Journal of Network and Computer Applications 77 (2017) 18–47

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Intrusion detection techniques in cloud environment: A survey

Preeti Mishra[a], Emmanuel S. Pilli[a,*], Vijay Varadharajan[b], Udaya Tupakula[b]

[a] Department of Computer Science and Engineering, Malaviya National Institute of Technology Jaipur, India
[b] Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, Australia

ARTICLE INFO

Keywords:
Intrusion detection
Cloud security
Virtual machine introspection
Hypervisor introspection
Cloud attacks

ABSTRACT

Security is of paramount importance in this new era of on-demand Cloud Computing. Researchers have provided a survey on several intrusion detection techniques for detecting intrusions in the cloud computing environment. Most of them provide a discussion over traditional misuse and anomaly detection techniques. Virtual Machine Introspection (VMI) techniques are very helpful in detecting various stealth attacks targeting user-level and kernel-level processes running in virtual machines (VMs) by placing the analyzing component outside the VM generally at hypervisor. Hypervisor Introspection (HVI) techniques ensure the hypervisor security and prevent a compromised hypervisor to launch further attacks on VMs running over it. Introspection techniques introspect the hypervisor by using hardware-assisted virtualization-enabled technologies. The main focus of our paper is to provide an exhaustive literature survey of various Intrusion Detection techniques proposed for cloud environment with an analysis of their attack detection capability. We propose a threat model and attack taxonomy in cloud environment to elucidate the vulnerabilities in cloud. Our taxonomy of IDS techniques represent the state of the art classification and provides a detailed study of techniques with their distinctive features. We have provided a deep insight into Virtual Machine Introspection (VMI) and Hypervisor Introspection (HVI) based techniques in the survey. Specific research challenges are identified to give future direction to researchers. We hope that our work will enable researchers to launch and dive deep into intrusion detection approaches in a cloud environment.

1. Introduction

Hacking incidents are increasing day by day as technology evolves. Companies are changing the way they operate. Security issues in such a complex technological environment are posing significant challenges. Attacks are reported by cloud providers and users regularly. For instance, the French research outfit VUPEN Security (Mimiso, 2012) discovered the Virtual Machine Escape attack. The exploit targets a vulnerability that affects the way Intel processors implement error handling in the AMD SYSRET instruction. In Jan 2013, European Network and Information Security Agency (ENISA) reported (Dekker et al., 2013) that Dropbox was attacked by Distributed Denial of Service (DDoS) attacks and suffered a substantial loss of service for more than 15 hours affecting all users across the globe. DDoS botnets attacks also happened against the Amazon Cloud. Security researchers (Dee, 2014) have found the exploit on the Amazon Cloud platform through the ElasticSearch distributed search engine tool. Hackers attacked Amazon EC2 virtual machines using cve-2014–3120 exploit in ElasticSearch ver. 1.1 x. Researchers have also found that many enterprises are still using these vulnerable versions. According to Symantec (2015), 494 vulnerabilities and two zero-day vulnerabilities were disclosed during the month of January in 2015. W32. Ramnit! html was the most common malware that had been blocked. Verizon (2015) reported 55% incidents were insider abuses/attacks this year. In case of web applications attacks, stolen credentials accounted for 50.7%, backdoors were 40.5%, SQL Injection were 19%, brute force were 6.4%, and cross site scripting (XSS) attacks were some 6.3%. Cisco (2015) has reported that malware developers are using web browser add-ons as a medium for distributing malware and unwanted applications. They stated that 56% of all OpenSSL versions were due to older versions leading to OpenSSL attacks.

In the last few years, research has been carried out to tackle such security problems. The importance of well-organized architecture and security roles have become even greater with the popularity of Cloud Computing. Cloud Security Alliance (CSA) (Smith, 2012) provides best practice in cloud security such as security as a service model for cloud environment. Various researchers working in the field of cloud security have proposed intrusion detection systems (IDS) as a defensive approach. An IDS is a security tool that captures and monitors the network traffic and/or system logs, and scans the system/network for

* Corresponding author.
E-mail address: espilli.cse@mnit.ac.in (E.S. Pilli).

http://dx.doi.org/10.1016/j.jnca.2016.10.015
Received 4 April 2016; Received in revised form 11 September 2016; Accepted 18 October 2016
Available online 20 October 2016

suspicious activities. It further alerts the system or cloud administrator about the attacks. There are different types of IDS based on the location where the IDS is deployed, e.g. Host-based IDS, Network-based IDS and Hypervisor-based IDS. Host-based intrusion detection system (HIDS) monitors individual hosts (physical/virtual). It sends alerts to the user if it detects suspicious activities such as modification or deletion of system files, unwanted sequence of system calls or unwanted configuration changes at virtual machine (VM) or in other cloud regions. Network-based intrusion detection system (NIDS) is usually placed at network points such as gateway or routers to check for anomalies in network traffic. Hypervisor based IDS is deployed at the hypervisor (Virtual Machine Monitor (VMM)) or privileged VM and is capable of capturing the state information of all VMs running on top of the hypervisor. It can maintain and enforce different security policies for each VM, based on its requirements.

Different intrusion detection techniques used in a cloud environment include misuse detection, anomaly detection, virtual machine introspection (VMI), hypervisor introspection (HVI) and a combination of hybrid techniques. Misuse detection techniques maintain rules for known attack signatures. These rules can be derived either by using the knowledge based systems which contain database of known attacks signatures or by using machine learning algorithms that are used in the determination of behavioral profiles of the users based on known suspicious activities (Barbara and Jajodia, 2002). Anomaly detection systems detect anomalies based on the expected behavior of the system. Any deviation from the expected behavior is signaled as anomalous (Garcia-Teodoro et al., 2009).

