A Double Circular Chain Intrusion Detection for Cloud Computing Based on AdjointVM Approach

Chung-Huei Ling[1], Wei-Fu Hsien[2], and Min-Shiang Hwang[1,3]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Management Information System, National Chung Hsing University[2]
Department of Medical Research, China Medical University Hospital, China Medical University[3]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received Oct. 7, 2014; revised and accepted Feb. 8 & Apr. 16, 2015)

Abstract

In the letter, we propose an improved model, which is built on AdjointVM. Our model can improve the situation where attackers can successfully intrude two adjacent virtual machines. Because of this situation, it will lead to the collapse of the entire cloud services. This model uses a double circular chain concept, which can be a virtual machine capable of double Intrusion Detection System detections. Therefore, it can effectively resist the two adjacent virtual machines are compromised. Finally, we compare the related methods. Although the proposed scheme consumes more time, it will improve the security invasion of virtual machines.

Keywords: Cloud computing, double circular chain, intrusion detection, VM

1 Introduction

With the popularity of cloud computing, there are many cloud services [4]. However, not every person or business has the ability to build his own cloud services. Therefore, a lot of cloud service providers have appeared, such as Google, Microsoft, Amazon, and so on. These major cloud service providers offer three service models, including SaaS, PaaS, and IaaS, which are either free or charged to the cloud users. Due to the popularity of cloud services, a growing number of cloud users will handle sensitive personal data in the cloud by cloud providers [2]. Because cloud providers have the privilege to manage the customer's virtual machine (VM), the guest VM is vulnerable to the impact of privileged VM. Although some cloud service providers are well-known companies, it does not mean that the cloud services they provide are safe. Therefore, cloud service providers may suffer internal or external attacks, causing the user data leakage, harming goodwill, and losing customers [5, 9].

Recently, Kong proposed a method, which protected guest VM from completely exposed to the privileged VM, and guest VM from being vulnerable to the attack of privileged VM [6]. His method is to create two VMs, protected VM and AdjointVM. Protected VM provides services to customers, it can also be detected by IDS from AdjointVM. However, Oktay et al. pointed out that there was a secure issue in Kong's scheme [6, 7]. If attackers intrude AdjointVM, it will not be detected by IDS. Thus, protected VM will be intruded successively. Therefore, Oktay et al. proposed a Circular Chain VM scheme to improve the problem, which was detected each other by two VMs.

2 The proposed scheme

We find a case; when attackers can successfully intrude adjacent two VMs, it will be unsafe in the Circular Chain model. Adjacent two VMs means that there is IDS connected between two VMs. For example, in the Figure 1, cloud service providers configure n VMs in hypervisor. Circular Chain model is the link between n VMs. When attackers intrude VM2 and VM3 at the same time, VM3 will not have the ability to detect the next one VM. Since VM2 and VM3 are intruded, a series of VM will be successful intruded until VM1. Because this situation causes each VM intruded, it leads to the collapse of the entire Circular Chain model. Then each VM users will leak private information stored on the service. This is a serious security problem, so we propose a scheme as shown in Figure 2.

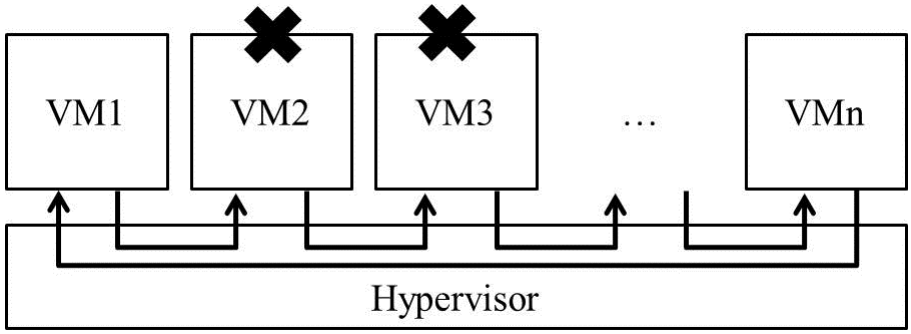

Figure 1: A circular chain model is under compromised situation

The proposed model uses Trusted Computing technologies to create a VM's boot, and the core of Trusted Computing is the Trusted Platform Module (TPM) [1, 3]. TPM is an integrated composition of security encryption keys, and it uses control commands defined in the software running on the system. Because TPM uses encryption methods implemented in hardware, software can effectively resist the attack.

