Cloud Computing Security Breaches in Bare Metal Hypervisors

Manasamithra P* and Prasana B T**
*M.Tech Student, Dept. of CSE, JSS Science and Technology University, Mysuru, Karnataka, INDIA
manasamithra.1@gmail.com
** Asst.Professor, Dept. of CSE, JSS Science and Technology University, Mysuru, Karnataka, INDIA
prasi.bt@gmail.com

Abstract: Cloud computing is a buzz word in the IT industry. Cloud significantly reduces OPEX and CAPEX. A technique called Virtualization is used to make cloud realizable to achieve much higher performance. One of the methods used to achieve virtualization in cloud is Hypervisor or Virtual Machine Monitor layer. Along with the benefits of virtualization there is also a risk associated with it. One among many risks is security. In this paper different types of security issues related to Hypervisor layer of the cloud is discussed and categorized.

Keywords: Cloud, Hypervisor, OPEX, Virtualization, Virtual Machine Monitor.

Introduction

Cloud computing is the service that provides the computing resource on demand over the internet on pay per use basis. Some of the important properties of cloud computing are elastically, measured service, on demand self service etc. Since cloud computing is used for reducing the infrastructure cost, there should be some way in which we should minimize the number of resources used through clod computing. The resources should also be available ubiquitously even though resources used are less in number. The technology that supports 24/7 service with very less infrastructure cost is virtualization. If we have not used this technology, then cloud computing would not have been served the original purpose for which it has been evolved.
The remainder of the paper is organized as follows. Section 2 provides an brief overview of Virtualization and Hypervisors and Section 3 explains about different categories of Hypervisor Security issues followed by conclusion and references in Sections 4 and 5.

Virtualization and Hypervisors

Virtualization is the illusion of creating instance of the available resources, such as server, storage, network etc. Virtual Machine (VM) is the simulated environment that runs on dedicated hardware. Basic virtualization technology is explained in Figure 1.
Hypervisor is the software program that enables the virtualization. It is an interface between host hardware resources and Virtual Machines providing services of host machine to VMs. It is also called as Virtual Machine Monitor(VMM). Examples are Xen, VMware ESX / ESXi, Microsoft Hyper-V etc.
There are two types of Hypervisors namely Type1 Hypervisor or Bare Metal Hypervisor and Type2 Hypervisor or Hosted Hypervisor.
Type 1 Hypervisor run directly on host machine's hardware. These hypervisors are more efficient and secure. It works as shown in Figure 2.
Type2 Hypervisors run on host operating system. These are rarely used type of hypervisors. It supports guest virtual machines by coordinating calls for CPU, memory, disk, network and other resources through the physical host's operating system. Examples for this type include VMware Fusion, Oracle Virtual Box, Oracle VM for x86, Solaris Zones, Parallels. The working of Type2 Hypervisor is shown in Figure 3.
Virtualization using Hypervisors has many advantages as well as challenges. One challenge that needs to be taken care before using virtualization is security.

Type 1 Hypervisor Security Breaches in Hypervisor

Hypervisor is the main component of virtualized system and responsible to enforce isolation between virtual machines and resource management of hardware. It is the main controller of any access to the physical server resources by VMs. The security breaches on Hypervisor layer are categorized into two categories, based on the functionalities the Hypervisor provides and the weak implementation of Hypervisors. Figure 4, 5 and 6 shows overview of security categorization.

