Elastic SIEM: Elastic Detector integrated with OSSIM

Pasquale Puzio
SecludIT and EURECOM
Nice, France
pasquale@secludit.com

Sergio Loureiro
SecludIT
Nice, France
sergio@secludit.com

***Abstract*—This paper introduces a new approach to overcome new threats and attacks which arise with the adoption of cloud computing. Traditional security solutions are not suitable for this new elastic and dynamic scenario. This paper shows a solution to protect cloud users against side-channel attacks by taking advantage of the integration of OSSIM with Elastic Detector.**

***Index Terms*—cloud computing; security; SIEM; elastic security; IaaS; cloud infrastructures;**

I. Introduction

Cloud computing adoption is rising fast [6]. Flexibility, pay-per-use and available resources on-demand with the promise of lower ownership costs are a very attractive value proposition. On the other hand, Infrastructure as a Service (IaaS) providers, such as Amazon Web Services (AWS) [5], are being asked for flexible cloud offerings while needing to answer to the security demand of their customers. Existing security solutions are not only time consuming for IT administrators, requiring advanced technical skills, but also were designed to implement static security perimeters for static infrastructures. At the time of elastic and programmable cloud IT infrastructure, a completely new approach to security is needed.

II. Problem statement: IaaS Security

Cloud Computing is transforming IT infrastructures and the way we handle infrastructure security. There is thus a set of underlying problems that need to be addressed:

- **Lack of visibility.** Cloud infrastructures is more dynamic than classical infrastructures, since servers, network and storage are launched for temporary usage and automatically. This makes it difcult to keep track of the availability of each server, network and storage as well as their security status.
- **Security degradation over time.** Modications to a cloud infrastructure environment, such as temporary access, starting new services, tests and starting new machines, generally reduce the level of protection of a system over time, which increases the risk of external and internal attacks.
- **Manual conguration errors.** IT administrators make mistakes, such as opening wrong firewall ports or giving access to unauthorized users. Due to the complexity and dynamic nature of cloud computing infrastructures, manually handling security in such environments raises probability of errors.
- **New attack vectors and threats.** The capabilities and the flexibility of cloud infrastructures brings as well new threats [1] as the nefarious use of resources by malicious insiders or threats related to the virtualization and APIs technologies [2], [3].

III. Solution: Elastic Detector

Benefiting from the advantages of cloud infrastructures while reducing security related risks is possible with our new *elastic* approach. The characteristics of our approach are:

- **Full Automation.** Keeping operating costs under control means being able to automate the whole or parts of their cloud computing security management by eliminating the majority of manual set up, security monitoring, corrective actions and implementation.
- **Agentless.** IT administrators can no longer spend time deploying and maintaining agents in every machine on a dynamic infrastructure. Through the virtualization layer, and using APIs such as VMware vShield or Amazon EC2 security groups, security solutions can analyze resource information and enforce security with no agents.
- **Comprehensive Security Assessment.** The traditional layered approach, where each security component takes care of a specific layer (such as the network, storage, compute, etc.) is not sufficient to handle the security threats which can arise in cloud infrastructures. In order to overcome the fragmentation of security components and automate their administration a more global and comprehensive approach is needed, through which it is possible to correlate security relevant events coming from different sources at different layers.
- **No Lock-in.** The ability to use different IaaS offerings for reliability, flexibility and being able to have full visibility through the same dashboards and metrics is important for CIOs and CSOs.

A. Elastic SIEM: Elastic Detector integrated with OSSIM

Elastic Detector brings an important contribution to the work of a SIEM. Without using Elastic Detector, a system administrator would need to reconfigure his own SIEM system every time there is a change (e.g. a new virtual machine

starts running) in the cloud infrastructure. Configuring a SIEM system is a difficult task which requires the experience and skills of a security expert. Therefore, in highly dynamic infrastructures, reconfiguring the SIEM system every time there is a change in the cloud infrastructure is not practical. A possible alternative could be to install agents on each virtual machine running in the cloud but this approach has various drawbacks affecting especially performance. Elastic Detector aggregates all the data retrieved by performing auto-checks in the cloud network, log any security-relevant activity and forward it to the SIEM system, where it can be processed together with data collected by other sources. Once the SIEM system has collected the information describing the state of the system, it can proceed to the correlation phase, where data collected by different sources are carefully analyzed in order to detect abnormal behaviors and, if necessary, take the proper countermeasures. In this paper we present the integration of Elastic Detector with OSSIM [4], an open-source and widely adopted system for SIEM.