First, hypervisor can get secure boot from TPM. Second, hypervisor creates n VMs. Because VM's boot will not cross the privileged VM in this process, guest VM's boot is not modified by privileged VM. Third, each VM is divided into guest applications, OSSEC Server, OSSEC Agent, KMD, Kernel Mapper, and Guest Kernel. Guest application is the provision of services to users. OSSEC Server/Agent is an IDS software, and it can detect the computer anomalies [8]. KMD monitors guest kernel by kernel mapper [6]. The left link refers to detecting the direction between VMs, from small to large detections. On the contrary, the right link refers to detecting from large to small directions. Finally, the model will become a Double Circular Chain.

3 External IDS

OSSEC is an open-source HIDS. It performs log analysis, rootkit detection, file integrity checking, policy monitoring, real-time alerting, and active response [8]. Installation is divided into two kinds, Local and Server/Agent. The first one is the Local mounted single host, the other is a Server/Agent installed on multiple hosts. Server/Agent way is to select one to install and configure multiple hosts for the Server, and other hosts install Agent. Before managers monitor the status of all Agents by Server, Agent will detect the event sent to the Server. With virtualization technology, OSSEC software can be installed to the VM's OS. Therefore, OSSEC software can establish Server/Agent mode on a virtual machine.

In this study, because the cloud services require multiple virtual machines, OSSEC Sever/Agent is more suitable to be chosen. First, each VM is installed and configured into OSSEC Server and Agent, so each virtual machine can have two kinds of identity. Second, each VM OSSEC Sever is set to connect two adjacent OSSEC Agents. Therefore, an OSSEC Server can detect two adjacent OSSEC Agents, and each OSSEC Agent is detected by two adjacent OSSEC Servers. Finally, each virtual machine has the ability to detect and to be detected.

4 Internal IDS

OSSEC software detects the external behaviour of the computer, such as malicious or incorrect behaviour [8]. However, we use VM to build cloud services, so it is necessary to consider the internal security such as VM's kernel. Kernel is software that manages application access to system resources in computer hardware. Therefore, each VM has kernel itself. If a VM's kernel has been invaded, an intruder may lead to control the computer hardware resources.

In order to enhance the VM's kernel security, Kernel Monitor Daemon (KMD) is added to monitor it. KMD has two parts, Guest Kernel and Kernel Mapper. Guest Kernel is a VM's kernel itself, and Kernel Mapper is detected by a mapping of VMs kernel. KMD checks kernel by mapping, reading and writing abilities to detect VM's memory. Before KMD is compared with the saved hash values, it generates a value of hash function for an important space in the memory. If there is a change event detected, KMD will record the event and report to the manager. Finally, the integrity of the memory can be achieved.

4.1 Analysis

Table 1 is a comparison among our scheme and others. In this study, the hypothesis n is the number of VMs, each VM to detect every time consuming for t. Because the proposed scheme uses double detections between VMs, the number of links is used more. When creating n VMs in the cloud environment, our method requires only n VM to protect all are safe. If the attacker invades two adjacent VMs, it will be detected. Because of this model, two fault-tolerant VMs, guest VM has twice the security.

