International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 5 Ver. III || May 2018 || PP 51-55

A Study On Virtualization And Virtual Machines

G. Sunitha Rekha

Information Technology, CVR College of Engineering/JNTUH, Telangana, India
Corresponding Author: G. Sunitha Rekha

Abstract : *Cloud computing is the one among the emerging technologies in the present world, It is mainly concerned with storage of data, providing on demand computing infrastructure for various applications. The users can store their data in cloud and can access that data very easily and fastly. Cloud data can be retrieved from anywhere and whenever users want because of this flexibility now a days many users are attracted to this technology, but the problem with this environment is privacy of users data. As the data of different users is stored in the same place, the users are worried about their data privacy. Virtualization is a type of process used to create a virtual environment to identify and isolate the user's data. It allows a user to run multiple operating systems on one computer simultaneously by creating virtual version of an operating system, server or network resources. Virtualization allows running multiple servers on a single machine while isolating servers from one another because they are running on separate virtual machines.*

Keywords: *Operating system, Servers, Security, Virtualization, Virtual machine.*

Date of Submission: 07-05-2018 Date of acceptance: 22-05-2018

I. Introduction

Cloud computing incorporates virtualization, on demand deployment, Internal delivery of services and open source software. Virtualization [9] [10] is very important for the cloud computing because this layer is responsible for maintaining virtual servers and it hides the physical characteristics/properties of computing resources. Cloud virtualization is very popular for its scalability, virtual servers are allocated with enough computing power and storage capacity that the client needs, but as these virtual servers grows more power and capacity is needed. The processing power and the storage capacity can be allocated to the servers or it can be lowered if needed. The customer pays only for their usage, this can be very affordable for most of the clients. This paper discusses about virtualization and its types, how vm's are attacked at virtualization level and the attacks at this level.

1.1 Virtualization Architecture

Virtualization comes in different forms. They are distinguished primarily by the layer in the computing system to which virtualization is applied. However, all virtualization forms have an entity called a hypervisor or virtual machine monitor (VMM). It is the central unit that controls how virtualized programs interact with the underlying layer of resources. In a sense, it is the administrator of a virtualized environment. Application virtualization is a virtual implementation of the application programming interface. It enables programs to run on different platforms by providing the common virtual API. Operating system virtualization is a virtual implementation of an operating system (OS) where programs written for that OS can run. Despite the common appearances of the virtualization forms mentioned above, most modern data centers and clouds utilize a form known as full virtualization, which comes in two different types [1].

Native virtualization

In this type of virtualization, the hypervisor is directly implemented on the hardware or the computer firmware without any host OS. Each instance that runs on the virtual hardware is called a guest OS or VM. The hypervisor allocates resources between the VMs. Fig.1 shows a high-level architecture of native virtualization.

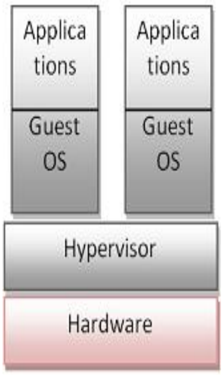


Figure 1: Native Virtualization Architecture

Hosted virtualization

In this, the hypervisor runs on a host OS that manages the hardware resources. The hypervisor still manages the guest OSs or VM, except the hypervisor is treated as an application on the host OS. Fig.2 shows a high-level architecture of hosted virtualization

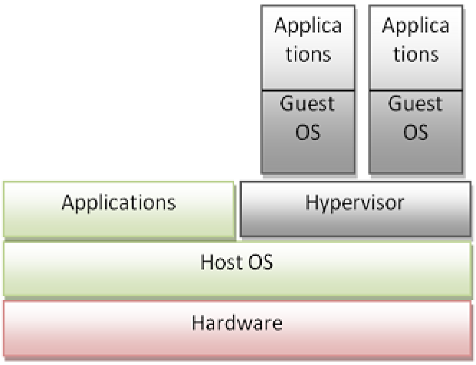


Figure 2: Hosted Virtualization Architecture

1.2 Benefits of virtualization

- Lower costs
- Better backup and disaster recovery
- Faster deployment of new applications
- Better migration to the cloud
- Centralized management

II. Different Methods Of Virtualization

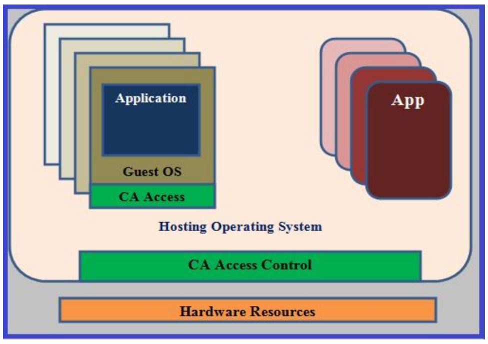
Virtualization is a layer that exists between the physical hardware and the operating system. A virtual infrastructure provides powerful computing that maximizes resource utilization and cost savings. Virtual machines are the key elements to virtual infrastructure. Virtualization allows us to run multiple virtual machines with heterogeneous operating systems and application to run in isolation on the same machine.

