International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
September-October-2020 Volume 7, Issue-5
Email: editor@ijermt.org www.ijermt.org

STUDY OF HYPERVISOR AND VIRTUAL MACHINE SECURITY

Anshu Mali Bhushan,
Research Scholar, Dept of Physics,
Himalayan Garhwal University

Dr. Rahul Solanki,
Associate Professor, Dept of Physics,
Himalayan Garhwal University

ABSTRACT
This article deals with the important concept in the development of hardware and software, virtualization technology. In this research paper, the topics covered are, virtualization and types of virtualization, before and after virtualization impacts, hypervisor, comparison between hypervisor types, advantages of virtualization. A hypervisor is a computer programme or software that facilitates to create and run multiple virtual machines. It is also known as Virtual Machine Manager. Due to their popularity, it exploits the attack surface, because the Hypervisor code contains much vulnerability. Since the Hypervisor is a core element of any cloud computing service, it is always on the top priority of the attackers. There are many Software (open source) and Hardware-based Solutions are available in the market to monitor and control the hypervisor activities. This paper summarizes various types of attacks, vulnerabilities, security issues and challenges related to hypervisor and virtual machines.

Keywords: Virtualization, Hypervisor, Virtual Machine.

INTRODUCTION
In computing, virtualization is known as or acts as the creation of a virtual (rather than actual) edition of something rather than the original. It is a methodology of separating the property of resources into numerous execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing and many others. In simple words virtualization is that you create a virtual version of something that's generally used for some type of execution. For example, some on wants to partition the basic hard storage drive and wants to create two hard drives, then they would be two 'virtualized hard drives,' as the hardware is technically a single hard drive that was digitally separated into two.

Virtualization allows multiple machines to run on a single Hardware. This VMM has the capabilities to share the resources of the physical machine. Resources of this physical machine are managed by the software Known as Hypervisor. Hypervisor works as an isolating layer which manages the physical hardware and the Virtual machines. This code increase attack surface, because Hypervisor has full access to Virtual machines data in CPU registers, Memory and I/O. Due to that Hypervisor is a lucrative target for the attackers. When a Hypervisor is a compromise, intruders can gain the full access of all the VMs hosted on particular Physical Machine. There are two types of Hypervisor available in Market.

(i) Type 1 Hypervisor

Type 1 Hypervisor direct installed and run on the Physical layer (Hardware). These are also known as Native Hypervisor or bare metal Hypervisor. There is no requirement of any Host Operating system. Type 1 Hypervisor has direct access and control over Hardware resources. Cloud service provider generally used this type of Hypervisor. Some of the Type 1 Hypervisor is Proxmox, VMware ESXI, and Citrix Xenserver, Ovirt, Hyper-V. In this Figure, there are showing the structure of Type 1 Hypervisor.

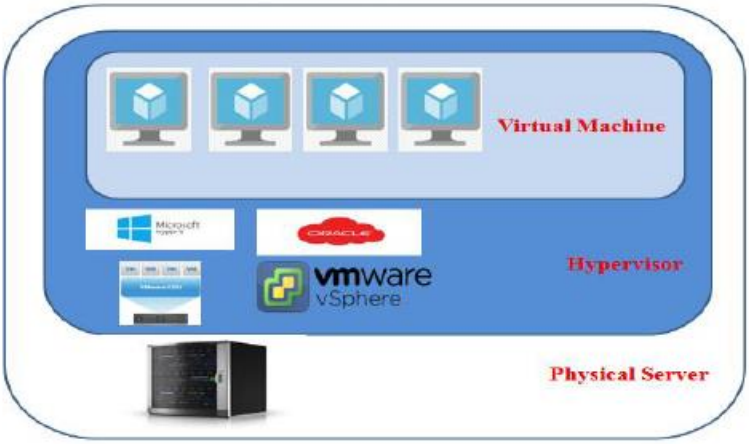

Figure 1. Structure of type 1 Hypervisor.

(ii) Type-2 Hypervisor

Type-2 hypervisor installs on Host operating system of a physical Machine. These hypervisors are also known as Hosted Hypervisor. It supports VMs by coordinating calls for CPU, memory, disk, network and other resources through the Physical host's operating system. Example of Type-2 Hypervisor is VMware Workstation and Oracle VM VirtualBox. In this Figure, there are showing the structure of Type 2 Hypervisor.

