Institute of IT-Security and Security Law

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

Master Thesis

VMI-based Cloud Monitoring Framework

Published: 4 November, 2015
Advisor: Benjamin Taubmann
Email: bt@sec.uni-passau.de

Prof. Dr. Hans P. Reiser
Security in Information Systems
University of Passau

Context

Virtual machines (VM) in infrastructure-as-a-service based cloud environments are an attractive target for attackers as they may contain confidential information or provide resources such as network bandwidth or storage.

For cloud providers this is a problem as one infected machine might infect more machines or even the cloud infrastructure which might cause bad reputation. Thus, cloud providers are interested to detect infected machines before they attack other machines.

Virtual machine introspections offers means to monitor the behavior of virtual machines at a very low level. This data has the advantage that it can not be manipulated by malware. The disadvantage of this data is that it requires complex interpretation to extract useful information.

Topic

The monitoring of virtual machines produces a lot of low level information that is often not manageable and hard to interpret for human operators. Thus, this data needs to be collected, aggregated and visualized in order to extract useful information and possible suspicious behavior.

The main task of this thesis is to create a framework that extracts different kinds of information of a running virtual machine and store them into a database. This includes:

- System load
- Network load
- Process list
- System call traces
- etc.

Afterwards, the contents of this database shall be displayed graphically in a dynamic website (e.g. with D3 and Django) or a monitoring system like Nagios.

Keywords

Cloud, Visualization, Virtualization, Web Site, Database,