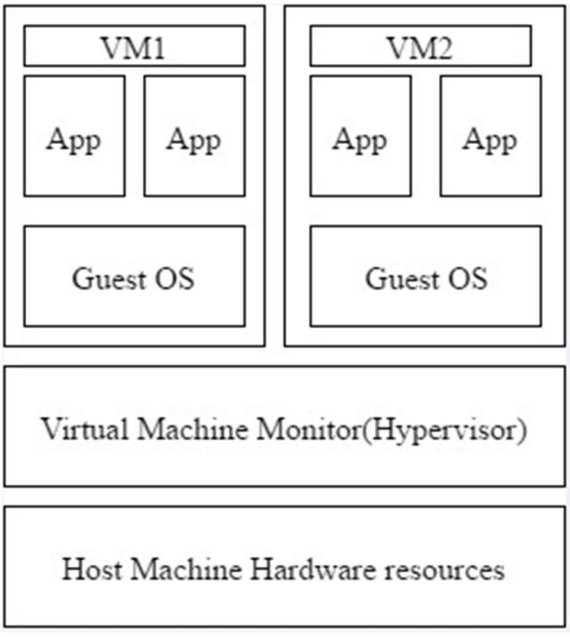

Figure 1. Virtualization

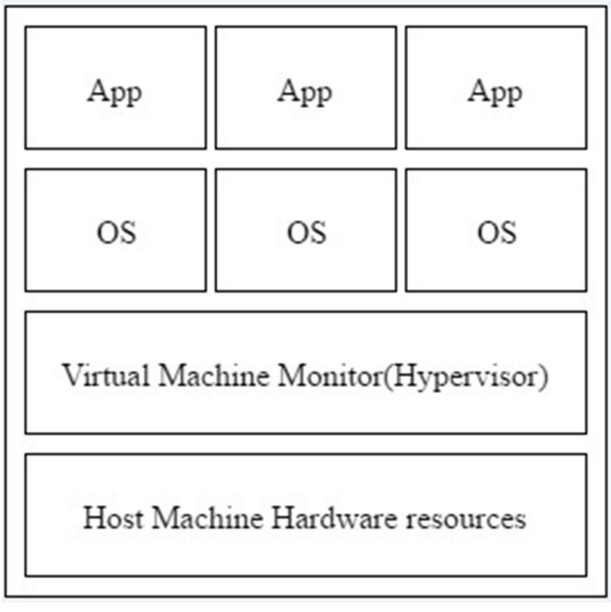

Figure 2. Type 1 Hypervisor

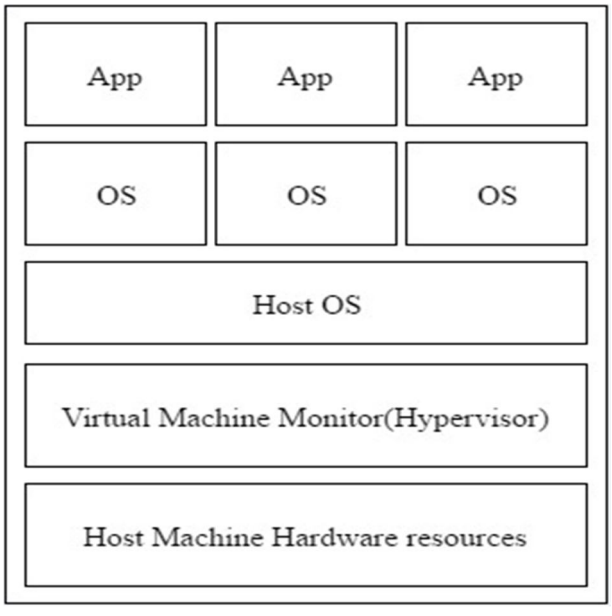

Figure 3. Type 2 Hypervisor

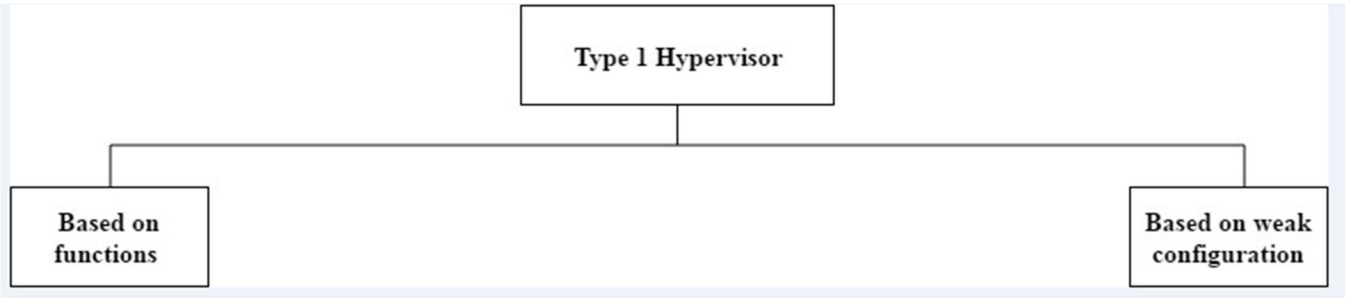

Figure 4. Categorization of Hypervisor vulnerabilities

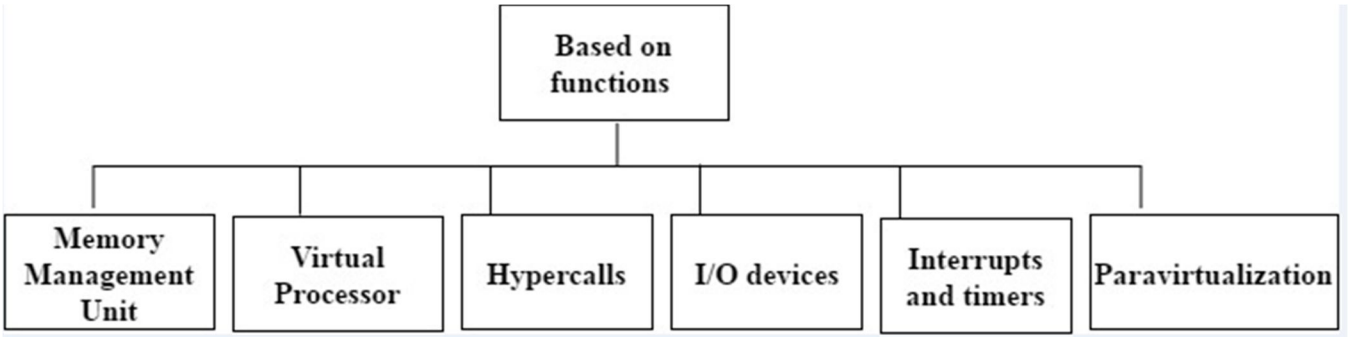

Figure 5. Categorization based on functions of hypervisor

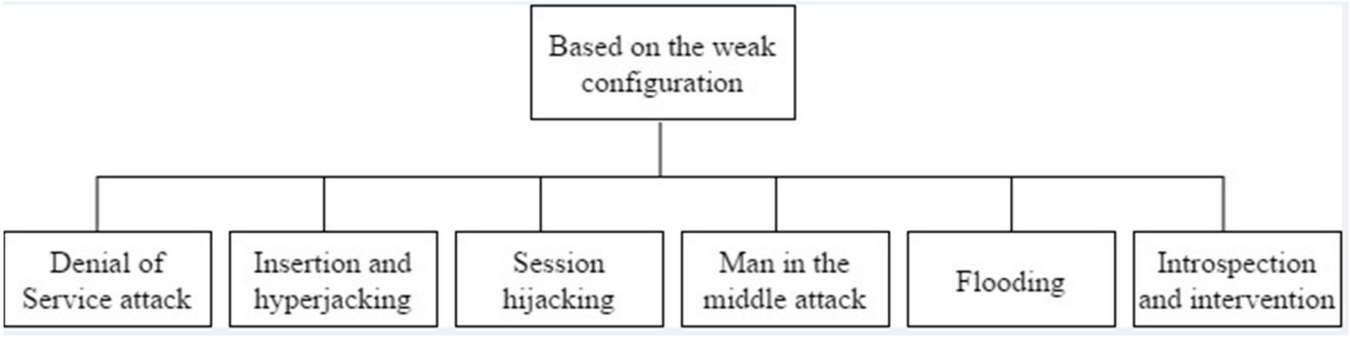

Figure 6. Categorization based on weak configuration of hypervisor

Security breaches according to their functionalities

Memory Management Unit

Hypervisor controls the memory protection mechanism without any restrictions. Hypervisor functionalities related to memory management are the memory resource management with paging and the memory isolation through address translation. When a VM requests a memory page, hypervisor determines the page to be allocated and maintains a mapping table from guest-physical to machine address (nested page table) for each VM. Whenever a VM is scheduled to a core, the hypervisor sets the register pointing to the nested page table for the VM, so that the hardware TLB walker can access the appropriate mapping table [3]. The memory of guest virtual machines will be completely exposed to the attacker if hypervisor is attacked successfully. In other words it discloses the data in arbitrary address space such as other VM's address space or hypervisor memory segment to the attacker.

