Scientific Research Publishing

Journal of Information Security, 2017, 8, 1-7
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment

Ahmad Fayez S. Althobaiti

Department of Computer and Information Sciences, Al-Imam Muhammad Ibn Saudi Islamic University, Riyadh, Saudi Arabia
Email: Afalthobaiti@imamu.edu.sa

How to cite this paper: Althobaiti, A.F.S. (2017) Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment. *Journal of Information Security*, **8**, 1-7.
http://dx.doi.org/10.4236/jis.2017.81001

Received: October 22, 2016
Accepted: December 4, 2016
Published: December 7, 2016

Abstract

The data and applications in cloud computing reside in cyberspace, that allowing to users access data through any connection device, when you need to transfer information over the cloud, you will lose control of it. There are multi types of security challenge must be understood and countermeasures. One of the major security challenges is resources of the cloud computing infrastructures are provided as services over the Internet, and entire data in the cloud computing are reside over network resources, that enables the data to be access through VMs. In this work, we describe security techniques for securing a VCCI, VMMs such as *Encryption and Key Management* (*EKM*), *Access Control Mechanisms* (*ACMs*), *Virtual Trusted Platform Module* (*vTPM*), *Virtual Firewall* (*VF*), *and Trusted Virtual Domains* (*TVDs*). In this paper we focus on security of virtual resources in Virtualized Cloud Computing Infrastructure (VCCI), Virtual Machine Monitor (VMM) by describing types of attacks on VCCI, and vulnerabilities of VMMs and we describe the techniques for securing a VCCI.

Keywords

Cloud Computing, Security Threats, Virtual Machine Monitors, Cloud Security

1. Introduction

Deploying cloud computing in an enterprise infrastructure brings significant security concerns. Monitoring of the virtual machines with high security and minimal overhead is always very important, especially in those environments where hundreds of Virtual Machines VMs are running on dozens of physicals servers. In this paper we focus on security of virtual resources in Virtualized Cloud Computing Infrastructure (VCCI), Virtual Machine Monitor (VMM) by describing types of attacks on VCCI, and vulnerabilities of VMMs and we describe the techniques for securing a VCCI. Also it is identified that either monitoring hypervisor only will be enough to collect detailed resources consumptions or VMMs will also be required. To complete the experiment of resource monitoring, techniques for securing a VCCI, VMMs such as Encryption and Key Management (EKM), Access Control Mechanisms (ACMs), Virtual Trusted Platform Module (vTPM), Virtual Firewall (VF), and Trusted Virtual Domains (TVDs) is required [1] [2] [3].

2. FIVESaaS Security Challenges

Top security concerns in cloud computing: Insecure Application Program Interface (APIs) or programming interfaces, Data protection, Access management inside employee threats, and Share technology issues:

1. Hypervisor security.
2. Cross-side channel attacks between VMs.

In this paper we discuss attacks between Virtual Machines, and how we protected and isolation from attackers. In his case, Virtual Machines share the physical memory, Central Processing Unit (CPU) cycles, network buffers, DRAM of the physical Machines. So Attacks takes place in two steps:

1) Placement of attacker virtual machine on the same physical machine.
2) Exploiting the shared resources.

CPU cache leakage attack:

Measure load of the other virtual web server.

Extract AES and RSA keys.

Keystrokes timing analysis.

Extract user passwords from SSH terminal.