There are 3 Methods of virtualization

1. Operating system based virtualization
2. Hypervisor based virtualization
3. Application based virtualization

1. Operating system based virtualization

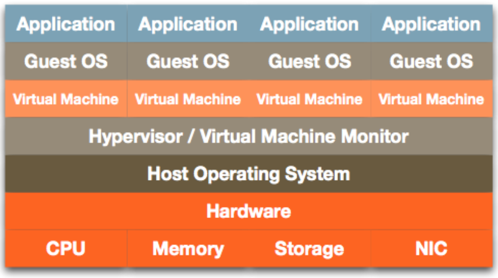
In OS based virtualization, we install the software on the top of the guest OS on host OS, but with each guest, OS have its own resources and are running in complete isolation from the other guest OS as OS based virtualization models.



ting system-based virtualization

2. Hypervisor based virtualization

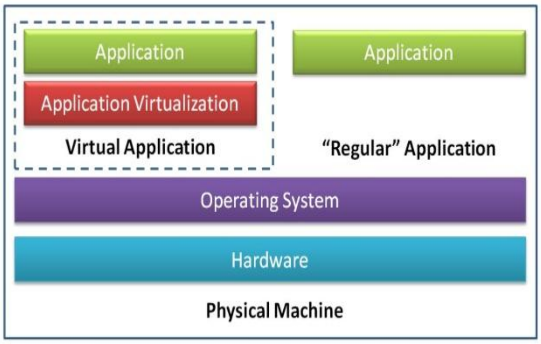
A hypervisor separates operating system (OS) and hardware in order to share the hardware among multiple virtual machines (VM), each running an isolated instance of an OS that caters for the execution of a subset of applications [2]. The resulting consolidation of multiple systems with maintained separation and resource partitioning is well-suited to combine independently developed software into a system of systems.



(c) Hypervisor-based virtualization

3. Application based virtualization

Application virtualization is layered on top of other virtualization technologies, such as storage virtualization or machine virtualization to allow computing resources to be distributed dynamically in real time. In standard computing, applications install their settings onto the host operating system, hard-coding the entire system to fit that application's needs. With application virtualization, each application brings down its own set of configurations on-demand and executes in a way so that it sees only its own settings. This leaves the host operating system and existing settings unaltered.



(c) Application-based virtualization

III. Virtualization Concerns

3.1 Virtualization and VM's

Virtualization enable single system to concurrently run multiple isolated virtual machines. If isolation of these Vm's is not properly implemented, intruders may perform unauthorized communication with other Vm's in the system. Assaulter can use Trojans, malwares etc to tamper the functionality of guest OS, they can also use viruses and worms to exploit the guest OS in Vm's. Attackers can even compromise the privileged host virtual machine Dom0 to tamper boot process of guest Vm's or access all guest Vm's including their memory, disk space and network traffic, the attacker can create multiple virtual machines to consume all the system resources simply by controlling Dom 0. The saved state of guest VM appears as a disk file in plain text to Dom0[8].

3.2 VM Sprawl

The single biggest vulnerability of VMs is due to the ease in which users can create many VMs, which become very difficult to secure, monitor, and maintain. VMs can be created and deployed in a matter of seconds, which is significantly smaller than the time to ensure that all VMs are up-to-date and secure. Traditional security methods need to be applied to each VM because the guest OS accesses the network directly [3]. A compromised VM is a potential entry point for attackers to the hypervisor and host [4]. There are significant manual processes each time a VM is made. Most current security products are not designed for efficient use in securing many VMs on the same physical server, but this is a problem many software companies are working on. In addition to creating more work for security administrators, VM sprawl wastes resources and creates more entry points for attackers [5]. An obsolete VM becomes an easy entry point for attackers, who could potentially access the hypervisor, other VMs, and the host OS.

3.3 Denial of service

DoS attacks try to render the service unavailable to its users. The attack consumes large amounts of system resources such as processing power, memory, and bandwidth. This consumption will leave the service inaccessible to the users or intolerably slow. An attacker aims to exhaust the resources from a physical host in order to deny service to the other VMs in the machine preventing the other VMs from running correctly [2], [6]. For example, In TCP SYN Flood attack [14] one victim machine receives more TCP-SYN requests than its capacity, so that other machines requests could not be served by the main host in the cloud environment. Fortunately, the solution is simple. Hypervisors prevent any VM from gaining 100% usage of any resources, including CPU, RAM, network bandwidth, and graphics memory. Additionally, the hypervisor can be configured so that when it detects extreme resource consumption, it can evaluate whether an attack is being made and automatically restart the VM. VMs can usually be initialized much faster than physical machines because their boot sequence does not need to initialize and verify hardware, so restarting the VM has a smaller effect than restarting a physical machine.