Virtual Processors

The first and most important functionality of hypervisor is to provide the physical processor cores to the virtual machines that have been created. Hypervisor provides as many virtual processors to the guest VMs as there are cores on the actual host hardware. One of the advantage of virtual processor is that provides isolation of Instruction set architecture. Emulating the functionalities of processor core is also a service provided by the hypervisor. It dynamically schedules the VM to the processor cores and run scheduler periodically, sometimes to run its own functionalities. Here Simultaneous multiprocessing vulnerabilities will arise because of the Hypervisor code assumptions that hold true on single threaded processes. Also virtual processors disclose the hypervisor memory contents because of an incomplete initialization of the virtual processor data structures. Given that the memory for the data structure is allocated in kernel space, the padding held might end up containing information from data structures previously used by the Hypervisor [5].

Hypercalls

We have seen that virtual processors provide isolation of instruction set. It means that certain processor instructions can be executed only by the operating system because they are privileged instructions. That is hypervisor and VM run as applications. So if one of the guest operating system wants to execute such privileged instructions, then those instructions will be trapped by virtual processor in VM and a call is made to hypervisor. Sometimes, hypervisor itself handles this or it can pass this to the host operating system, and then emulates the response of host in the virtual processor. Hypercalls are responsible for invoking the host operating system for running the privileged instructions. Attackers could exploit Hypercalls

to open new attack vectors. Hypercall interface can also be exploited to inject malicious code into the VMM. If the attacker compromises one of the applications on a guest OS, they could be infected with malware.

I/O devices
Hypervisor provides the instance of host operating system to all virtual machines. Similarly, it should also provide the instances of input and output devices to the VMs. In some cases, it may directly provide the physical devices in which hypervisor need not emulate the functionalities of the I/O devices. Here only provisioning and de provisioning of the device is necessary. In both cases, Peripheral Component Interconnect will be emulated. The guest OS running in the VM interacts with PCI during boot up to discover and configure available resources. In some cases, devices can be added while the VM work is in progress which is called as hot unplugging [1]. But sometimes hot unplugging is not supported by the system. Therefore, the lack of state cleanup by some virtual devices resulted in use-after-free opportunities, where data structures that were previously being used by a hot-unplugged virtual device remained in memory and could be hijacked with executable code by an attacker.

Interrupts and Timers
The hypervisor must also emulate the interrupt subsystem and timers for the guest VMs. For interrupts, the main parts of the underlying hardware interrupt subsystem emulated by the hypervisor include the I/O APIC1 (which routes interrupts from devices to processor cores) and local APICs (which are attached to each core as an interface to the interrupt subsystem for sending and receiving interrupt messages to and from other local APICs or the I/O APIC). These APICs are emulated so the guest OS can use them to configure and manage interrupts inside the VM, while physical APICs are controlled by the hypervisor for the management of the physical platform. For timers, since the hypervisor utilizes the physical timer devices to get periodic clock ticks itself, it has to emulate the timer device for each guest VM [2]. Today, VMs can be scheduled on different cores and as such, the interrupts and timers must first go through the hypervisor which will deliver the interrupts to the VM by utilizing its knowledge of the VM's current location. Lack of validation of the data contained in the PIT-related data structures enabled a rogue VM to cause a full host OS crash, a serious denial of service attack [1].

Paravirtualization
Recent technology supports paravirtualization by the hypervisor. Here the guest OS is aware of it is running in a virtualized environment. Virtualized resources, such as virtual network and storage devices, can be accessed directly without the need for virtual device drivers. The main disadvantage of paravirtualization is the need to modify the guest OS kernel space. This modification is applied all the supported VMs. This will cause the Denial of service in paravirtualized front end drivers [6]. While performing the modification, attacker possibly executes arbitrary code which requires privileges.

