How to Secure Application-Level Firewalls in IaaS Clouds

Anna Giannakou, Inria, IRISA
Louis Rilling, DGA
Christine Morin, Inria, IRISA
Jean-Louis Pazat, INSA, IRISA

1. Introduction

Cloud environments have emerged as a durable solution for outsourcing information systems. Some of the key IaaS clouds features are multi-tenancy, elasticity and on demand availability. Tenants can create, destroy or reconfigure virtual resources with unprecedented ease. However, the same characteristics that make cloud environments agile and dynamic, also affect the ability of a security monitoring framework to successfully detect attacks in outsourced information systems [3] and sometimes introduce new security vulnerabilities. Large scale security monitoring frameworks include various components (firewalls, IDSs, log collectors etc.) that perform different functionalities and are located in different areas or even outside the virtual infrastructure. Consequently, a successful cloud-tailored security monitoring infrastructure should be able to adapt its components based on changes in the infrastructure with little to no human intervention.

2. Problem Addressed

In opposition to a typical host- or network-level firewall which filters network traffic based on a list of rules that use IP addresses and ports, application-level firewalls operate based on an access policy that is defined from a white list of processes that are allowed to make connections. This fine-grained level of filtering is achievable because application-level firewalls have a complete overview of the host in which they are running. Unfortunately, increasing visibility of the host system comes at the cost of weaker isolation between the firewall and vulnerable applications. This increases the probability of a successful attack that disables the firewall (i.e removing hooks from packet filtering functions).

3. Approach

A solution to this impediment is leveraging virtual machine introspection for pulling the application-level firewall outside of the virtual machine it is monitoring. Deploying the firewall in a completely different protection domain introduces a high-confidence barrier between the firewall and the attacker's malicious code.

Virtual machine introspection is a mechanism that allows, through memory mapping, indirect inspection of and control over the current state of a virtual machine from software running outside of the virtual machine. The approach is based on building higher-level semantics that can be accessed by a monitoring application (data structures, files) from the mapped memory pages. The indirection offered has been the base for various security applications that leverage the associated isolation properties [1] [2].

4. Two-level Firewall Architecture

We present a secure, introspection-based, two-level, application-level firewall. It is part of our self-adaptable security monitoring framework for IaaS clouds [4].

The proposed architecture consists of two different components that operate at distinct infrastructure levels: first an external firewall responsible for filtering network traffic between the outside world and the cloud infrastructure, and second a virtual switch-level firewall that filters traffic in the virtual switch of each physical host. Both components, executed outside the untrusted virtual machine, become application-level firewalls by using virtual machine introspection. The rulesets on both components will be automatically reconfigured upon the occurrence of changes in the cloud infrastructure (e.g virtual machine migration, creation or deletion)

We are currently conducting a thorough performance evaluation of our approach with executing various migration scenarios. We plan to examine the ability of our architecture to filter out packets created by different attack classes, both external and internal to the cloud, while allowing connections from white-listed processes to pass unimpeded.

5. Future Work

We plan to address cost minimisation by combining the security monitoring of tenants and provider infrastructure. Next steps include giving partial control of the monitoring framework to tenants and expanding our architecture by including other types of devices such as log collectors and aggregators. We also intend to address scalability issues.

References

[1] T. Garfinkel et al. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *Proc. NDSS*, 2003.

[2] B. D. Payne et al. Secure and Flexible Monitoring of Virtual Machines. In *Proc. ACSAC*, 2007.

[3] N. Shirazi et al. Assessing the impact of intra-cloud live migration on anomaly detection. In *Proc. CloudNet*, 2014.

[4] A. Giannakou et al. Towards Self Adaptable Security Monitoring in IaaS Clouds. In *Proc. CC-GRID* , 2015.