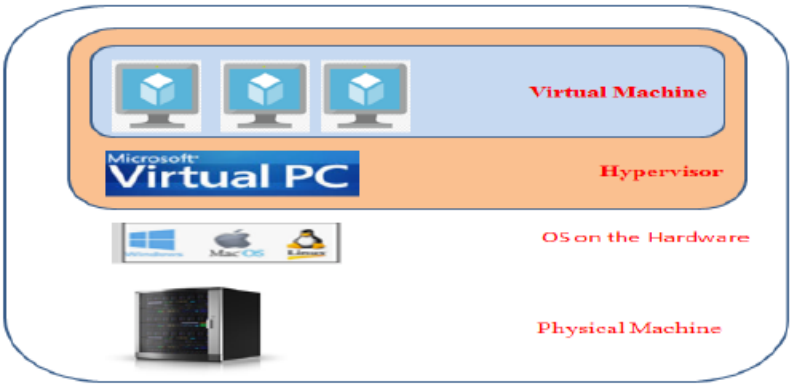

Figure 2. Structure of type 2 Hypervisor.

(iii) Hypervisor Security

Each Virtual Machine installed in the virtual environment has its security zone which is not accessed by the other Virtual Machines security zones. A hypervisor is an abstraction layer that breakup host machine from the guest machines. A hypervisor is the centralized controlling agent of all the virtual machines and has its security zone. All the security zones in the virtual environment lay within the same physical environment and same security zone .

To explore the security issues related to Hypervisor security, first, we have to know about the various privilege mode for CPU. There is three privilege level in any processor. These are shown in the Figure-3.

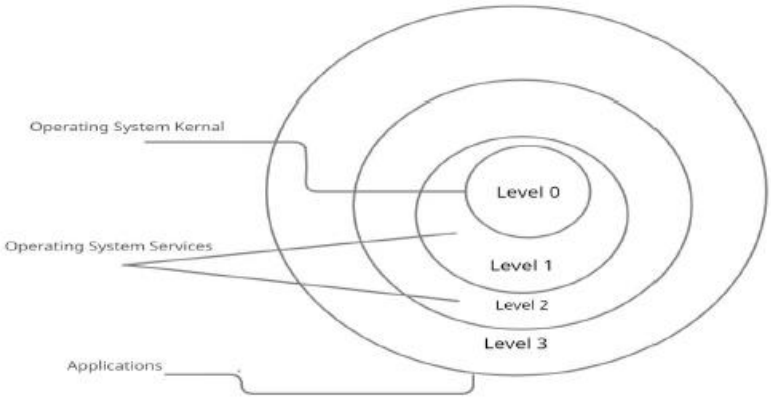

Figure 3. Privilege level in any processor.

In First case the guest machine is compromised, In second case Multiple Virtual Machines are compromised and in the third case, the Host Machine or Hypervisor compromised. First and Second case can be restored to previous well-known configuration state, but in the third case, attackers have full control of the physical hardware. According to a survey based on VMs security, it is found that around 60-65% Virtual machines which are in production are less secure than the Physical Machines because of ignoring the traditional security measure.

The attacker used the compromised guest to communicate with other guest installed on the same physical hardware. When Hypervisor has compromised then attacker it can access all the resources of guest machine and host also, He can perform the various attacks linked Denial of Service (DOS) attack and Botnet attacks.

ADVANTAGES OF VIRTUALIZATION:

There are several advantages to virtualization across several dimensions:

- Security: by compartmentalizing environments with security requirements in different virtual machines one can select the guest operating system and tools that are more appropriate for each environment. For example, we may want to run the Apache web server on top of a Linux guest operating system and a backend MS SQL server on top of a guest Windows XP operating system, all in the same physical platform. A security attack on one virtual machine does not compromise the others because of their isolation.
- Reliability and availability: A software failure in a virtual machine does not affect other virtual machines.
- Cost: It is possible to achieve cost reductions by consolidation smaller servers into more powerful servers. Cost reductions stem from hardware cost reductions (economies of scale seen in faster servers), operations cost reductions in terms of personnel, floor space, and software licenses.
- Adaptability to Workload Variations: Changes in workload intensity levels can be easily taken care of by shifting resources and priority allocations among virtual machines. Autonomic computing-based resource allocation techniques, such as the ones in, can be used to dynamically move processors from one virtual machine to another.
- Load Balancing: Since the software state of an entire virtual machine is completely encapsulated by the VMM, it is relatively easy to migrate virtual machines to other platforms in order to improve performance through better load balancing.
- Legacy Applications:Even if an organization decides to migrate to a different operating system, it is possible to continue to run legacy applications on the old OS running as a guest OS within a VM. This reduces the migration cost.

