Exploring Security Support for Cloud-based Applications

Hai Nguyen
Dept. of Computer Science

8/22/2018 at 10:00 am
CoRE B (305)

Abstract

Users are increasingly adopting cloud services for various purposes such as storing and processing data or using cloud-based software. However, this computing model poses cloud-specific security challenges to these cloud-based applications.

This dissertation describes novel solutions to three security problems of cloud-based applications. First, the introduction of hardware-based implementations of isolated execution such as Intel SGX makes it challenging to enforce security compliance of cloud applications. It is desirable to have a mechanism that allows cloud providers to inspect the code and data of cloud applications while still preserves the integrity and confidentiality offered by Intel SGX. Second, cloud services have increasingly become the target of ransomware attacks. However, current ransomware detection techniques are prone to false positives and some of them are unable to distinguish ransomware from benign programs that exhibit ransomware-like behaviors. Third, in todays cloud platforms, clients do not have much power and flexibility to deploy security services. Clients often rely heavily on cloud providers for deployment of security measures such as intrusion detection systems (IDSs) or have to manually install and configure software stack with security tools.

This dissertation makes the following contributions. First, it implements EnGarde, an enclave inspection library that preserves the security and privacy benefits offered by Intel SGX and allows the cloud provider to verify the client's SGX-based enclave against predefined policies mutually agreed by the cloud provider and the client. Second, it builds HRD, a system that can detect ransomware in cloud-based environments with low false positives. HRD uses Hardware Performance Counters (HPCs) and machine learning to build classifiers that effectively detect ransomware with high accuracy. Third, it demonstrates the utility of a new cloud computing model where the client can make use of cloud apps, implemented as virtual machines (VMs), to implement security measures.

Defense Committee: Prof. Vinod Ganapathy (Chair), Prof. Thu Nguyen, Prof. Abhishek Bhattacharjee, and Prof. Trent Jaeger (Pennsylvania State University)