ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 2, No.8 , March 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Traditional Host based Intrusion Detection Systems' Challenges in Cloud Computing

Masoudeh Keshavarzi[1]

[1] **Department of Computer, Payame Noor University**
Tehran, Iran
Masoudeh_k@yahoo.com

Abstract

Cloud computing is one of the hottest topics in IT today. It can help enterprises improve the creation and delivery of IT solutions by allowing them to access services more flexibly and cost-effectively. Security concerns in the cloud environment are the main obstacles in cloud adoption. As clouds are distributed in nature, it becomes an easy target for the intruders to exploit the vulnerabilities of the network. Intrusion Detection Systems are one of the key components for securing computing infrastructures. But there are some issues in applying traditional intrusion detection systems on the cloud. This paper discusses each of the three cloud models, their security risks and covers the study of intrusion detection system implemented in cloud environment for dealing with various security issues related to cloud, and offers solutions for it.

Keywords: ***C****loud computing, Security, Intrusion detection system, Virtualization.*

1. Introduction

Cloud computing [1,2] is becoming increasingly popular. Many companies utilize cloud computing services to minimize IT infrastructure costs. Virtualization and cloud computing have changed the face of today's datacenter. With the development of information technology, cloud computing becomes a new direction of grid computing. Cloud Computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. To provide secure and reliable services in cloud computing environment is an important issue. According to the statistical report [3] on the buzzword from Google, cloud computing becomes more popular than grid computing with the vigorous push of virtualization [4,5].

Intrusion detection systems (IDSs) are nowadays recognized as fundamental tools for the security of computer systems. IDSs aim at identifying violations of security policies and perform automatic counteractions to protect computer systems and information. As soon as IDSs are deployed, they may become target of attacks that may severely undermine or mislead their capabilities. Intrusion detection systems are one of the most popular devices for protecting cloud computing systems from various types of attack. But the traditional intrusion detection system is not flexible in providing security in cloud computing because of the distributed structure of cloud computing. Since cloud computing is distributed in nature, supports multi-user and multi-domain platform, it is more prone to security threats. In addition to the contemporary security issues, Clouds present novel security challenges which require dedicated efforts for their solution. This paper has focused on one such challenge i.e. intrusion detection problem for Clouds. In an effort to address this challenge, the paper presents a virtual machine introspection based approach which makes use of virtual machine monitor' parameters such as isolation, inspection and interposition for build an effective IDS in cloud environment.

The rest of this paper is organized as follows. Section 2 describes the overall architecture of cloud computing and introduces type of cloud and the service models. Section 3 discusses security issues in cloud environment. In Section 4, we describe traditional intrusion detection system and type of that. Section 5 and 6 present challenges and solutions to design intrusion detection system in cloud environment. Section 7 discusses some related works. Finally, Section 8 concludes this paper and outlines future work.

2. Cloud computing architecture

Cloud computing is an emerging and evolving architecture, and as a result, many definitions and expectations of the architecture exist. The National Institute of Standards and Technology (NIST) has defined "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,

storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [6]. Cloud computing represents a paradigm shift for delivering resources and services; this results in important benefits for both cloud providers and cloud consumers. Advantages of the cloud computing technology include cost savings, high availability and easy scalability. Consumers rent resources from a third-party provider, consume them as a service and pay only for resources that they use.

This cloud model promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service), three service models, and four deployment models [6].

2.1 Cloud Service models

About the services, which are served over cloud computing systems there is a definition as Anything as a Service (XaaS). The type of computing resource that is offered in a cloud defines a cloud's service model. NIST and the industry have identified three common service models that are based on what cloud services are provided: applications, platform, and/or infrastructure. [7] refers to these three as the SPI model. These three main service models of the cloud computing are shown in Figure 1 and detailed as follows.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. With Software as a Service, service consumers get their software applications from the service provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. She just uses the software as an application while the provider manages the underlying platform software and infrastructure hardware (e.g., Google Apps [8]).

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. The platform may include databases and middleware in addition to application development tools (e.g., Google App Engine [9], Microsoft's Azure [10]).

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. With Infrastructure as a Service, the provider manages the underlying physical cloud infrastructure (servers, storage, network, and the associated virtualization and operating systems software) while the consumer deploys and runs his or her own application and platform software. Virtualization software is often a key enabler for IaaS architectures (e.g., Amazon Web Service (AWS) [11], Eucalyptus [12], OpenNebula [13]).

