Int.J.HIT.TRANSC:ECCN.Vol.3: Issue 2A(1) (2017) Page 9-13 ISSN: 0973-6875

Available Online at www.hithaldia.in/locate/ECCN

ORIGINAL CONTRIBUTION

Implementation of Hypervisor Using VMWARE to Secure Virtual Machine by Isolation in Virtualization

Apratim Mitra* and Manigrib Bag

Haldia Institute of Technology, Hatiberia, Haldia, WB, India

(Received Date: 20th August, 2017; Acceptance Date: 30th September, 2017)

ABSTRACT

Virtualization is introduced since 2006 and it has been changed impressively thereafter. At that time, it was done in programming using binary translation where a technique is used to change the normal mechanism to overcome the complicated computation using resource sharing. Now-a-days, the hypervisor is the management interface to isolate the CPU, memory, and I/O. Now it is done at an equipment level with the hypervisor overseeing the amount of the equipment assets. A virtual machine can utilize, like a choreographer or traffic officer. This type of the hypervisor is called the virtual machine Monitor (VMM). With the capacity to use these CPU extensions, the attack surface of the hypervisor shrinks significantly. Numerous security-related threats about virtualization are unjustifiable. Various equipment and programming isolation systems with other vigorous security mechanisms are used to get the control. In this paper, we clarify how these innovations address these security threats. We have done full Virtualization, Para-virtualization, and Hardware Assist using VMware virtualization. VMM or a Hypervisor is a virtual machine manager/monitor manager, which is a program that allows multiple operating systems to share a single hardware host. Each guest operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources and is allocating what are needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

Key words: Hypervisor, VMM, Virtualization, VMware

1. INTRODUCTION

What virtualization means is creating more logical IT resources, called virtual systems, within one physical system. That's called system virtualization. It is most commonly uses the hypervisor for managing the resources for every virtual system. The hypervisor is software that can be virtualized the hardware resources.

There are two types of hypervisors:

a) Type 1 hypervisor: hypervisors run directly on the system hardware.

b) Type 2 hypervisor: hypervisors run on a host operating system that provides virtualization services, such as I/O device support, memory management and space management.

1.1. Type 1 hypervisor

a) VMware ESX and ESXi

These hypervisors offer advanced features and scalability, but require licensing, so the costs are higher.

There are some lower-cost bundles that VMware offers and they can make hypervisor technology more affordable for small infrastructures.

VMware is the leader in the Type-1 hypervisors. Their vSphere/ESXi product is available in a free edition and 5 commercial editions.

b) Microsoft Hyper-V

It was first released with Windows Server, but now Hyper-V has been greatly enhanced with Windows Server 2012 Hyper-V. Hyper-V is

*Corresponding Author: apratim777@yahoo.com

available in both a free edition (with no GUI and no virtualization rights) and 4 commercial editions – Foundations (OEM only), Essentials, Standard, and Datacenter. Hyper-V

c) Oracle VM

The Oracle hypervisor is based on the open source Xen. However, if you need hypervisor support and product updates, it will cost you. Oracle VM lacks many of the advanced features found in other bare-metal virtualization hypervisors.

1.2. Type 2 hypervisor

a) VMware Workstation/Fusion/Player

VMware Player is a free virtualization hypervisor. It runs only one virtual machine (VM) and does not allow creating VMs. VMware Workstation is a more robust hypervisor with some advanced features, such as record-and-replay and VM snapshot support.

VMware Workstation is basically used for running multiple different operating systems or versions of one OS on one desktop,

b) Microsoft Virtual PC

This is the latest Microsoft's version of this hypervisor technology, Windows Virtual PC and runs only on Windows 7 and supports only Windows operating systems running on it.

c) Oracle VM VirtualBox

VirtualBox hypervisor technology provides reasonable performance and features if you want to virtualize on a budget. Despite being a free, hosted product with a very small footprint, VirtualBox shares many features with VMware vSphere and Microsoft Hypervisor.

2. VIRTUALIZATION ARCHITECTURE

A Virtual machine (VM) is an isolated runtime environment (guest OS and applications). Multiple virtual machines can run on a single physical system shown in Figure1.