Another well known technique is that of VMI. The basic principle behind the VMI technique is that it performs introspection of programs running in a VM to determine any malicious program change or execution of some abnormal or malicious code (Hebbal et al., 2015). There are different approaches to VM introspection such as guest-OS hook based, VM state access based, kernel debugging based, interrupt based and hypercall authentication based; they bridge the semantic gap in interpreting the low-level information available at a VM to high level semantic state of a VM. There are several open source based VMI tools such as Ether (Dinaburg et al., 2008) and DRAKVUF (Lengyel et al., 2014) that perform introspection of VMs from outside.

VMI techniques leverage VMM technology that was lacking in traditional IDS approaches. Hypervisor or VMM is a software that creates and runs VMs. It can access any of the VM spawned by it. It emulates the physical hardware and prevents direct access to physical hardware. In Xen hypervisor based cloud environment such as Openstack (2015), VMI based IDS can be configured to run at the privileged domain of VMM; In Xen, Dom0 is a privileged domain that starts first and manages the unprivileged domains (untrusted guest domains), DomU. However, if a VMM is compromised, the VMI tool will be under the control of the attackers. HVI based security approach mainly depends on the hardware assistance to perform introspection of hypervisor/host OS kernel states and detect various attacks such as hardware attacks, rootkit attacks and side channel attacks.

In this paper, we address the limitations of existing surveys (Modi et al., 2013; Patel et al., 2010) and provide a detailed study of the detection mechanisms in the IDS. We also give a detailed discussion of the threat model, attacks and deployment approaches of IDS in a cloud environment. Our major contributions of this paper can be summarized as follows:

- We propose a threat model and attack taxonomy and provide a detailed discussion of the various attacks related to the cloud environment.
- We provide a classification of IDS deployment approaches for a cloud environment, with an analysis of their advantages and disadvantages.
- We propose a classification of intrusion detection mechanisms in the cloud environment. The detailed analysis of techniques is intended to provide the readers a coherent view of the security solutions that currently exist.
- A classification of VMI techniques is proposed and discussed in detail, especially for detecting attacks from VM to hypervisor (VM-VMM) and stealthy rootkit attacks at the VM.
- A classification of HVI techniques is proposed and discussed especially for detecting attacks from hypervisor to VM (VMM-VM) and hardware attacks at the VMM.
- Finally, we identify specific research challenges and outline some possible future directions in cloud based IDS.

The rest of the paper is organized as follows: Section 2 gives the background on cloud based IDS and and highlights the difference between traditional IDS and cloud based IDS. Section 3 describes the threat model for a cloud environment and outlines an attack taxonomy. Section 4 describes the different deployment approaches of IDS in a cloud. Section 5 describes the proposed IDS taxonomy and presents a detailed study of intrusion detection techniques for a cloud environment. Section 6 provides observations and summarizes some potential research challenges. Section 7 provides a comparison of our paper with other related surveys. Finally, section 8 concludes the paper.

2. Evolution of cloud based IDS

Traditional IDS systems have been applied to a cloud environment by several researchers. For example, Roschke et al. (2009) proposed a Snort based IDS architecture named as VM-Integrated IDS to detect anomalies. Modi et al. (2012a) used Snort and machine learning classifiers to detect anomalies in the network traffic between VMs. Alarifi and Wolthusen (2012) used traditional 'Bag of System Calls' based approach to detect anomalous sequences present in the user programs during execution. Gupta and Kumar (2015) proposed immediate sequence of system call based approach which is similar to traditional look-ahead based approach (Forrest et al., 1996). Li et al. (2012) applied Artificial Neural Network (ANN) to detect attacks in the cloud. Pandeeswari and Kumar (2016) applied Fuzzy C-Mean Clustering based ANN to detect intrusions in the cloud. In all the above approaches, the IDS works in a standard manner and is deployed at the end host cloud servers or tenant virtual machines. However, while adopting a traditional IDS to the cloud, one needs to define the various components of the IDS and where they are placed and the access privileges they have.

Modern malwares can easily thwart traditional HIDS based on signature matching or static analysis techniques by using obfuscation and encryption techniques (Baysa et al., 2013). Dynamic analysis based traditional IDS can be evaded by checking the presence of specific security processes in the memory of monitored tenant VM or end host as security analyzer is deployed in the monitored machine. In addition, a malicious malware program can sense the virtual environment by checking the registry key values and the presence of drivers specific to virtualization. An attacker can also try to sense the periodic behavior of security analyzer by observing the monitored machine (Wang, 2014a). Some other malware attacks check the modification in the processor specific register values (set by the security analyzer to hide their presence from the VM) to detect the presence of security analyzer (Pék et al., 2011). VM-rootkit attacks perform the guest OS kernel modification. They hide their presence from the traditional IDS deployed at monitored machine. The detection of such attacks is essential at the primary stage since it can lead to further attacks such as side channel attacks (Zhang et al., 2012). Traditional HIDS are limited in their capability to detect such attacks in virtualized environment.

On the other hand, some traditional NIDS based cloud security frameworks have been proposed to detect network intrusions (Roschke et al., 2009; Gul and Hussain, 2011). They are based on rule-matching techniques and can detect network attacks targeting tenant VMs.