B. Case study

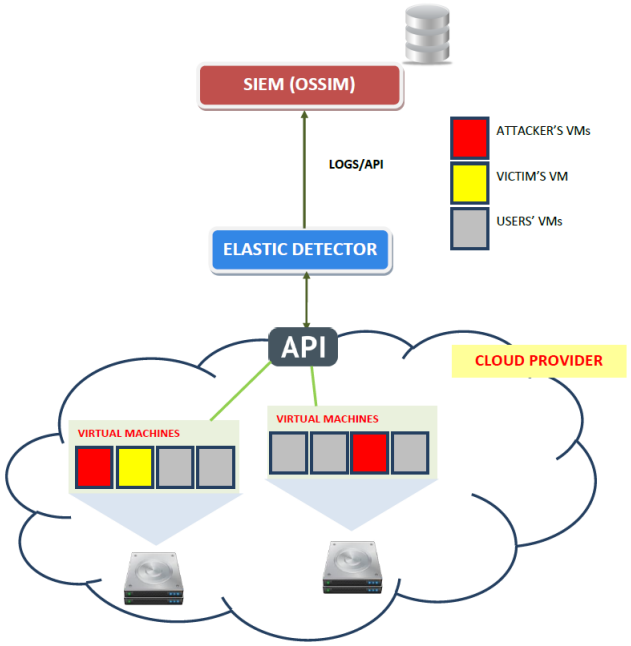

Fig. 1. Example of integration between Elastic Detector and OSSIM for Side-Channel Attacks Detection

The goal is to build a solution for cloud providers in order to supervise the security of their cloud infrastructures. In this section we show our proposal for adopting OSSIM in cloud infrastructures. In the scenario depicted in Fig. 1, Elastic Detector cooperates with the SIEM system by retrieving security relevant information and events concerning the whole data center. At the SIEM, these information can thus be aggregated and correlated in order to detect threats and attacks affecting cloud users. One of the main causes for these new threats is multi-tenancy [8]. Cloud Computing widespread new scenarios in which users data share the same physical host. Because of co-residency, an attacker has a new way to access the victims data: he can leverage the co-residency factor and infer victims data by observing the activity of a shared component (e.g. the processor cache) on the physical host. This new class of attacks is called *side-channel attacks* [7]. Our proposed solution is aimed to help IaaS providers to detect such attacks and protect users' data automatically and without affecting the way the infrastructure is managed. Indeed, Elastic Detector is able to automatically detect changes in the cloud infrastructure and its configuration. When a relevant event (e.g. a new VM is launched) occurs, Elastic Detector can seamlessly for the user communicate with the SIEM system and deliver the required information. In the context of side-channel attacks, the SIEM system can effectively detect a potential malicious activity by noticing that a user is launching many VMs on different physical hosts. Elastic Detector's approach supports SIEM systems by providing additional security relevant information such as the result of automated audits. These information, combined to the contribution of other security components, improve the detection capabilities of a SIEM system.

Pasquale Puzio is a CIFRE PhD Student at SecludIT and EURECOM, under the supervision of Sergio Loureiro and Refik Molva. He got a Master's Degree in Computer Science from University of Bologna and a Master's Degree in Ubiquitous Computing from University of Nice-Sophia Antipolis. The topic of his PhD thesis is *Data Storage Security in Cloud Computing* but his research interests include also infrastructure security in cloud computing.

Sergio Loureiro CEO and Co-Founder of SecludIT, has worked in network security for more than 15 years. He has occupied top management positions in 2 startups where he was responsible for email security products and services, and security gateways. Sergio holds a Ph.D. in computer science from the ENST Paris and MSc and BSc degrees from the University of Porto (Portugal). He is the holder of 3 patents.

REFERENCES

[1] *Cloud Security Alliance Top Threats* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[2] Marco Balduzzi, Jonas Zaddach, Davide Balzarotti, Engin Kirda, Sergio Loureiro *A Security Analysis of Amazons Elastic Compute Cloud Service* http://secludit.com/wp-content/uploads/2012/09/securecloud.pdf
[3] *There's a Hole in 1,951 Amazon S3 Buckets* https://community.rapid7.com/community/infosec/blog/2013/02/14/1951-open-s3-buckets
[4] *OSSIM* http://communities.alienvault.com/
[5] *Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta* http://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2—beta/
[6] *Gartner Top 10 Strategic Technology Trends for 2013* http://apmdigest.com/gartner-top-10-strategic-technology-trends-for-2013-big-data-cloud-analytics-and-mobile
[7] Y Zhang, A Juels, MK Reiter, T Ristenpart *Cross-VM Side Channels and Their Use to Extract Private Keys* https://mexico.rsa.com/rsalabs/presentations/cross-vm-side-channels.pdf
[8] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds* http://www.cs.cornell.edu/courses/cs6460/2011sp/papers/cloudsec-ccs09.pdf