An Approach for Security Evaluation and Analysis in Cloud Computing

Thibaut Probst, Eric Alata, Mohamed Kaâniche, Vincent Nicomette, Yves Deswarte

An Approach for Security Evaluation and Analysis in Cloud Computing

T. Probst[1,2], E. Alata[1,3], M. Kaâniche[1,4], V. Nicomette[1,3], Y. Deswarte[1,4]
[1]CNRS, LAAS, 7 Avenue du colonel Roche, F-31400 Toulouse, France
[2]Univ de Toulouse, INP de Toulouse, LAAS F-31400 Toulouse, France
[3]Univ de Toulouse, INSA de Toulouse, LAAS F-31400 Toulouse, France
[4]Univ de Toulouse, LAAS, LAAS F-31400 Toulouse, France
{probst,ealata,kaaniche,nicomett,deswarte}@laas.fr

***Abstract*—This paper describes a novel approach for security evaluation and analysis in cloud computing environments. The objective is to provide an automated way to evaluate the efficiency of security mechanisms aiming at protecting the cloud computing infrastructures and applications. In particular, we focus on access controls and intrusion detection/prevention systems. We leverage cloud benefits to optimize the audit and assessment processes. The proposed approach is currently under implementation on our cloud platform.**

I. Introduction

By offering various service and deployment models [1], cloud computing provides easy ways to host and manage infrastructures and applications, while reducing deployment and operation costs. However, the rapid development of cloud computing over the last few years has raised new security concerns [2], [3]. Enforcing the security and dependability of cloud computing infrastructures is necessary to allow their use for the deployment of critical applications. Different levels of protection are needed to implement security policies, as done in traditional environments. Nevertheless, there are specific characteristics and challenges that need to be taken into account carefully in cloud computing environments. Among others, we can cite: 1) the co-residence of several clients on the same physical infrastructure; 2) the mix of different technologies like virtualization, new network architectures, Web applications and services; 3) the co-existence of different levels of security controls on the client side and on the cloud provider side; and 4) the emergence of new attacks involving cloud infrastructures. Thus, usual security mechanisms must be adapted so they can be efficient in such a context. Our purpose it to assess the efficiency of these mechanisms.

Except for recommandations such as the Cloud Security Alliance guidance on security assessments [4], very few approaches for cloud security evaluation have been developed so far. We can cite Bleikertz's work [5], addressing security audits in public cloud infrastructures. His approach allows to generate attack graphs from network accessibility graphs and vulnerability scans. However, it only addresses network-based attacks and the attack scenarios found are never executed. Furthermore, no in-line firewall or Intrusion Detection/Prevention Systems (IDS/IPS) evaluation is performed.

In this paper, we propose an approach to efficiently conduct automated security evaluations and analysis of Infrastructure as a Service cloud computing environments. The ultimate goal is to give the client a detailed picture of the risks he takes by using the cloud, and the provider a good insight of what sort of threats a client may represent. In particular, we are interested in two challenges regarding cloud computing security: access controls (including network and user access filtering) and intrusion detection and prevention. To evaluate the efficiency of these security measures, we follow a two-phase process: 1) access control analysis to evaluate the performance of network and user access filtering, and get the accessibilities; 2) IDS/IPS evaluation by executing relevant attack scenarios that take into account the accessibilities found.

Further details about the proposed approach are presented in the remainder of this paper.

II. Proposed approach

Various security mechanisms are deployed in the cloud to implement security policies: firewalls, IDS/IPS, Identity and Access Management (IAM) tools. Our objective is to verify that they are correctly deployed and configured to fit the security requirements of the client and of the provider.

Our methodology and its corresponding steps are illustrated in Fig. 1. It is based on the elaboration and execution of attack scenarios targeting the hosts involved in the client's virtual infrastructure. As these attacks may compromise hosts and, as a consequence, could interfere with the client's business, we chose to clone (step a) this infrastructure (virtual datacenters: networks, firewalls, machines and applications) and perform attacks on this clone. Furthermore, cloning the client's infrastructure allows us to purposely inject vulnerabilities on the different hosts, to set up and perform complex attack scenarios, which is particularly useful when one needs to assess the efficiency of IDS/IPS in the presence of some specific vulnerabilities and attacks. We take into account the presence of other potentially malicious concurrent clients that we represent through other infrastructures we control.

To be automated, our approach takes advantage of cloud computing embedded technologies to run audit operations (cloning infrastructures, executing virtual machines, deploying applications).