REVIEW OF LITERATURE

Apple's Parallel Desktop (2018) uses hardware virtualization technology to handle both Apple and Intel architecture in a single Physical CPU (pCPU). The hypervisor uses resource mapping to share the virtual CPU's

(vCPU) resources with the physical CPU (pCPU). The Boot Camp Assistant, a utility programme for multi-boot software that helps to install Microsoft Windows/Linux on an Intel-based Mac, partitions the HDD for top CPU and vCPU installation of Apple OS and Windows/Linux OS. This utility tool helps users manage their HDD partitions and launches the Apple system's Windows installer (device driver). This utility also instals the Windows control panel applet that allows you to select the boot OS.

Virtualization at the hardware level can be accomplished by putting the hypervisor on top of the bare system or at the kernel level, according to studies (KVM). A few strategies used to develop simple and quick VMs include hyper call extension, register-based approach, and binary translation approach. VMs based on hypervisor and kernel have been developed by a number of authors for a variety of applications ranging from standalone systems to networking, grid, and cloud computing environments. A few studies were published on the performance of virtual machines (VMs) in terms of scalability, security concerns, and enhancing hardware performance and computing time in various situations.

Meso-virtualization (Megumi & Shuichi 2017) is a lightweight hypervisor for embedded devices created by (Megumi & Shuichi 2017). In a Linux/RTOS hybrid system, the hypervisor modifies the guest OS source code to assist hypervisor configuration using techniques such as page fault, segment descriptor, memory management, and privilege level. The virtualization works with Linux as a guest operating system on any x86 processor. Meso-virtualization is the most cost-effective, easy-to-manage, and dependable option for embedded systems.

(Walters et al. 2008) used industry standard benchmark tools and full and para virtualization approaches to investigate the performance of several hypervisors such as OpenVZ, Xen, and VMware in order to establish an optimum hypervisor for High Performance Computing (HPC). In HPC, the VMware ESX Server product is pitted against the OpenVZ and Xen hypervisors. OpenVZ's overall performance is ideal for Message Passing Interface (MPI) in HPC applications, and it performs best in this area. Dex-OS, a kernel-based Operating System, was used by (Hermocilla 2019) to improve the learning capabilities of an OS by users utilising Instructional Operating System (ICS-OS). In an Open Source Linux environment, ICS-OS used para-virtualization with a Netwide Assembler (NASM) and Bochs Emulator. Users learned about user space, kernel space, programme loading, process creation and execution, system calls, software development kit benefits, and application programming interfaces, among other things. The users' learning curves were found to be improved. The cited articles provided a framework for creating a hardware emulation/simulation and managing the kernel in order to create an operating system.

Sascha et al. 2013 created a lightweight approach for separating numerous Android users from dependable and protected entities on mobile platforms using the Isolation and Integration Mechanism. Tunneling and encryption are used to connect mobile devices across networks without the need of cryptographic keys between Android users. This method makes remote administration and management of mobile devices relatively simple. When verifying the application efficiency in several machines utilising architecture-independent methods in computing environments, (Ivo et al. 2018) advised decreasing the inconsistency observation. The authors recommended that variable characterisation be reduced across numerous hardware platforms. The authors suggested that the researchers check the bandwidth and lower it across the various hardware platforms.

Yu Adachi & Yoshihiro 2019 created Bit Saucer, a malware investigation system that uses less resources and takes less time to execute. In Network Virtual Environment, it developed a number of virtual execution environments. Using honey pots, the system administrator studied how malware works with genuine applications. The Bit Saucer's performance is measured with the Apache Bench Benchmark tool in a VMM. The Bit Saucer outperforms the basic honeypot system in this benchmark. In server and workstation environments, (Salomie et al. 2018) tested the performance of apps that managed their own memory using Application Level Ballooning (ALB). Memory consumption in shared virtual machines is well-suited to the ALB method. In stiff applications, this ALB allocates a specific amount of RAM for dealing with either static or dynamic virtual machines.

