ABHIYANTRIKI
An International Journal of Engineering & Technology
(AIJET)
Vol. 1, No. 2 (December, 2014) http://www.aijet.in/ eISSN: 2394-627X

Overview and Study of Various Techniques for Secured Virtualization in Cloud Environment

Apurva R. Pisalkar*
PG Scholar
St. Vincent Pallotti College of Eng. & Technology, Nagpur, INDIA

M. V. Bramhe
Associate Professor
St. Vincent Pallotti College of Eng. & Technology, Nagpur, INDIA

Abstract

Virtualization is a technology that increase the effectiveness of computing services provided to users in terms of performance, preservation, and cost. Virtualization provides perception of physical hardware resources that allows for the operation of the same services on different physical hardware platforms. By controlling access to the physical resources, virtualization can also be used to run different services in parallel on the same physical hardware. It allows, executing multiple operating systems simultaneously on the single physical host. The resources can be utilized more capably, and users can decrease their expenditures on computing services. For all these reasons, virtualization plays an important role in cloud computing. Although the virtualization is having number of advantages it has many security challenges. It is susceptible to various security attacks. One of these attacks is cross-vm side channel attack. In our project we will try to design the system which will protect the virtual environment from attack which will make the system unsecured and untrustable. In our system we will design a monitoring program which will continuously monitor the virtual machines and will block the virtual machine which will perform any malicious activity.

Keywords*: VM, VMWare, VMM, OS.*

****Author for Correspondence*** pisalkar.apurva@gmail.com

1. Introduction

Virtualization plays key role in cloud computing. In virtualization virtual version of a device or resources, such as a server, storage device, network or operating system, are created. Virtualization is a powerful technology to increase the effectiveness of computing services provided to private and business users in terms of performance, preservation and cost. In virtual environment multiple operating systems can work simultaneously on a single physical machine. As virtualization have number of advantages like increasing effectiveness of computing services, parallel execution of different services on the same physical hardware. By doing this, resources can be utilized more economically, and users can decrease their expenditures on computing services notably. Virtualization is a method for hiding the substantial characteristics of

computing resources from the way in which other systems, applications, or end users interact with those resources. This includes making a single physical resource, such as a server, an operating system, an application, or storage device appear to function as multiple logical resources or it can include making multiple physical resources.

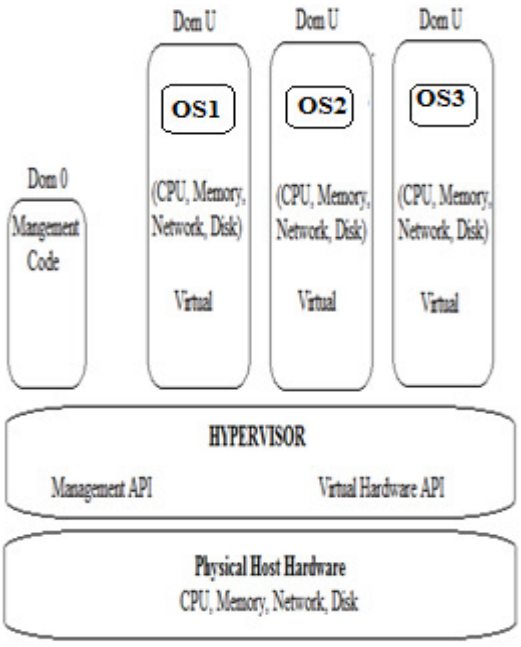


Fig. 1: Block Diagram of Virtualization

1.1 Cloud Computing

According to definition given by NIST: "Cloud computing [1] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

The primary types of cloud deployment models are as follows:

Private Cloud, Public Cloud and Hybrid Cloud: The public cloud structure is operated solely for an organization. It is manageable by the organization or a third party. The private cloud infrastructure is made accessible to the general public or a large industry group and is owned by an organization selling cloud services. This cloud infrastructure is a composition of two or more clouds (private, community, or public) that stay unique entities but are bound together by consistent or proprietary technology that enables data and application portability.

1.2 Types of Virtualization

Part of the problem of the intangible project is that there are many different types of virtualization [3] and uncertainty over their definitions. In this section, we define many of the important terms associated with virtualization.

Operating System Virtualization

Operating System Virtualization is a method of running multiple virtual operating systems on a single host operating system. This technique of virtualization usually uses a standard operating system such as Windows or Linux as the host, plus a virtual machine supervisor, to run multiple guest operating systems. This type is illustrated in the figure.

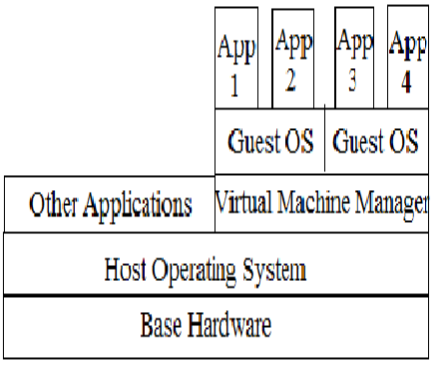


Fig: Operating System Virtualization

Server Virtualization

In Server Virtualization, the foundation hardware is virtualized, allowing multiple guest operating environments to run directly on it, without requiring a whole host operating system. In

this the virtualization software will run on the base hardware, and the operating systems will be installed onto that virtualization software. This virtualization is presented in the figure.