<table>
<tr><td>Applications</td><td>Applications</td><td>……</td><td>Applications</td></tr>
<tr><td>VM
Guest OS</td><td>VM
Guest OS</td><td>…….</td><td>VM
Guest OS</td></tr>
<tr><td colspan="4">Virtualization Platform (VMware, Oracle VM.., Microsoft VM)</td></tr>
<tr><td colspan="4">Physical Box</td></tr>
</table>

2.1. Benefits of Virtualization

Following are the benefits of virtualization:

a) Cost Reduction: Sharing of resources helps cost reduction

b) Isolation: Virtual machines are isolated from each other as if they are physically separated

c) Encapsulation: Virtual machines encapsulate a complete computing environment

d) Hardware Independence: Virtual machines run independently of underlying hardware

e) Portability: Virtual machines can be migrated between different hosts.

2.2 Virtualization in Cloud Computing

Cloud computing helps virtualization one step ahead:

a) We do not need to own the hardware.

b) Resources are rented as needed from a cloud.

c) Various providers allow creating virtual servers using some of the following:

1. Choose the OS and software

2. The chosen OS will run on a large server farm.

3. Instantiate more virtual servers or shut down existing ones within minutes.

d) We can get bill only for what you used [3].

2.3. Virtualization Security Challenges

The trusted computing base (TCB) of a virtual machine is too large. A small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security. Smaller TCB causes more security [4].

3. VIRTUALIZATION SECURITY REQUIREMENTS

A secure run-time environment is the most fundamental are Network interface: Transport layer security (TLS) and Secondary storage: Network file system (NFS).

The security mechanisms in the first two rely on a secure run-time environment. All the cryptographic algorithms and security protocols reside in the run-time environment Figure2.