3.4 VM Escape Attack

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker access to the host operating system and all other virtual machines (VMs) running on that host. Although there have been no incidents reported in the wild, VM escape is considered to be the most serious threat to virtual machine security [13].

Virtual machines are designed to run in self-contained, isolated environments in the host. Each VM should be, in effect, a separate system, isolated from the host operating system and any other VMs running on the same machine. The hypervisor [11], [12] is an intermediary between the host operating system and virtual machines. It controls the host processor and allocates resources as required to each guest operating system.

If the attacker can compromise the virtual machines, they will likely have control of all of the guests, since the guests are merely subsets of the program itself. Also, most virtual machines run with very high privileges on the host because a virtual machine needs comprehensive access to the host's hardware so it can then map the real hardware into virtualized hardware for the guests. Thus, compromising the virtual machine means not only that the guests are goners, but the host is also likely lost."

To minimize vulnerability to VM escape

- Keep virtual machine software patched.
- Install only the resource-sharing features that you really need.
- Keep software installations to a minimum because each program brings its own vulnerabilities.

IV. Conclusion

Virtualization itself is not inherently unsecure, it is a technology that has new vulnerabilities and requires restructuring of manual security processes. One of the biggest challenges is to maintain and secure all of the VMs, since many instances and configurations can be rapidly created. The contents of each guest OS is a virtual disk, stored as a file. If this file is accessed, copied, or modified on the host by an unauthorized party, then the privacy and integrity of the VM is compromised. Likewise, if an attacker accesses the host and directly modifies the hypervisor, then he or she will be able to run arbitrary code, but the hypervisor has additional layer of abstraction from physical hardware and further restricts malicious attempts to control the machine from the hardware. This abstraction encapsulates malicious attacks and allows external monitoring for malicious attacks on a VM. Since the hypervisor monitors each VM, it can record the states and allow the VM to return to a previous state, which has many backup and malware removal advantages. The hypervisor should strictly control communication between VMs and limit resource consumption of each VM to a finite bound to prevent DoS attacks. All known vulnerabilities of VMs can be prevented, but it is absolutely essential to secure the host and each guest OS in order to create a secure virtual environment.

References

[1]. Hoffman, P., Scarfone, K., Souppaya, M.: Guide to security for full virtualization technologies. National Institute of Standards and Technology (NIST) (2011) 800– 125.

[2]. J.E. Smith and R. Nair, Virtual Machines. San Francisco, CA: Elsevier, 2005, pp. 369–443.

[3]. L.McLaughlin,“How to Find and Fix 10 Real Security Threats on Your Virtual Servers,” CIO, 2007.

[4]. J.Brodkin, “Virtual server sprawl highlights security concerns,” Network World, 2008.

[5]. T. Garfinkel, M. Rosenblum, “When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments,” USENIX Association, 2005.

[6]. S. N. Brohi, Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures, *International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, 2012, pp. 151-155.

[7]. M. A. Bamiah, S. N. Brohi, “Seven Deadly Threats and Vulnerabilities in Cloud Computing”, *International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 9, Issue No. 1*, 2011, pp. 87 – 90.

[8]. Kong, J.” Protecting the confidentiality of virtual machines against untrusted host”, *International Symposium on Intelligence Information Processing and Trusted Computing (*IPTC), IEEE,2010,364–368.

[9]. B. Loganayagi, S. Sujatha, “Creating virtual platform for cloud computing”, *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2010),* 28-29 Dec. 2010, pp.1-4.

[10]. Dawei Sun, Guiran Chang, Qiang Guo, Chuan Wang, Xingwei Wang., “A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques”, *First International Conference on Pervasive Computing, Signal Processing and Applications (PCSPA)*,2010, pp.305-310.

[11]. Joanna Rutkowska and Alexander Tereshkin, Bluepilling the Xen Hypervisor, *Xen 0wning Trilogy part III,Black Hat USA*, Aug 2008.

[12]. Samuel T. King, Peter M. Chen, Yi min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch,” Subvirt: Implementing Malware with Virtual Machines”, *IEEE Symposium on Security and Privacy*, 2006.

[13]. Reuben JS,” A Survey on Virtual Machine Security”, Vol. 2, Helsinki University of Technology: Helsinki, 2007, 36.

[14]. Aborujilah A, Ismail MN, Musa S. “Detecting TCP SYN-based flooding attacks by analyzing CPU and network resources performance”. In Advanced Computer Science Applications and Technologies (ACSAT), 2014 ,3rd International Conference on. EEE, 2014.

G. Sunitha Rekha" A Study On Virtualization And Virtual Machines "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 05, 2018, pp 51-55