For expanding the flexibility of virtual machine image deployment in Cloud Computing Environments, (Youhui et al. 2018) created application software employing Double Isolation Mechanism, On-Demand Software, Central Distribution, and Content-addressable storage (CAS). The application includes features such as a runtime system, application provisioning, workflow usage, and a centralised deployment mechanism. Adaptive scheduling improves the management of virtual machine images, reusability, and storage policies in a large-scale system.
(As stated by Ally in 2018) In server and workstation contexts, Software Tamper- Proofing and Code Obfuscation were used to safeguard code segments in virtual machine security. These code parts are tailored for virtual machine integration and protection. This research demonstrated how essential code parts are protected from virtual machines.

FEATURES OF HYPERVISORS/VMS (SECURITY)

Virtualization gaining popularity day by day because of their features like restoring the VMs to pre-attack states, isolation of users, imitate computing environment, support remote computation. These are some benefits concerning security.

Abstraction of physical resources

Hypervisor abstract the Physical layer and strictly bounded resources are allocated to the Guest Machine. Through abstracting the Hardware details Hypervisor restrict the access of physical hardware. The Guest machine running inside the Hypervisor doesn't know about the host operating system and Hardware. When an attacker doesn't know about the details of the operating system and Hardware of the Hypervisor the surface of attack level is reduced and compromising of Machine is difficult. The Hypervisor aims to allocate the resources to the resources to each Virtual Machine. Each Virtual Machine encapsulates itself and prevents other VMs from accessing their resources. An attacker cannot compromise the physical machine and only one virtual machine at a time.

Pre-attack State Restore

The virtual disk of each Virtual Machine stored at the Host machine as a file. Virtual Machine takes a backup (Snapshot) of the virtual disk on a regular time interval or any changes made in configuration. In case of Machine Compromization or any other type of infection, We can restore the VMs from backup disk files. It provides the integrity of the data and disinfection of Machine.

2.3 Isolation of Physical resources

Hypervisor makes partitions of the physical resources and makes isolated entities. A hypervisor allows each VMs to run independently. Attack and compromisation of one VM can not affect the other. Isolation and Abstraction characteristics of the Hypervisor an additional security feature. In case any VM compromised, Hypervisor remove this VM and restore it to pre-attack state.

VULNERABITLITIES AND ATTACKS

Virtual machines and Physical Machines both are vulnerable to the theft and various type of attacks like Denial of service attack(DoS). VM Infrastructure is vulnerable to the DOS attack, which withholds resources from all VMs installed on Physical Machine. We can Fix it in many cases by applying QOS for the resource consumption per VMs. There are some Vulnerabilities and attacks at Hypervisor Level.

Modification in Hypervisor

In this type of attack, attackers try to modify the Hypervisor(OS). One form of this type of attack is Virtual Machine Machine based Rootkits (VMBR). VMBR is malware, it is difficult to detect and remove through malware detectors. It is capable to breach the guest OS security and dig out the way to compromise the hypervisor or directly attack a hypervisor to gain the full control of the system. Blue Pill and Subvirt are examples of these type of Malware. There are many methods to prevent from Hypervisor modification. A host can use a trusted relationship with a hypervisor or the guest verify the integrity of the hypervisor at the time of booting.

Guest to guest attack

It is also known as VM communication. In this type of attack, One Infected VM try to infect the other machines on the same environment. A malicious Guest can probably access another guest through shared resources like

Memory, Network connections. For example, if a VM opts the memory allocation lies of the other VM then it can perform the read-write operation to that location and distributed the other operations. For the prevention of these type of attack system or cloud, an administrator has to define the rules and policies for communication between VMs and only authorized VMs to take part in communication within the VM Infrastructure. Example of these type of attacks is SQL injection attack and spoofing attacks.

Data Stealing / Mobility

Theft of the Virtual Machine can happen without physical access of the machine. The data of each VM are store in a virtual disk in the form of an image. Most of the hypervisor provides the facility to copy this disk image and run on other physical Machine. This is a good feature of hypervisor but it has some drawback also. Attackers can copy the VM over the network and access data in their environment and have enough time to dig out all the security arrangments like passwords type of encryption used.

Hypervisor Intrusion

Abstraction, Isolation and resource allocation between the guest and host is managed by the Hypervisor. The main target of the attackers to get full control of the hypervisor and execute the malicious code with root access. The function of hypervisor is to convert instructions received from the guest to the instruction for the Host Operating System. If the Guest is compromised, then the instructions sent by the guest to hypervisor may be aberrant.