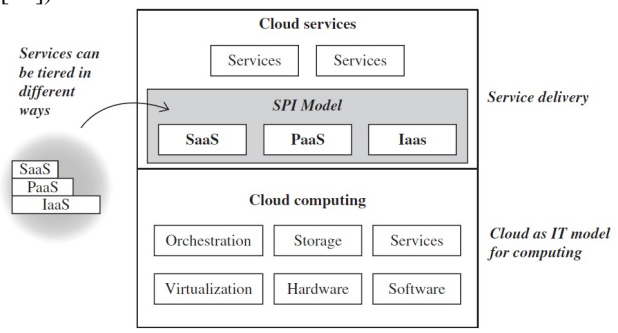

Fig 1. The SPI model [7]

2.2 Type of clouds

These are commonly known as Public, Private, and Hybrid models. The following sections use the National Institute of Standards and Technology definition of cloud to introduce these different types of cloud [6];

Public cloud- According to NIST, a public cloud is one in which the infrastructure is open to the general public for consumption. Due to the nature of public clouds, they are exposed to a higher degree of risk.

Private cloud- According to NIST, a private cloud is provisioned for exclusive use by a single organization comprising multiple consumers, such as business units. It may be owned, managed, and operated by the organization, a third-party, or some combination of them.

Community cloud- NIST defines a community cloud as one whose infrastructure is provisioned for the exclusive use by a specific community of consumers from organizations that have shared concerns. For example, mission, security requirements, policy, and compliance considerations. It may be owned, managed, and operated by one or more of the organizations in the community, a third-party, or some combination of them.

Hybrid cloud- The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

3. Security issues in cloud environment

Cloud computing presents exciting opportunities to establish large scale computing infrastructures which are available on demand to fulfill customized user requirements. In addition to the contemporary security issues, Clouds present novel security challenges which require dedicated efforts for their solution.
Cloud computing has some security issues that need to be addressed before enterprises consider switching to the cloud computing model [7,14]. They are as follows:
Network availability- Since a public cloud is by definition accessed over the Internet, the cloud provider must address the potential for catastrophic loss of Internet backbone connectivity.
Privileged user access- information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership.
Regulatory compliance- clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by third party organizations that check levels of security and providers that don't.
Privacy and Data location- Data may not remain in the same system, the same data center, or within the same cloud provider's systems. Conceivably, data may even be stored in another country, incurring considerable concern.
Data segregation and Control over data- encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.
Disaster recovery and Business continuity- every provider should have a disaster recovery protocol to protect user data.
Investigative support- if a client suspects faulty activity from the provider, it may not have many legal ways pursued an investigation.
Long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.
Systems vulnerabilities and Risk of common attacks- All software, hardware, and networking equipment is subject to exposure of new vulnerabilities. Some components may pose greater risks based on a history of vulnerabilities and exploits. Tenants may not tolerate specific vulnerabilities or risk areas for a range of reasons. A specific cloud may be subject to new attack types, or it may be immune to common attack types based on various reasons.

According to latest case, Security threats can be categorized as follow [15];

- Cloud data confidentiality issue
- Network and host based attacks on remote Server
- Cloud security auditing
- Lack of data interoperability standards

4. Traditional Intrusion Detection System

Intrusion detection systems (IDSs) are a critical part of an organization's overall network and system's protection strategy and a critical part of a defense-in-depth architecture. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [16]. Intrusion detection involves determining that some entity, an intruder, has attempt to gain, or worse, has gained unauthorized access to the system.
Intrusion detection systems use different methods to detect security incidents. Traditionally, there are two major types for these detection systems: signature-based IDS and anomaly-based IDS. A signature-based IDS [17,18] (or called rule-based IDS), detects an attack by comparing incoming events with its stored signatures. A signature is a kind of descriptions to represent a known attack using some features. An anomaly-based IDS [19,20] aims to identify great deviations by comparing current system or network events with a predefined normal profile. An anomaly event is detected if the deviation exceeds a pre-determined threshold.
Based on the protected objective, IDS can be classified into host-based intrusion detection systems (HIDS), network-based intrusion detection systems (NIDS), or distributed intrusion detection systems (DIDS), which contain both types of sensors.
HIDS. Host-based intrusion detection systems install on a host and monitor multiple data on one specific machine, such as system log files, operating system data structures, or system calls.
NIDS. Network-based intrusion detection systems are used to monitor network traffic between multiple computers.
DIDS. One type of self-monitoring system is the distributed intrusion detection systems, a security system

designed to detect suspicious activity with a system [21]. The DIDS uses multiple IDSs to protect a distributed system.

5. Challenges

Traditional NIDS and HIDS cannot identify suspicious activities in a cloud environment. As an example, a NIDS may not detect an attack sometime when node communication is encrypted. Attacks can also be invisible to HIDS, because they may not leave traces in the node operating system where the IDS resides [22]. Moreover, the traditional security tools lack either isolation from an attacker or have little visibility of the monitored system. It does not adequately address the new security risks unique to virtualization and cloud computing. At the same time, such security tool negatively impacts performance on these platforms.

Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDOS) and Cross Site Scripting (XSS). In cloud computing, user data and application is hosted on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Intrusion detection systems are defeated either through attack or evasion [23]. Evading an IDS is achieved by disguising malicious activity so that the IDS fails to recognize it, while attacking an IDS involves tampering with the IDS or components it trusts to prevent it from detecting or reporting malicious activity. HIDS will often be compromised along with the host OS because of the lack of isolation between host and attacker. HIDSs operate at either user or kernel space, giving them good visibility because they can report process lists, network connections, files, etc. Unfortunately, HIDSs do not have high resilience because their control and the data structures they rely on can be taken over by an attacker. Once the HIDS is compromised, it is easily blinded and may even start to report misleading data, or provide the adversary with access to additional resources to leverage for their attack. A compromised IDS is useless.

Network-based intrusion detection systems that offer high attack resistance at the cost of visibility, and host-based intrusion detection systems that offer high visibility but sacrifice attack resistance. Hence, traditional IDSs are not suitable for a dynamic and distributed cloud environment.

6. Solutions

Virtualization [24–25] is the cornerstone technology for cloud computing to multiplex computing resources on a single cloud platform for multi-tenant computing capability. With the fusion of cloud computing and virtualization technology, system security under virtualization becomes a key point in recent research. As above paragraph discussed, traditional IDSs are not suitable for a dynamic and distributed cloud environment. Therefore, use of virtualization technology presents a new architecture for building intrusion detection systems that provides good visibility into the state of the monitored host, while still providing strong isolation for the IDS, thus lending significant resistance to both evasion and attack.

Virtualization and cloud computing are revolutionizing information technology by facilitating a more efficient use of computing resources. Virtualization is the technology that enables many separately running operating system instances to occupy a single computer. Each virtual machine (VM) instance runs as though it were occupying its own dedicated server. This can enable an organization to more easily deploy and manage servers. Virtual machine introspection (VMI) is the key technology widely used in the existing security protection system [23]. This mechanism allows us to pull our IDS "outside" of the host it is monitoring, into a completely different hardware protection domain, providing a high-confidence barrier between the IDS and an attacker's malicious code. IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach.

7. Related work

There are several problems about deploying IDS and security in cloud environment. Different researchers raise various models or schemes for solving such problems [26, 33]. Many efforts have been taken in the area of Cloud computing and intrusion detection system but still there are more attacks that have not been detected. For example, the researchers worked in this field to overcome the current security threats in the Cloud computing through implementing IDS in Cloud environment which is responsible of monitoring the utilization of resources for the virtual machine using data acquired from virtual machine monitors. More specifically, all monitoring operations are done outside the virtual machines so the attacker cannot modify the system in the case of tenant's instance is breached.

Virtual machine introspection (VMI) is a technique whereby an observer can interact with a virtual machine client from the outside through the hypervisor. In 2003, Garfinkel and Rosenblum [23] first demonstrated a technique for intrusion detection inside a virtual guest using VMI. In 2009 using VMware's VMSafe, Symantec demonstrated injecting anti-virus code into a virtual machine from the VMware hypervisor [34]. In 2012, [26] introduces Maitland as a prototype proof-of-concept implementation a lighter-weight introspection tool, which exploits paravirtualization and Supports Cyber-Security in the Cloud. Kleber, schulter et al. [35] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect, and so on.

8- Conclusion and future work

Cloud Computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet. It is an internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Security attacks are a threat to virtually any system connected to the Internet. Currently the biggest hurdle in cloud adoption by most of the corporate organizations is its security. As the basis of cloud computing, the virtualization technology is paid more and more attention from academia and industry.

Intrusion Detection Systems are nowadays recognized as necessary tools for the security of computer systems. Their objective is to protect against attempts to violate defense mechanisms. In this paper, we discussed each of the three cloud models, their security risks and covered the study of intrusion detection system implemented in cloud environment for dealing with various security issues related to cloud, and offers solutions for it. We find out traditional IDSs are not suitable for cloud environment and the best approach is using VMI technology in design security system in virtual and cloud environment. We're implementing monitoring system via introspection in virtual environment, with focus file integrity monitoring [36] and we're going to extend that to cloud computing.

References

[1] M. Armbrust, A. F. (2009.). Above the clouds: a Berkeley view of cloud computing. University of California, Berkeley: EECS Department.

[2] R. Buyya, C. Y. (2009). Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing. 5th utility, Future Generation Computer Systems , pp. 599–616.

[3] Foster I, K. C. (2001). The anatomy of the grid: enabling scalable virtual organizations. International J High Perform Comput, (pp. 200–222).

[4] M. Rosenblum, T. G. (2005). Virtual machine monitors: current technology and future trends. IEEE Computer , 39–47.