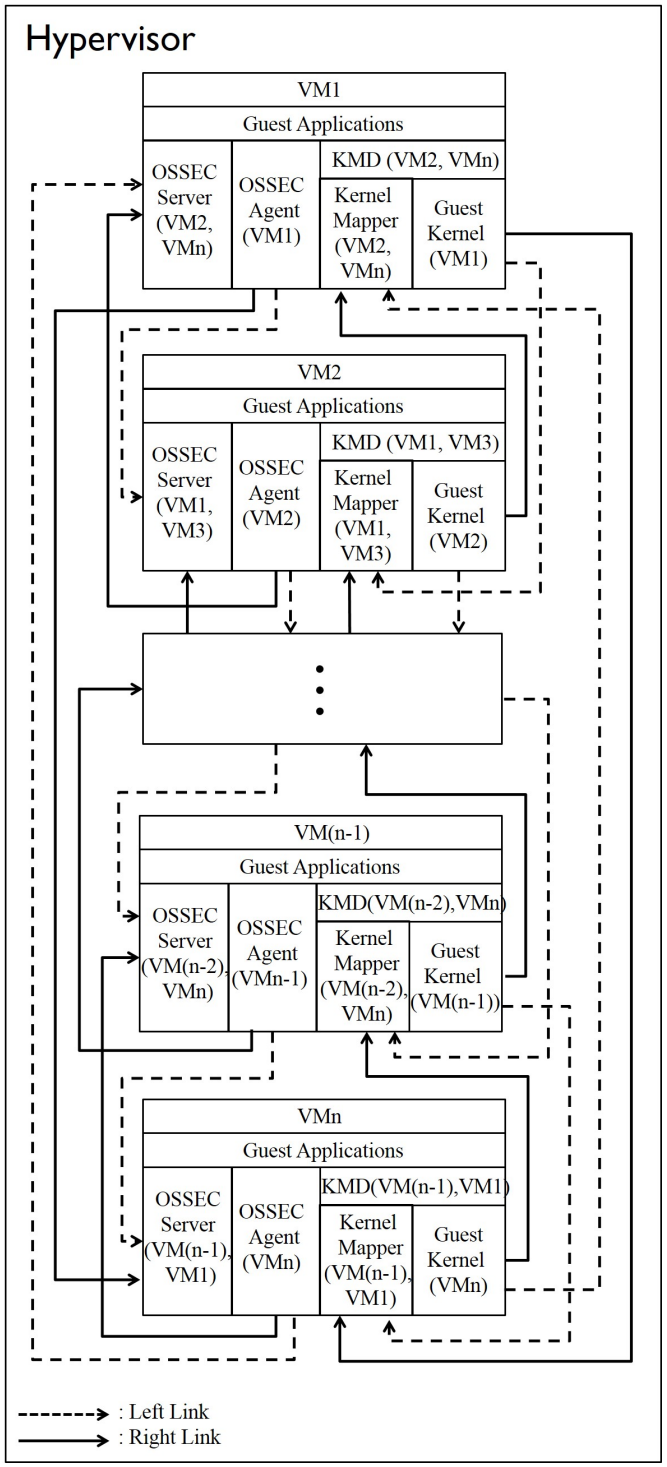

Figure 2: Detailed overview of double circular chain model

Although the proposed scheme consumes more time, it will improve the security invasion of virtual machines.

5 Conclusions

In the letter, we propose a method to improve the AdjointVM, so it can doubly detect between VMs. Therefore, we can strengthen the VM fault tolerance to be attacked. When two adjacent VMs are invaded, it will be detected by the IDS, which does not lead to the collapse of the entire cloud environment. Thus, our method can avoid two adjacent VMs are compromised. Although our method can improve the safety, we use a lot of time, which leads to increased cost of the chain. Because our model needs to plan the number of virtual machines, it is more difficult to dynamically adjust the link. In the future, we will improve the link costs and the elasticity of the expansion in the model.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC102-2221-E-468-020 and NSC101-2622-E-468-002-CC3. The authors gratefully acknowledge the reviewers for their valuable comments.

References

[1] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, L. van Doorn, "vTPM: Virtualizing the trusted platform module," in *Proceedings of the 15th USENIX Security Symposium*, pp. 21–21, 2006.

[2] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[3] P. England, L. Loeser, "Para-virtualized TPM sharing," in *Trusted Computing - Challenges and Applications*, LNCS 4968, pp. 119–132, Springer, 2008.

[4] M. Hogan, F. Liu, A. Sokol, J. Tong, *NIST Cloud Computing Standards Roadmap*, NIST Special Publication 500-291 (SP500-291), National Institute of Standards and Technology, 2011.

[5] C. C. Lee, P. S. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[6] U. Oktay, M. A. Aydin, O. K. Sahingoz, "A circular chain intrusion detection for cloud computing based on improved AdjointVM approach," *IEEE International Symposium on Computational Intelligence and Informatics*, pp. 201–206, 2013.

[7] U. Oktay, M. A. Aydin, O. K. Sahingoz, "Circular chain VM protection in AdjointVM," *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering*, pp. 93–97, May 2013.

Table 1: A comparison among our scheme and others

Feature	J. Kong [6]	U. Oktay [7]	Our scheme
Detection of direction	Single	Single	Double
Number of VMs to protect n VMs	$2n$	n	n
Fault tolerance	1	1	2
Security VM	$n/2$	n	$2n$
Initial number of link	n	$2n$	$4n$
Time complexity	nt	$2nt$	$4nt$

[8] OSSEC, *Open Source Security (OSSEC)*, Nov. 1, 2014. (`http://www.ossec.net/`)

[9] M. Uddin, A. A. Rehman, N. Uddin, J. Memon, R. Alsaqour, and S. Kazi, "Signature-based multi-layer distributed intrusion detection system using mobile agents," *International Journal of Network Security*, vol. 15, no. 2, pp. 97–105, 2013.

Chung-Huei Ling received his M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California , USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and radio frequency identification.

Wei-Fu Hsien received his B. S. in Department of Information Management from National Kaohsiung Marine University, Kaohsiung, Taiwan, ROC, in 2013. He is currently pursuing the M.S. degree with the Department of Management Information Systems from National Chung Hsing University. His research interests include security and privacy of cloud computing, and applied cryptography.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.