Virtualization Layer Security in Cloud Architecture

S. Jyothsna
Department of IT, CVR College of Engineering, Ibrahimpatnam, Hyderabad, India
Email:jyothsna.sundaragiri@gmail.com

Abstract: **Cloud Computing is a type of service based computing or utility computing. Cloud computing is based on virtualization technology. Virtualization architecture is categorized as hypervisor architecture, para virtualization and host based virtualization depending on the position of the virtualization layer. The hypervisor supports hardware-level virtualization on devices like CPU, disk, memory etc. The hypervisor provides hyper calls for the guest operating systems and applications. The architecture of processor supports the ability to run number of virtual machine instructions on one CPU after virtualization. Virtual machine instructions can be categorized as privileged and unprivileged instructions. Privileged instructions must be run in supervisor mode in Hypervisor. To provide reliable computing in cloud, virtualization layer security is a major concern. Hypervisor is a program responsible for allocation and de allocation of resources to each virtual machine (VM) connected to the cloud. Hypervisor security compromise affects all the privileged and sensitive instructions. Hypervisor is very small program compare to the operating system so it is easy to attack . A set of additional instructions must be added to control the hypervisor attacks and regular CPU state checking must be done in each virtual machine.**

Index terms: **cloud computing, virtualization, hypervisor, virtual machine, virtual machine monitor, hypervisor security**

I. INTRODUCTION

1.1 Cloud Computing

A Cloud can be considered as an enormous collection of resources. Cloud computing is providing easy accessibility for required services and users can also deploy applications at competetive costs. Large data centers provide services through virtualized cloud platforms. Cloud computing is providing services at infrastructure level are called as infrastructure as a service.

The cloud service provider (CSP) provides on demand provisioning of Hardware like processing power, I/O, large amounts of storage etc... By utilizing virtualization, each user accesses the services of cloud through a virtual machine, where number of virtual machines shares a single physical server. cloud computing provides a service oriented platform for cloud users.

1.2 Security in Virtualized Environment

The main idea of virtualization technology is to separate the hardware from software to improve efficiency of the system. The Cloud Service Provider provides the infrastructure usually in the form of virtual machines to manage compute resources efficiently. The virtualization software creates the images of computer system at application level is called a virtual machine(VM).Each user's application runs virtually on their VM, but VM cannot run instructions directly, most of the unprivileged VM instructions are executed directly on the host processor,these instructions must be handled carefully to avoid vulnerabilities and maintain stability of the system.

Virtualization Layer is the critical element of cloud computing, VMM (virtual machine monitor) is responsible for creation of virtual machines, resource allocation to virtual machines, isolation of virtual machines from each other etc.., virtualization improves resource utilization but security risk also increases, to provide an efficient cloud environment more standard security mechanism is required at virtualization layer.

1.2.1 Customers in Cloud Attack Vectors

The fig. 1 shows the customer environments 1 and 2 connected to the common cloud, where customer 2 being the attacker (red), and customer 1 being the victim (green).

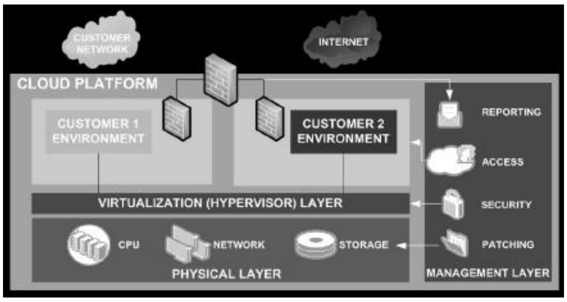

Fig. 1. Customer Environments Connected to Common Cloud

In this case, customer 1 also connects its own internal network (a situation common for many IaaS solutions). The parts shown in blue are managed by the Cloud Service Provider (CSP).