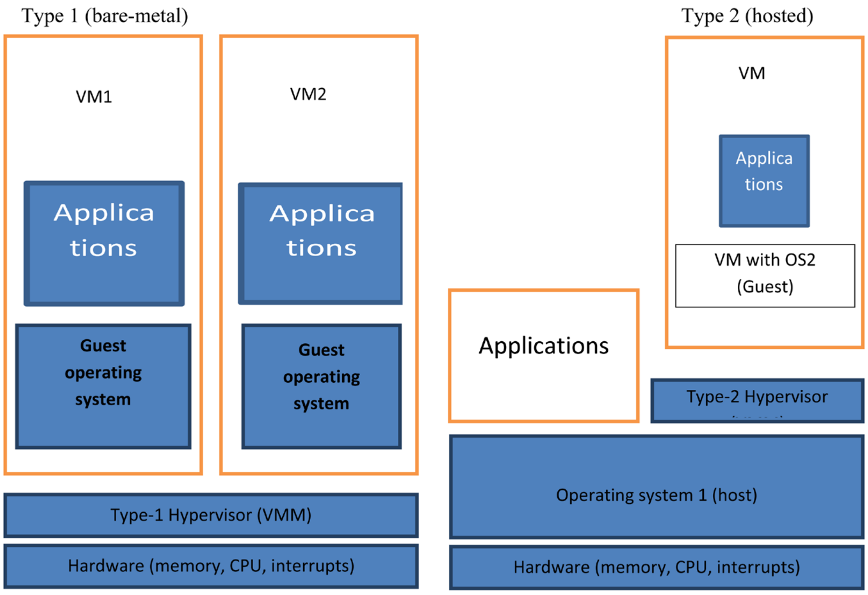
3. Security Issues in Cloud Environment

Infrastructure-as-a-service (IaaS) security issues:

The resources such as servers, storage, networks, and other computing resources are provided by IaaS in the form of virtualized systems, which are accessed through the Internet. Access to cloud resources over the network takes essentially three distinct forms: Admin command to the cloud provider, admin command to Virtual Machine, and user interaction with the virtual machine using network services [4].

4. Security Threats to Cloud Computing Infrastructures

Application of clients running on Virtual Machine residing on Virtual Cloud Computing Infrastructure (VCCI), VMs aren't deal directly with physical hardware, VMs are manage by Virtual Machine Monitor, which is running in physical infrastructure. The VMM or hypervisor is software layer that allows several Virtual Machines to run on a physical machine. We have two types of hypervisors: type1 run directly upon HW. Type 2 run together with host OS. Type 2 includes Xen, and Kernel Virtual Machine (KVM), as shown in **Figure 1**.



VMware ESX, Microsoft hyper-v, XenVMware workstation, Microsoft Virtual PC, KVM.

Figure 1. Types of hypervisors [5].

Cross VM Side Channel Attacks

Attackers can use security gaps to attack on any component of VCCI that may effect on the others. In this paper we describe technique to overcome attackers on VCCI, and vulnerabilities of VMMs, the infrastructure needs to be secured by implementing security techniques that isolates the VMM, guest/host OS and physical hardware from the side effects of each other [2]. Identified two major attacks on VCCI (VM to VM and VM to Hypervisor) as shown in the **Figure 2**.

From above figure, attacks can take place through the major vulnerabilities (VM hopping, VM escape and VM mobility) identified in hypervisors. *VM hopping:* this attack can effect on denial of service, which make resources unavailable to user. *VM Escape*: this vulnerability allows a guest-level VM to attack its host. *VM Mobility*: under a VCCI, VMs can move from one physical host to another is called as VM mobility [5] [6].

5. Some of the Security Techniques for Securing the VCCI

In this work we identified and analyzed some major approaches for securing a VCCI; these include EKM, ACMs, vTPM, VFs, and TVDs.

Describe Security Threats to Virtualized Cloud Computing Infrastructures A multi-tenant Cloud Computing Infrastructure(CCI) consists of several Virtual Machines (VMs) running on same physical platform by using virtualization techniques. The VMs are monitored and managed by kernel based software *i.e.* Virtual Machine Monitor (VMM) or hypervisor which is main component of Virtualized Cloud Computing Infrastructure (VCCI). Due to software based vulnerabilities, VMMs are compromised to security attacks that may take place from inside or outside attackers. In order to formulate a secure VCCI, VMM must be protected by implementing strong security techniques such as Encryption