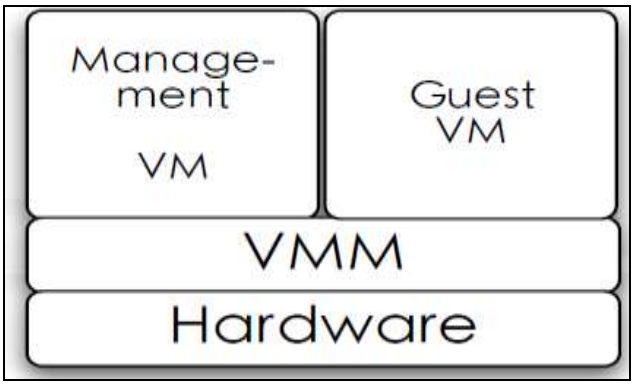

Figure.2 Smaller TCB Solution

4. DOMAIN BUILDING PROCESS: Figure.3

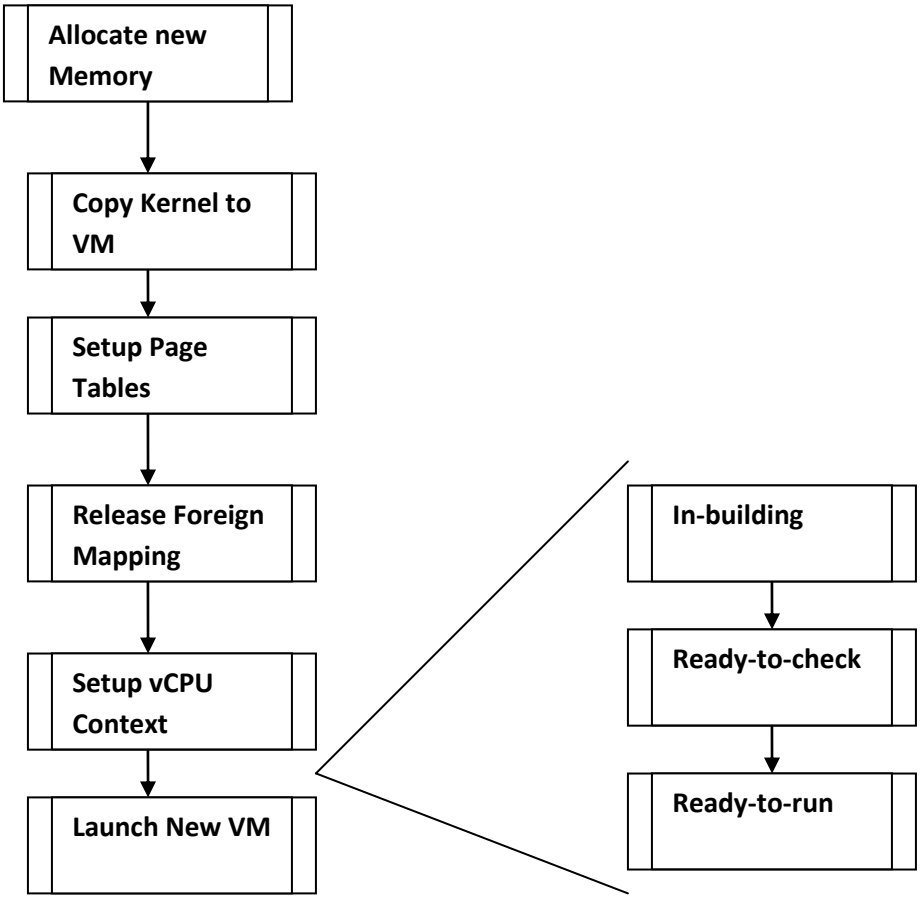

Figure 3: Domain building Process

5. HYPERVISOR VULNERABILITIES

Malicious software can run on the same server which will attack hypervisor or may access/obstruct other VMs Figure.4.

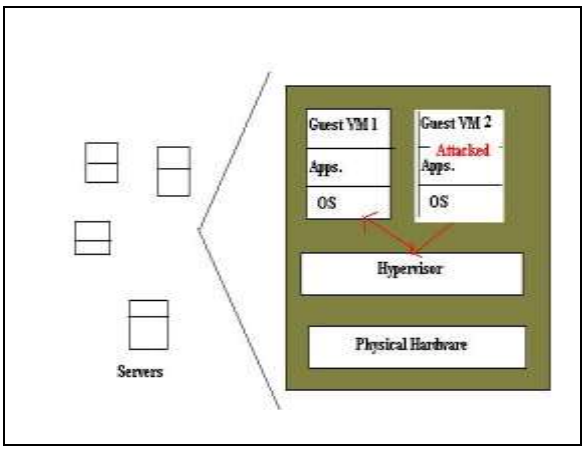

Figure.4: Attack on one VM propagate to all VM

We have taken a procedure through which this problem can be solved is removing of Hypervisor which removes the Hypervisor, there's nothing to attack and still retains the needs of a virtualized cloud infrastructure Figure.5.

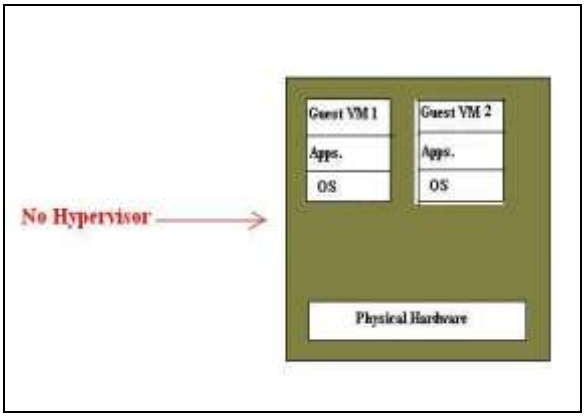

Figure.5 Removing of Hypervisor

5.1. Roles of Hypervisor:

a) Isolating/Emulating resources:

1) CPU: Scheduling virtual machines (Push to HW/ Pre-Allocation)

2) Memory: Managing memory (Push to HW/ Pre-Allocation)

3) I/O: Emulating I/O devices (Remove)

b) Networking (Push to side).

c) Managing virtual machines (Push to side).

5.2. Removing the Hypervisor:

a) Scheduling virtual machines - One VM per core.

b) Managing memory - Pre-allocate memory with processor support.

c) Emulating I/O devices - Direct access to virtualized devices.

d) Networking - Utilize hardware Ethernet switches.

Managing virtual machines - Decouple the management from operation.

6. CONCLUSION

In this way we can isolate an affected VM and can stop polluting all VM from attack. Here we have implemented IAAS (Infrastructure as a Service), SAAS (Software as a Service).

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[2] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616.

[3] Feng, D. G., Zhang, M., Zhang, Y., & Xu, Z. (2011). Study on cloud computing security. Journal of software, 22(1), 71-83

[4] Hwang, Kai, Sameer Kulkareni, and Yue Hu. "Cloud security with virtualized defense and reputation-based trust management," Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on. IEEE, 2009

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, 2012, 28, pp. 583-592.

[6] Jing, Xue, and Zhang Jian-Jun. "A brief survey on the security model of cloud computing." Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium on. IEEE, 2010