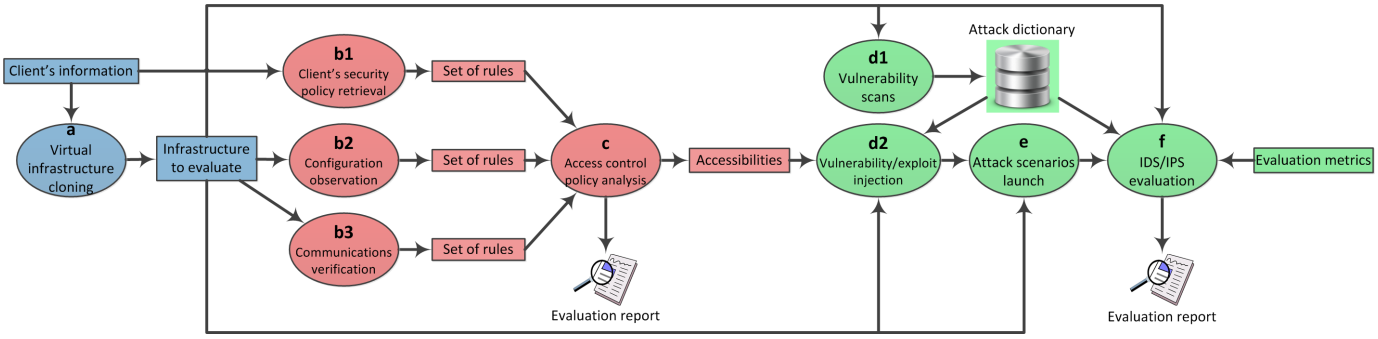

Fig. 1. Overall evaluation and analysis process

A. Analysis of access control policy

The list of authorized communications (so-called accessibilities) inside the infrastructure to be assessed, is identified using three ways:

1) By retrieving statically the client's security policy, written in a formal or informal specification document (step b1).
2) By extracting information from the cloned cloud component's configuration (networks, hypervisor-based firewalls, virtual firewalls, IAM tools) (step b2).
3) By performing experiments: sending traffic such as network sweeps in order to verify the effective possible communications (step b3).

These accessibilities are translated into a set of handy rules. We chose the Prolog logic programming language because it is well adapted to express predicates and compute some logic to deduce rules characterizing the accessibilities, such as:

```
communication(source, sproto, sport, destination, dproto, dport).
```

This rule specifies the kind of traffic a source object (IP address, network, security group...) can send to a destination object. By processing these rules, one can identify inconsistencies in the implementation of the policy (normally the three set of rules should be equivalent), and deduce the accessibility matrix (taking the second or the third set of rules). The confrontation of the outcomes highlighting the inconsistencies produces an access control policy evaluation as a first result (step c).

B. Evaluation of Intrusion Detection and Prevention Systems

To compose attack scenarios, we need to use a simple attack taxonomy based on the attack vector. For this purpose, we follow a dimension-based classification [6], using the attack vector as the dimension. To be as exhaustive as possible in the evaluation of the IDS/IPS, we plan to execute every possible attack category on behalf of every possible attacker (insiders and outsiders) and towards every possible target. The actually running virtual machines and their images are first scanned to find potential vulnerabilities (step d1). Additional exploitable vulnerabilities that are associated to the accessibilities found (step d2) will be injected on purpose to check the IDS/IPS reaction under some specific attack campaigns for which alarms are expected to be raised. A dictionary containing the description of attacks (exploit, vulnerability, environment parameters, and expected results) for each class of our taxonomy is used to perform the injection of these vulnerabilities and their matching exploits. The preconditions, postconditions and objectives are deduced from the attack scenarios built and launched on the fly (step e). The output of the Security Information and Event Management (SIEM), which aggregates and correlates the IDS/IPS probes, along with the state of the targets, will be used to give us the verdict to know whether the attacks have been detected/prevented or not, according to the expected results from the aforementioned dictionary (step f). Finally, quantitative metrics will be derived to assess false negative and false positive detection rates for each attack class, and also to identify optimal configurations of the IDS/IPS in the cloud infrastructure.

III. Conclusion

This paper presents the principles of an approach we are developing to automatically conduct security evaluations and analysis in cloud computing infrastructures. Our approach is aimed at optimizing the overall process while providing accurate assessments of the major security aspects of the cloud. The proposed approach is currently investigated and implemented using a VMware vCloud Suite platform including various security mechanisms.

Acknowledgment

This research is supported by the French project Investissements d'Avenir Secured Virtual Cloud (SVC).

References

[1] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0", 2011.
[2] M. Jensen et al., "On Technical Security Issues in Cloud Computing", in *IEEE International Conference on Cloud Computing*, Bangalore, India, 2009, pp. 109-116.
[3] I. Studnia et al., "Survey of Security Problems in Cloud Computing Virtual Machines", in *Computer and Electronics Security Applications Rendez-vous*, Rennes, France, 2012, pp. 61-74.
[4] Cloud Security Alliance, "SecaaS Implementation Guidance: Security Assessments", 2012.
[5] S. Bleikertz, "Automated Security Analysis of Infrastructure Clouds", M.S. thesis, Department of Informatics and Mathmatical Modelling, Technical University of Denmark, and Department of Telematics, Norwegian University of Science and Technology, 2010.
[6] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks", in *Computers and Security*, 2005, 24 pp. 31-43.