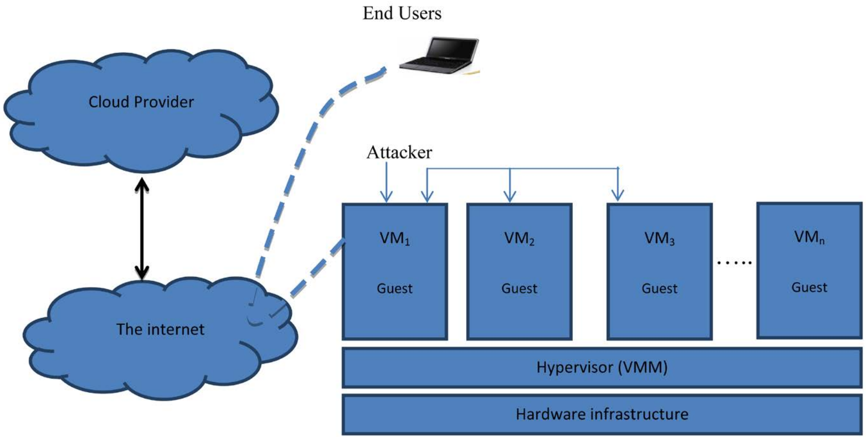


Figure 2. Attack on Virtual Cloud Computing Infrastructure (VCCI).

and Key Management (EKM), Access Control Mechanisms (ACMs), Intrusion Detection Tools (IDTs), Virtual Trusted Platform Module (vTPM), Virtual Firewalls (VFs) and Trusted Virtual Domains (TVDs). In this work we describe the techniques of virtualizing a CCI, types of attacks on VCCI, vulnerabilities of VMMs and we describe the significance of security techniques for securing a VCCI.

5.1. Encryption and Key Management (EKM)

Encryption and Key Management (EKM) is the common encryption methods that can be used on VCCI include symmetric and asymmetric algorithms. In this method, we protected data against the loss and theft is a shared responsibility of cloud customer and CSP. The common strongly encryption technique is Service Level Agreements (SLAs) [6]. Three different stages for protect confidential data for consumer:

a) Encryption of data-at-rest (encrypting the data on desk storage that protects data from illegal used and malicious CSP).
b) Encryption of data-at-transit (encrypting the confidential information such as credit cards while transmitting over the internet).
c) Encryption of data on backup media (external or internal storages), this protect from misuse of lost or stolen media.

5.2. Access Control Mechanisms (ACMs)

ACMs are responsible of protecting of a VCCI by restricting access, denying, limiting or to a system or an entity such as processes, VM and VMMs according to the well-defined security policies. Most common ACMs used in VCCI include Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these techniques are known as identity based ACMs as user subjects and resources objects are identified by unique names. Identification may be done directly or through roles assigned to the subjects [7]. ACMs guarantees integrity and confidentiality of the resources.

5.3. Virtual Trusted Platform Module (vTPM)

It's proposed by IBM researchers, is based on certificate chain linking vTPMs to the physical TPM in order to provide its capabilities and make it available to all VMs running on a platform. vTPMs can be located in a specific layer over the hypervisor. A vTPM instance is created for each VM by vTPM Manager which is built in a specific VM and may invoke its own vTPM through the hypervisor [8]. Each VM has its associated vTPM instance that emulates the TPM functionality to extend the chain of trust from the physical TPM to each vTPM via careful management of signing keys and certificates. A vTPM has its own virtual Endorsement Key (EK) and virtual Storage Root Key (SRK) beside some software on the host. In multi-tenant VCCI the system of vTPM virtualizes a physical TPM to be used by a number of VM on a single hardware platform.

5.4. Virtual Firewall (VF)

It is a firewall service running in a virtualized environment which provides usual packet filtering and monitoring services that a physical firewall provides [9]. VFs can execute in hypervisor-mode (hypervisor resident) and bride-mode. In order to protect the VMs and VMM, hypervisor-resident VFs must be implemented on the VMM where it is responsible to capture malicious VM activities including packet injections. These VFs require a modification to the physical host hypervisor kernel to install process hooks or modules allowing the VF system access to VM information and direct access to the virtual networks witches as well as virtualized network interfaces moving packet traffic between VMs. The hypervisor-resident VF can use the same hooks to then perform all firewall functions like packet inspection, dropping, and forwarding but without actually touching the virtual network at any point. Hypervisor resident VFs can be faster as compared to bridge-mode VFs because they are not performing packet inspection in VFs, but rather from within the kernel at native hardware speeds.