[5] Adams K, A. O. (2006). A comparison of software and hardware techniques for x86 virtualization. 12th international conference on architectural support for programming languages and operating systems (pp. 2–13). California: ACM.

[6] National Institute of Standards and Technology (NIST) Definition of Cloud Computing. (n.d.). Retrieved from http://csrc.nist.gov/groups/SNS/cloudcomputing/

[7] Winkler, V. (2011). Securing the Cloud. USA: Syngress.

[8] Google apps. [Online]. Available: http://www.google.com/apps/business

[9] "Google apps engine." [Online]. Available: URL http://code.google.com/appengine.

[10] Azure services platform. [Online]. Available: http://www.microsoft.com/azure

[11] Amazon web services. [Online]. Available: http://aws.amazon.com

[12] Eucalyptus. [Online]. Available: http://eucalyptus.cs.ucsb.edu/.

[13] Opennebula. [Online]. Available: http://www.opennebula.org

[14] Sanjay Ram M, V. N. (2012). Effective Analysis of Cloud Based Intrusion Detection System. ijcait, I(2), 16-22.

[15] Richard Chow, P. G. (2009). Controlling Data in the Cloud: Outsourcing Computation without utsourcing Control. ACM Computer and Communications Security Workshop. CCSW 09.

[16] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1by Cloud Security Alliance 2009 https://cloudsecurityalliance.org.

[17] Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX Conference on Large Installation System Administration, (pp. 229-238).

[18] Kemmerer, G. V. (1998). NetSTAT: A Network-based Intrusion Detection Approach. Proceedings of the 14th Annual Computer Security Applications Conference (pp. 25-34). ACSAC.

[19] A.K. Ghosh, J. W. (1998). Detecting Anomalous and Unknown Intrusions Against Programs. Proceedings of the 14th Annual Computer Security Applications Conference (pp. 259-267). ACSAC.

[20] Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks 31(23-24), pp. 2435-2463.

[21] S. Snapp, J. B. (1991). A system for distributed intrusion detection. In Proceedings of the COMPCON, (pp. 170–176).

[22] Shun-Fa Yang, W.-Y. C.-T. (2011). ICAS: An inter-VM IDS Log Cloud Analysis System. Cloud Computing and Intelligence Systems (CCIS) (pp. 285-289). IEEE Press.

[23] Garfinkel T, R. M. (2003). A virtual machine introspection based architecture for intrusion detection. Proceedings of the

10th annual symposium on Network and Distributed System Security (pp. 191–206). NDSS 2003.
[24] S. Nanda, T. C. (2005). A survey on virtualization technologies. SUNY at Stony Brook: ECSL-TR-129.
[25] Rosenblum M, G. T. (2005). Virtual machine monitors: current technology and future trends. IEEE Comput, 39–47.
[26] Chris Benninger, S. W. (2012). Maitland: Lighter-Weight VM Introspection to Support Cyber-Security in the Cloud. 2012 IEEE Fifth International Conference on Cloud Computing, (pp. 471-478).
[27] Iti Raghav, S. C. (2013). Intrusion Detection and Prevention in Cloud Environment: A Systematic Review. International Journal of Computer Applications, 68, 7-11.
[28] Junaid Arshad, P. T. (2013). A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 416–428.
[29] Kenichi Kourai, S. C. (2005). HyperSpector: Virtual Distributed Monitoring Environments for Secure Intrusion Detection. 1st ACM/USENIX international conference on virtual execution environments (pp. 197-207). Chicago: ACM.
[30] Martin Crawford, G. P. (2013). Insider Threat Detection using Virtual Machine Introspection. 46th Hawaii International Conference on System Sciences (pp. 1821-1830). US: IEEE.
[31] Sang-Soo Yeo, J. H. (2013). Security Considerations in Cloud Computing Virtualization Environment. Springer, 208–215.
[32] Tongwook Hwang, Y. S. (2013). Design of a Hypervisor-based Rootkit Detection Method for Virtualized Systems in Cloud Computing Environments. The 2013 AASRI Winter International Conference on Engineering and Technology (pp. 27-32). AASRI-WIET.
[33] U. Oktay, O. S. (2013). Attack Types and Intrusion Detection Systems in Cloud Computing. 6th INTERNATIONAL INFORMATION SECURITY & CRYPTOLOGY CONFERENCE (pp. 71-76). Ankara: ISC.
[34] Conover M, Chiueh T. Code injection from the hypervisor: removing the need for in-guest agents. In: Proceedings of Blackhat USA; 2008 [accessed 01.11.11].
[35] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.
[36] Keshavarzi, M., & Heidarinezhad, M. R. (2013). A novel file integrity monitoring method via introspection virtual machine. 7th International Conference on e-Commerce in Developing Countries with focus on e-Security. Kish Island, Iran: ECDC 2013.