The attacks in cloud can be any of the following

1. Hypervisor/Virtualization Layer Attack, which is the focus of this paper.
2. Management layer vulnerabilities (blue)
3. External attacks from Internet (red)
4. Internal customer network threats

In multi processing environment more standard protection mechanism is mandatory to avoid system crash because direct accessing of hardware may take place by processes. Therefore, all processors have at least two modes, user mode and supervisor mode to ensure controlled access of critical hardware. There are relatively more layers in the machine stack in a virtualized environment so it is more difficult to make operating systems and applications run correctly.

DOI:10.32377/cvrjst0813

II. Hypervisor Architecture

2.1 Hypervisor

The hypervisor is a virtual layer between the physical hardware and its operating system, in cloud architecture virtualization software (ex. xen) is used to create virtual machines. Virtual machines may run on different operating systems such as linux and windows, i.e. different operating systems run on the same physical hardware simultaneously. converting portions of the real hardware into virtual hardware is the major responsibility of virtualization layer . Hypervisor may be placed above hardware as a separate layer or as part of real operating system.

The Hypervisor supports hardware-level virtualization on CPU, memory, disk and network interfaces. The hypervisor provides hyper calls for the guest operating systems shown in figure 2.

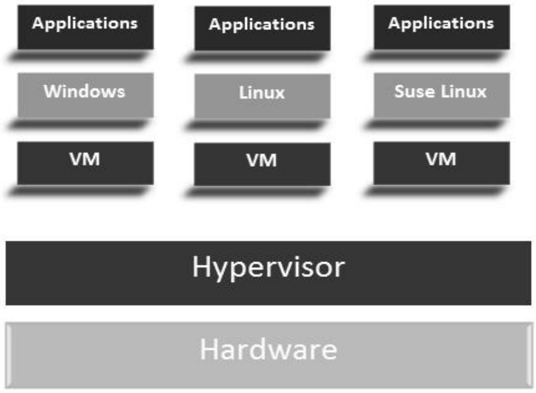

Fig. 2 Hypervisor Architecture

2.2 Hypervisor Design Goals

This virtualization layer is referred to as either the VMM or the hypervisor. Depending on the functionality, a hypervisor can assume micro- kernel architecture like the Microsoft Hyper-V or it can assume monolithic hypervisor architecture like the VMware for server virtualization.

Hypervisor provides

- Physical memory management
- Processor scheduling
- Converts physical devices into virtual resources

Virtual layer is responsible to distribute and assign resources to virtual machines in cloud environment. At the cloud layer, sets of virtual devices are sandboxed and offered to clients as if they were completely separated data centers. Thus, cloud computing is very dependent on the quality of the hypervisor security. The hypervisor provides a very strong barrier between virtual machines and thus between different customers.

2.3 Virtualization Networking

Xen Server and VMware ESX Server are virtualization platforms and supports a bridging mode which allows all domains to appear on the network as individual hosts. By using this mode, VMs can communicate with one another freely through the virtual network interface card and configure the network automatically.

In a network built with mixed nodes of host and guest systems, the normal method of operation is to run everything on the physical machine. When a VM fails, its role could be replaced by another VM on a different node, as long as they both run with the same guest OS. The Potential drawback is that a VM must stop playing its role if its residing host node fails.

VMs can be live-migrated from one physical machine to another. Virtual clusters can be applied in Cloud Platforms. Virtual clustering plays a key role in cloud computing. The virtual clustering provides dynamic resources that can be quickly put together upon user demand or after a node failure. When a VM runs a live service, the following three metrics must be considered.

1. Negligible downtime
2. Lowest network bandwidth consumption
3. Reasonable total migration time

Furthermore the migration must ensure that it should not disrupt other active services residing in the same host through resource contention.

A migrating VM should maintain all open network connections without relying on forwarding mechanisms on the original host or on support from mobility or redirection mechanisms. To enable remote systems to locate and communicate with a VM, each VM must be assigned a virtual IP address known to other entities. This IP address can be distinct from the IP address of the host machine where the VM is currently located. Each VM can also have its own distinct virtual MAC address. The VMM maintains a mapping of the virtual IP and MAC addresses to their corresponding VMs.