Security breaches according due to weak implementation of hypervisor

Denial of Service attack
This type of attack in cloud environment is very harmful. This is caused by the Misconfigurations of the hypervisor that makes single VM to consume all the available resources and making remaining VMs to starve which are running on the same host machine. Due to this type of attack, network hosts will function abnormally due to the hardware resource storage[3].

VMM Insertion and Hyperjacking
Various methods exist for covert insertion of a VMM under an OS, moving the OS from physical to virtual nearly undetectably, either on boot or while the system is running. These VMM rootkits are a serious security risk, as they may be used to subvert an operating system completely. The methods used to accomplish the VMM insertion are varied. Two methods used include the use of raw disk reads to alter device drivers that are paged out to disk, and the modification of system startup files.

Session hijacking
Here attacker tries to hijack the session of the host machine on which hypervisor is running so that attacker get all access to the management environment i.e. hypervisor. Once hypervisor is compromised, all VMs can be easily copied and modified. It leads to confidentiality breaches by compromising cryptographic keys.

Man in the middle attack
This is done by placing an attacker machine in between two VMs so that messages sent from the sender passes through attacker machine via ARP spoofing technique. When VM is compromised, attacker gets access to the hypervisor in turn to host machine. IDS hypervisor can detect this type of attack. It breaches confidentiality, integrity and authenticity.

Flooding

Infinitely large number of service requests to hosts through locally attacking the hypervisor is known as flooding. Hypervisor should check the assignment of instances of host machine to the VMs regularly. Eavesdropping of the hypervisor is also possible in this type of attack.

Introspection and Intervention by hypervisor

VMM will observe behavior of processes within the VM. The VMM may also observe I/O channels to, from, and within the VM. This is due to the resource control property of virtualization, and has associated information security issues that can both improve and threaten security.

Conclusion

Cloud computing is the most emerging field in computer science. Virtualization is the technology which helps in bringing the cloud computing benefits. Hypervisor is the software program which implements the virtualization. There are different types of hypervisor. But using the hypervisor brings many security issues in the virtualized environment. In this paper, an overview of security breaches in hypervisor layer is explained based on the services provided by hypervisor and the attacks caused due to weak configuration. Here totally twelve possible security issues are explained, that can happen in the virtual machine management layer.

References

[1] Diego Perez-Botero, Jakub Szefer and Ruby B. Lee; Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers, Princeton University, Princeton, NJ, USAdiegop@cs.princeton.edu,{szefer,rblee}@princeton.edu in in Proceedings of the Workshop on Security in Cloud Computing (SCC), May 2013.

[2] Gabriel Cephas Obasuyi, Arif Sari The Management Centre of the Mediterranean, Nicosia, Cyprus, Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment, published 17 July 2015.

[3] W. Dawoud, I. Takouna, and C. Meinel. Infrastructure as a service security: Challenges and solutions. In Proceedings of the International Conference on Informatics and Systems, INFOS, pages 1 - 8, March 2010.

[4] Seongwook Jin and Jaehyuk Huh; Secure MMU: Architectural Support for Memory Isolation among Virtual Machines, Computer Science, KAIST (Korea Adanced Institute of Science and Technology), 2011.

[5] Jakub Szefer, Eric Keller, Ruby B. Lee and Jennifer Rexford Princeton, Eliminating the Hypervisor Attack Surface for a More Secure Cloud University Princeton, NJ, USA {szefer, ekeller, rblee, jrex}@princeton.edu, 2011.

[6] Cuong Hoang H. le , Protecting Xen hypercalls Intrusion Detection/ Prevention in a Virtualization Environment,THE UNIVERSITY OF BRITISH COLUMBIA (Vancouver) July, 2009 °c Cuong Hoang H. Le 2009.

[7] Virtualization: Issues, Security Threats, and Solutions MICHAEL PEARCE, The University of Canterbury SHERALI ZEADALLY, University of The District of Columbia RAY HUNT, The University of Canterbury, 2013.