4). In that case, the automation algorithms try to minimize the protection cost (from 0.65 to 0.25), by deactivating some security mechanisms.

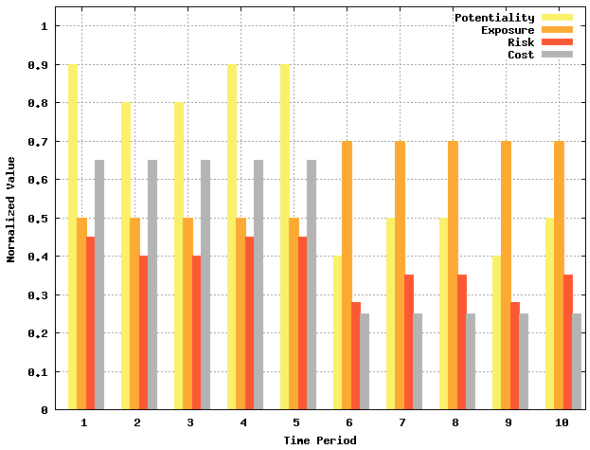

Fig. 4. Relaxation example during a cloud resource migration

V. Conclusions

The large-scale deployment of cloud services poses important security challenges. In particular, the migration of a cloud resource may generate configuration changes that introduce new vulnerabilities. This may compromise a whole cloud service built on top of this resource, and lead to important damages. Our proposed approach aims at automating security enhancement for cloud services, with a focus on issues related to resource migration. It considers exploiting service descriptions as an important knowledge source to drive security enhancement. The first pillar of this work consists in extending an orchestration language for specifying different orchestrated security levels and supporting security automation. The second pillar concerns the design of a framework with selection algorithms to determine the security mechanisms to be activated for protecting a whole cloud service during the migration of one or several of its resources. Finally, the third pillar is focused on the complementary of exogenous and endogenous security mechanisms. We have shown through illustrative examples (restriction, proactive restriction and relaxation use cases) to what extent the selection of exogenous and endogenous mechanisms could be supported by risk management algorithms. As future work, we are interested in formalizing the specification of extensions for the TOSCA language, as well as in developing a proof-of-concept prototype in order to evaluate the solution performance through experiments over a realistic environment.

References

[1] P. M. Mell and T. Grance, “SP 800-145. The NIST Definition of Cloud Computing,” Gaithersburg, MD, USA, Tech. Rep., 2011.

[2] M. Aiash, G. Mapp, and O. Gemikonakli, "Secure Live Virtual Machines Migration: Issues and Solutions," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, May 2014, pp. 160–165.

[3] D. Fernandes, L. Soares, J. Gomes, M. Freire, and P. Inácio, "Security issues in cloud environments - a survey," *Int. J. Inf. Secur.: Security in Cloud Computing*, p. 113–170, 04 2013.

[4] Y. Yamato, M. Muroi, K. Tanaka, and M. Uchimura, "Development of Template Management Technology for Easy Deployment of Virtual Resources on OpenStack," *Journal of Cloud Computing*, vol. 3, no. 1, p. 7, Jun. 2014. [Online]. Available: https://doi.org/10.1186/s13677-014-0007-3

[5] OASIS, "Topology and Orchestration Specification for Cloud Applications Version 1.0," p. 114, 2013.

[6] P. Lipton, D. Palma, M. Rutkowski, and D. A. Tamburri, "Tosca solves big problems in the cloud and beyond!" *IEEE Cloud Computing*, pp. 1–1, 2018.

[7] A. CloudFormation, "AWS CloudFormation - API Reference," p. 283.

[8] G. M. Tihfon, J. Kim, and K. J. Kim, "A new virtualized environment for application deployment based on docker and aws," in *Information Science and Applications (ICISA) 2016*, K. J. Kim and N. Joukov, Eds. Singapore: Springer Singapore, 2016, pp. 1339–1349.

[9] A. Esposito, B. Di Martino, and G. Cretella, "Defining Cloud Services Workflow: a Comparison between TOSCA and OpenStack Hot," Jul. 2015.

[10] M. Compastie, R. Badonnel, O. Festor, and R. He, "A TOSCA-Oriented Software-Defined Security Approach for Unikernel-Based Protected Clouds," Jun. 2019, pp. 151–159.

[11] M. Barrere, R. Badonnel, and O. Festor, "A SAT-based Autonomous Strategy for Security Vulnerability Management," May 2014, pp. 1–9.

[12] M. Anisetti, C. A. Ardagna, and E. Damiani, "Security certification of composite services: A test-based approach," in *Proceedings of the IEEE 20th International Conference on Web Services*, 2013, pp. 475–482.

[13] M. Anisetti, C. Ardagna, E. Damiani, and F. Gaudenzi, "A Semi-Automatic and Trustworthy Scheme for Continuous Cloud Service Certification," *IEEE Transactions on Services Computing*, Jan. 2017.

[14] N. Chandrakala and D. B. Rao, "Migration of Virtual Machines to Improve the Security in Cloud Computing," *International Journal of Electrical and Computer Engineering*, vol. 8, pp. 210–219, 02 2018.

[15] N. Schnepf, R. Badonnel, A. Lahmadi, and S. Merz, "Automated verification of security chains in software-defined networks with synaptic," Jul. 2017, pp. 1–9.

[16] M. Pattaranantakul, R. He, Z. Zhang, A. Meddahi, and P. Wang, "Leveraging Network Functions Virtualization Orchestrators to Achieve Software-Defined Access Control in the Clouds," *IEEE Transactions on Dependable and Secure Computing*, Dec. 2018.

[17] U. M. Ismail, S. Islam, and H. Mouratidis, "Cloud Security Audit for Migration and Continuous Monitoring," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1081–1087.

[18] K. W. Ullah, A. S. Ahmed, and J. Ylitalo, "Towards Building an Automated Security Compliance Tool for the Cloud," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Jul. 2013, pp. 1587–1593, iSSN: 2324-9013.

[19] O. Dabbebi, R. Badonnel, and O. Festor, "An Online Risk Management Strategy for VoIP Enterprise Infrastructures," *Journal of Network and Systems Management*, vol. 23, no. 1, pp. 137–162, 2015. [Online]. Available: https://doi.org/10.1007/s10922-013-9282-4