Xen as a VMM allows multiple operating systems to share x86 hardware in a safe and orderly fashion. Xen supports live migration. It is a useful feature and natural extension to virtualization platforms that allows for the transfer of a VM from one physical machine to another with little downtime of the services hosted by VM. Xen Hypervisor uses a send/recv model to transfer states across Virtual machines.

2.4. Preventing Hypervisor Attacks

Guest hopping and hijacking or VM root kits are the major attacks in virtual layer (hypervisor) along with buffer overflows, distributed denial of service attacks in a cloud environment, another type of attack is the man-in-the-middle attack for VM migrations. Virtualization enhances resource provisioning in cloud but virtual machines add an additional layer of software that could become a single point of failure.

To prevent from failures

- Use redundant utilities at multiple sites
- Alternate network connections
- Multiple databases at separate sites
- Data watermarking and user authentication...
- Trust delegation and negotiation

DOI:10.32377/cvrjst0813

- All datacenters can be secured from distributed denial of service attack by distributed defence and internet worm containment.
- Fine grained access control at file or object level.
- Use double authentication, biometric identification, intrusion detection and disaster recovery etc... for privacy protection

III. Implementation of Hypervisor

The Hypervisor is a program executed by the server. When hypervisor is executed it loads the client operating systems of the virtual machines. The hypervisor allocates the correct CPU resources, memory, bandwidth and disk storage space for each virtual machine.

The main function of the VMM is to virtualize the physical hardware of a host machine into virtual resources to be used by the virtual machines. This can be implemented at various levels.

There are two types of hypervisors:

1. Bare metal or native hypervisors
2. Embedded or hosted hypervisors

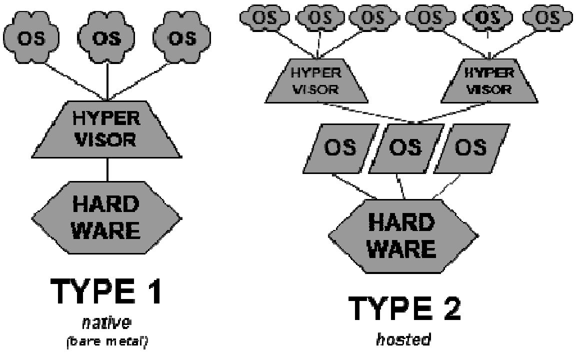

Fig. 3 Hypervisor Types

A virtual machine can create requests to the hypervisor through a variety of methods, including API calls.

3.1 Bare Metal or Native Hypervisors

This is also called as full virtualization. In this, non critical instructions are discovered and replaced with traps in to the VMM to be emulated by software. Non critical instructions do not control hardware or threaten the security of the system, but critical instructions do. Therefore running non-critical instructions on hardware improve efficiency by ensuring security.

The method used in this emulation is called binary translation. Binary translation is time consuming and increases the cost of memory usage. (To store translated instructions in cache). The Performance of full virtualization may not be ideal.

3.2 Host-Based Virtualization

In Host-Based virtualization, hypervisor is installed on top of host operating system. This host operating system is responsible for managing hardware. The guest operating systems are installed and run on top of the hypervisor. Dedicated applications may run on the virtual machines. Some other applications can also run with the host operating system directly.

Host based virtualization have following advantages

- The user can install VM architecture without modifying host operating system.
- Host based approach appeals to many host machine configurations.

The host based architecture has flexibility but the performance of the host based architecture also may be low because it involves four layers of mapping when an application requests hardware access.

IV. Security At Hypervisor Layer

Many guest Operating systems can run on top of the hypervisor, one among those guest operating systems controls the others. This is called as Domain O, and the others are called Domain U in Xen. Domain O is the privileged guest operating system, which access the hardware resources directly, if Domain O is compromised, the hacker can control the entire system.

