Chapter 34

TVGuarder: A Trace-Enable Virtualization Protection Framework Against Insider Threats for IaaS Environments

Li Lin
Beijing University of Technology, China

Shuang Li
Beijing University of Technology, China

Bo Li
Beihang University, China

Jing Zhan
Beijing University of Technology, China

Yong Zhao
Beijing University of Technology, China

ABSTRACT

Cloud computing has a most vulnerable security concerns as virtualization. This paper presents a Trace-enable Virtualization protection framework named TVGuarder, which protects IaaS user's important data from being illegally accessed or maliciously damaged by insider attacks. A threat model is established to characterize cloud-oriented insider attacks and countermeasures are proposed in TVGuarder. First, LSM hooks in host OS kernel are leveraged to enforce that VM images could only be accessed by host virtualization service. Second, a trusted loading mechanism is proposed to prevent tampered or disguised virtualization process from being executed in Host OS. Third, a log-based back tracing mechanism is designed to record full call trace of VM operations and guarantee that only legitimate VM operations are allowed. TVGuarder has been implemented in Openstack platform and several comprehensive experiments are conducted. Experimental results show that TVGuarder can identify several important insider attacks and protect virtual machine images with only a small performance degradation.

DOI: 10.4018/978-1-5225-5634-3.ch034

1. INTRODUCTION

Recent years witness the rapid development of cloud computing. In cloud environments, resources are virtualized and provided as various kinds of services over the Internet. Based on the service level, cloud services could be classified into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Among the three, IaaS is the most popular one which leverages virtualization technology to multiplex the underlying hardware, encapsulates applications and operating systems (OS), and provides users with secure and dedicated computing environments. Many IaaS cloud platforms such as Amazon EC2, Microsoft Azure and Aliyun have emerged and provided great flexibility and convenience to the cloud users. However, with the prevalence of cloud computing, new security challenges arise. The security of customers' sensitive data become a key concern if being put into cloud environments (Tang, Cui, Li, Ren, Liu, & Buyya, 2016).

Though Cloud Service Providers (CSP) usually make privacy commitments to the cloud users, users' data is still at risk of leakage or damage (Lin, Liu, Hu, & Ni, 2016). Recent research works focus on protecting users' data or virtual machines from untrustworthy CSPs. Ali et al. (2015) proposed a cloud-based secure data storage and sharing methodology which leverages third-party to help protect user data. However, it is not practical in real IaaS cloud environments. The cloud system performance will suffer a lot since data needs to be transferred from third-party to cloud platforms when doing computation. Murugaiyan et al. (2014) presented a generic privacy preventing framework to protect cloud digital data from unauthorized user attackers. Kazim et al. (2013) and Pandey et al. (2014) focused on the risk that virtual images of cloud users could be leaked after being uploaded to cloud environments, and used encryption-based schemes to encrypt the virtual images before uploaded. Virtual images will be decrypted before use but after leaving cloud platforms. Though encryption and decryption can ensure the secrecy and privacy of virtual images, it will also consume lots of CPU cycles and greatly degrade system performance. Tan et al. (2012), Xia et al. (2013) and Miu (2015) proposed leverages nested virtualization to monitor the behavior of CSPs and protect the security of users' virtual machines from being tampered by malicious CSPs. However, this approach requires distinguishing VMM-level operations from guest-level operations and needs to do a large amount of patch work on current implementation of cloud platforms, which limits its usability.

The above research works hold a basic assumption that CSPs are untrustworthy, but the reality is that CSPs has no motive to deliberately leak users' data. On the other hand, the real enemy that threaten the security of cloud users most is insider attack. According to the report from Cloud Security Alliance (2010), malicious insider attack is listed as one of the most important classes of cloud-specific threats in 2016, and another important risk is misoperation of cloud operators. However, the detection and prevention of insider attacks is a non-trivial task. First, the insiders such as cloud operators usually have administrator privileges and could arbitrarily access and manipulate the data of cloud users. Second, even if we restrict the privileges of insiders, we can still not guarantee that these privileges are not abused. For example, a malicious administrator could directly access the images of a user's virtual machine on the compute nodes without being known by the user who owns this virtual machine. Third and last, it is hard to trace the behaviors of malicious insiders since they could evade detection by deleting system logs or disguising as normal users. The practical need suggests the design and development of new security techniques to protect the data of cloud users from misoperations and malicious insider attacks.

To address the above issues, this paper present a novel framework, named TVGuarder, for protecting cloud users' data from being illegally accessed or maliciously damaged by insider attacks. And the