5.5. Trusted Virtual Domains (TVDs)

It is security technique formed at VCCI by grouping the related VMs running on separate physical machine into a single network domain with a unified security policy. The multiple instances of TVDs co-exist on a single platform under a shared resource policy. The use of TVD provides strong isolation among un-related VMs as the communication among TVDs takes places only according to the security policies defamed by administrator configured in the VMM. A malicious VM cannot join any TVD because in order to join TVD, a VM should fulfill the requirements of the policy so no malicious VM can affect the VMs of trusted users on cloud [10]. Normally the VMs residing in a TVD are labeled with a unique identifier. For instance the VMs of one customer will be labeled differently from the other customer. The labeling is used to identify the assigned VMs to a particular customer and to allow the same labeled VMs to run on inside the same TVD that must be designed by following a proper security guidelines and policies that doesn't exhibit any loop holes [11].

6. Conclusion and Future Work

Many security challenges are facing the cloud computing, and it will be difficult to achieve end to end security. According to the above analysis, we can see that, each client assigned with one or multiple Virtual Machines, VMM is major target of the attack on VCCI. However, to achieve secure VMM, we describe several techniques applied by various researchers to secure VCCI. However, the security must be applied at different layers of resources such as storage, network, and applications by considering to resource management issues such as SLAs (Service Level Agreements) are concerned in delivering software for a million users to use as a service via a data center, which is a lot more complex, as compared to distributing software for a million users to run on their individual personal computers. Our future work would investigate new models and techniques for securing VMM, VCCI depending on resources efficiency and cost of cloud computing providers.

References

[1] Kulkarni, G., *et al.* (2012) Cloud Security Challenges. *7th International Conference on Telecommunication Systems, Services, and Applications* (*TSSA*), India, October 2012, 88-91.

[2] Zhang, L.J., *et al.* (2009) CCOA: Cloud Computing Open Architecture. *IEEE International Conference on Web Services*, IBM T.J. Watson Research Center, New York, 6-10 July 2009, 607-616.

[3] Mehra, P., Katsaros, D., Vakali, A., Pallis, G. and Dikaiakos, M.D. (2009) Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE Internet Computing*, **13**, 10-13.

[4] Shengmei, L., *et al.* (2011) Virtualization Security for Cloud Computing Service. *International Conference on Cloud and Service Computing*, China, 174-179.

[5] Fu, W. and Li, X. (2011) The Study on Data Security in Cloud Computing Based on Virtualization. *International Symposium on IT in Medicine and Education* (*ITME*), Chongqing College of Electronic Engineering, 9-11 December 2011, 257-261.

[6] Buyya, R., Garg, S.K. and Calheiros, R.N. (2011) SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions. *International Conference on Cloud and Service Computing*, IEEE Computer Society, Washington DC, 1-10.

[7] Liang, C., Zhang, Y. and Han, Z.H. (2013) Quantitatively Measure Access Control Mechanisms across Different Operating Systems. *7th International Conference on Software Security and Reliability*, Beijing, 18-20 June 2013, 50-59. https://doi.org/10.1109/sere.2013.12

[8] Berger, S., *et al.* (2006) vTPM: Virtualizing the Trusted Platform Module. Security'06: 15*th USENIX Security Symposium*, Vancouver, BC, 31 July-4 August 2006, 305-320.

[9] Brohi, S.N., Bamiah, M., Brohi, M.N. and Kamran, R. (2012) Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures. *Proceedings of International of Cloud Computing, Technologies, Applications & Management*, 151-155.

[10] Griffin, J.L., Jaeger, T., Perez, R., Sailer, R., van Doorn, L. and Cáceres, R. (2005) Trusted Virtual Domains: Toward Secure Distributed Services. *The 1st Workshop*

on Hot Topics in System Dependability, Yokohama, 30 June 2005, 1-6.

[11] Iqbal, A., Pattinson, C. and Kor, A.-L. (2015) Performance Monitoring of Virtual Machines (VMs) of Type I and II hypervisors with SNMPv3. *World Congress on Sustainable Technologies* (*WCST*), Leeds, 14-16 December 2015, 98-99.