The processor power of the hardware is distributed among virtual machines belonging to different customers by the hypervisor layer. Hypervisor does not function natively on the host and can only access host resources through a separate control layer commonly named the virtual machine monitor (VMM).

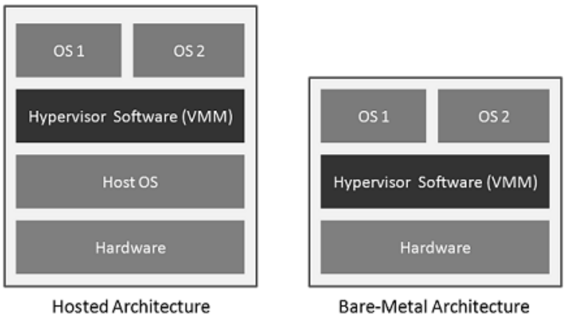

Fig. 4 VMM Architecture

There are four major levels in security management of hypervisor as mentioned below:

*Attribute based Authentication***:** Just-in-time tokens must be generated for users accessing applications of each guest OS separately for each access based on the attributes of application

Controlled Authorization: A model that includes pre-defined application roles and user roles and API based on user-role bindings only can be used to access.

Minimized Hypervisor Intervention: Hypervisor should be responsible for the creation of virtual machine, allocation of resources to virtual machine and shutting down of virtual machines only but runtime intervention of the hypervisor must be restricted i.e. resource allocation to virtual machines must be static so that security compromise of virtual machine monitor may not effect virtual machines.

DOI:10.32377/cvrjst0813

Secure Code Execution: onion routing can be used to execute each virtual machine's code .Onion routing is a technique where messages are encapsulated in layers of encryption, The encrypted data is transmitted through a series of nodes from each virtual machine to datacenter in cloud.

Security Recommendations for Hypervisor Security

1. Resource allocation, processor core assignment and input/output calls must be done statically for each virtual machine to avoid active interaction with virtual layer.
2. Standard public key encryption techniques like RSA should be used to access management layer.
3. Every virtual machine data transmission activity must be controlled by VM Security Monitor (VSEM).
4. Clear segregation of security zones should be provided in the cloud environment for each virtual machine.
5. Standard encryption systems which can efficiently encrypt large volumes of data at boot level is preferred.
6. Memory regions of hypervisor can only be modified by instructions that are intended part of the hypervisor.

V. CONCLUSIONS

Cloud Computing is based on the virtualization technology, Virtualization provides more resources than actually available by multiplexing virtual machines into single hardware. Hypervisor based virtualization creates a new layer between the hardware and host operating system. The virtualization layer called virtual Machine Monitor (VMM) actually accesses the real hardware to provide infrastructure services to cloud users. Each client connected to the cloud, uses their own guest operating system for its functionality. VMM security compromise may affect all virtual machines. So that standard security mechanism must be provided to VMM to achieve reliable services of cloud.

REFERENCES

[1] Kai Hwang. Geoffrey C.Fox. Jack J.Dongarra (2012) - Distributed and cloud computing, Mogan Kaufmann publishers

[2] "Cloud_Security_demystified", CSC

[3] http://cybersecurity.mit.edu/2013/10/virtualization vulnerabilities-related-to-hypervisors/

[4] "Cloud Security Is Not (Just) Virtualization Security",Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales.

[5] "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology" - Farzad Sabahi, Member, IEEE

[6] "An Architecture for Concurrent Execution of Secure Environments in Clouds", Ramya Jayaram Masti, Claudio Marforio, Srdjan Capkun

[7] http://www.cpd.iit.edu/netsecure 08/ROBERT_RANDELL.pdf

[8] https://www.ernw.de/download/ERNW_DCVIH ypervisors To Clouds.pdf

DOI:10.32377/cvrjst0813