CONCLUSION

Virtualization technology probably has new vulnerabilities. For Security professional, it is a big challenge to make all VMs secure in the computing environment. In this paper, we describe the features of the hypervisor and discussed the attacks and vulnerabilities in Virtualization environment. The hypervisor should rigorously control the communication between the VMs, limit the resources and monitoring the consumption of the resources by VM on regular basis for preventing the Daniel of Services (DoS) attacks. It is mandatory to secure the host and each VMs (guest) to secure the whole virtual environment. We have to Compliance all the advisory released by the CERT-In related to cloud security and Vulneability.

As a future work of my paper, we will install the VMs on the different type of open source-based hypervisor like proxmox,oVirt, Citrix and perform the Vulnerability Assessment and penetration testing to exploit the vulnerabilities of the system using the various freeware tools. Some of the tools are Burp Suite, Network Miner packet analyzer, TCPDump, Nmap and hydra etc.

REFERENCES

- John patrick and Rameez Asif," Securing Cloud Hypervisors: A Survey of the threates,Vulnerabilities and Conutermeasures", 11 June 2018.DOI-10.1155/2018/1681908.
- Nguyen TH, Di Francesco M, Yla-Jaaski A (2017) Virtual machine consolidation with multiple usage prediction for energy-efficient cloud data centers. IEEE Trans Serv Comput.
- Basu D,Wang X, Hong Y, Chen H and Bressan S (2019) Learn-as-you-go with megh: Efficient live migration of virtual machines, IEEE Trans Parallel Distrib Syst 30(8):1786–1801.
- Nasim R, Zola E, Kassler AJ (2018) Robust optimization for energy-efficient virtual machine consolidation in modern datacenters. Cluster Comput 21(3):1681–1709.
- Shidik GF, Azhari A, Mustofa K (2016) Improvement of energy efficiency at cloud data center based on fuzzy Markov normal algorithm VM selection in dynamic VM consolidation. Int Rev Comput Soft (IRECOS) 11(6):511–520.
- Abdullah M, Lu K, Wieder P, Yahyapour R (2017) A heuristic-based approach for dynamic vms consolidation in cloud data centers. Arab J Sci Eng 42(8):3535–3549.

- Zhang, T., Lee, R.B.. Cloudmonatt: An architecture for security health monitoring and attestation of virtual machines in cloud computing. In: Proceedings of the 42nd Annual International Symposium on Computer Architecture. 2015:362–374.
- Pang S, Xu K, Wang S, Wang M Wang S (2020) Energy-saving virtual machine placement method for user experience in cloud environment. Math Prob Eng 1–9.
- Singh N, Dhir V (2019) Hypercube based genetic algorithm for efficient vm migration for energy reduction in cloud computing. Stat Opt Inf Comput 7(2):468–485.
- Kansal NJ, Chana I (2016) Energy-aware virtual machine migration for cloud computing-a firefly optimization approach. J Grid Comput 14(2):327–345.
- Wu Q, Ishikawa F, Zhu Q, Xia Y (2016) Energy and migration cost-aware dynamic virtual machine consolidation in heterogeneous cloud datacenters. IEEE Trans Serv Comput 1–13.
- Rybina K, Schill A (2016) Estimating energy consumption during live migration of virtual machines. In: IEEE international black sea conference on communications and networking (BlackSeaCom), pp 1–5.
- Dave Shackleford(2013).”Fundamentals of Virtualization Security.In:Judy Flynn. Virtulization security :Protecting Virtualized Environments,Canada:Jhon Wiley,PP2-13.
- Li X, Garraghan P, Jiang X, Wu Z, Xu J (2017) Holistic virtual machine scheduling in cloud datacenters towards minimizing total energy. IEEE Trans Parall Distrib Syst 29(6):317–1331.
- Ismaeel S, Karim R, Miri A (2018) Proactive dynamic virtual-machine consolidation for energy conservation in cloud data centres. J Cloud Comput 7(1):1–28.
- Kim J, Ruggiero M, Atienza D, Lederberger M (2013) Correlation-aware virtual machine allocation for energy-efficient datacenters. Des Automat Test Eur Conf Exhib (DATE), 1345–1350.