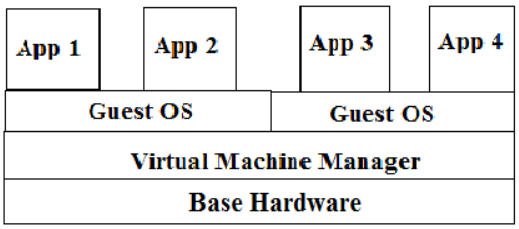


Fig: Server Virtualization

Desktop Virtualization
Desktop Virtualization provides the end user with a desktop environment that in turn allows right to use to any authorized application, apart from of where the application is actually located.

Storage Virtualization
Storage virtualization provides a means for many users or applications to access storage without being worried with where or how that storage is actually located. Storage Virtualization is of mainly 2 types: Block Virtualization and File Virtualization.

1.3 Advantages of Virtualization
Some advantages of virtualization are as follows:

1. Lesser number of physical servers is required and because of this the hardware maintenance cost can be reduced.
2. By keeping each application within its own virtual server one application can be prevented from affecting other function when changes are made to it.
3. A standard virtual server can be developed that can be easily duplicated, which will speed up server operation.
4. Multiple operating system technologies can be deployed on a single hardware platform.

1.4 Problems in Virtual Environment
Use of virtualization in cloud environment has added number of security issues [2]. These security issues can be explained as follows:
Multi-tenancy: Multi-tenancy is style in which a single instance of a software application serves for multiple customers. Each customer is called a tenant. Tenants may be given the ability to modify some parts of the application, such as color of the user interface, but they cannot modify the application's code.
Loss of control: The users of cloud are not aware of the location of their data and services and the cloud providers run VMs and they are not aware of their contents.
Network topology: The architecture of cloud is very active and the current workload on cloud changes over time, because of creating new VMs and removing existing VMs. In addition, the mobile nature of the VMs that allows VMs to roam from one server to another leads to non-predefined network topology.
Single point of access: Virtualized servers have a restricted number of access points available to all VMs. This represents a crucial security vulnerability where compromising these access points compromise the VMs, hypervisor or the vSwitch.

2. Security Attacks on Cloud Virtual Infrastructure

The virtual cloud infrastructure is vulnerable to various attacks. Different security attacks on cloud virtual infrastructure can be categorized into following categories:

Hypervisor Attacks
Hackers consider the hypervisor as target because of the greater control afforded by lower layers in the system. Compromising the hypervisor enables achievement of control over the installed VMs, the physical system and hosted applications. The VM-Based Root kits are capable of inserting a malicious hypervisor on the fly or modifying the installed hypervisor to gain control over the host workload.

vSwitch Attack
The vSwitch is vulnerable to a large range of layer-2 attacks like a physical switch. These attacks include vSwitch configurations, VLANs and trust zones, and ARP tables.

Virtual Machine Attacks
Cloud servers contain tens of VMs, these VMs may be either active or offline, and in both states they are susceptible to various security attacks. Active VMs are susceptible to all traditional attacks that can affect physical servers. Once a VM is compromised, this gives the VMs on the same physical server a chance of being able to attack each other, because the VMs share the same hardware and software resources e.g. memory, device drivers, storage, hypervisor software. Collection of multiple VMs in a single server and sharing the same resources increases the attack surface. When a VM becomes offline, it is still available as VM image files that are susceptible to malware infections and patching. Some examples of virtual machine attacks are as follows:

Virtual Code Injection Attack
In virtual code injection attack, malicious code is injected in program to change the course of execution of program. This type of attack exploits poor handling of untrusted data. These types of attacks are usually made possible due to a lack of proper input/output data justification, for example, allowed characters, data formats, amount of expected data etc.

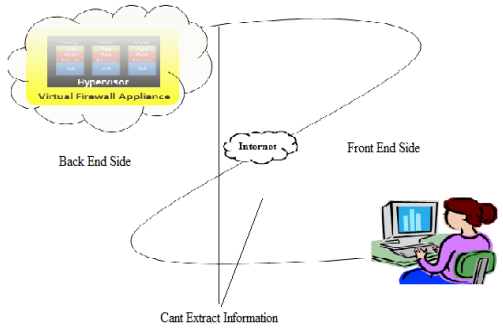
VM Escape Attack
Normally virtual machines are encapsulated. The operating systems running inside the virtual machine doesn't know that they are virtualized. These virtual machines cannot directly interact with the hypervisor. The process of breaking out and interacting with the hypervisor is called a "VM escape." Since the hypervisor controls the execution of all of the virtual machines running on the host then the attacker that can gain access to the hypervisor can gain control over every other virtual machine running on the host.

Cross VM Side Channel Attack
Cloud computing provides infrastructures which is a collection of multiple computers, virtual machines (VMs) and other resources to its users to store their application, files, confidential information, documents and so on [2]. By mapping the cloud infrastructure the target virtual machine is selected. New virtual machine is placed co-resident to the target virtual machine. After successful placement of instantiate virtual machine it can successfully extract the confidential information from the targeted virtual machine. This type of attack is called cross-vm attack. Side channel attack requires two main steps: Placement and Extraction. Placement refers to the attacker arranging to place their malicious VM on the same physical machine. Extraction: After successfully placement of

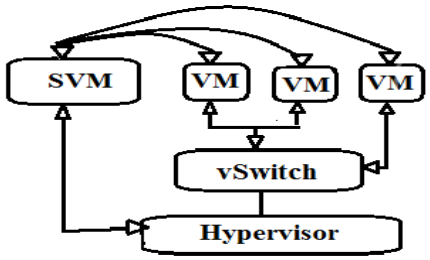
the malicious VM to the targeted VM extract the confidential information, file and documents on the targeted VM.

3. Literature Review

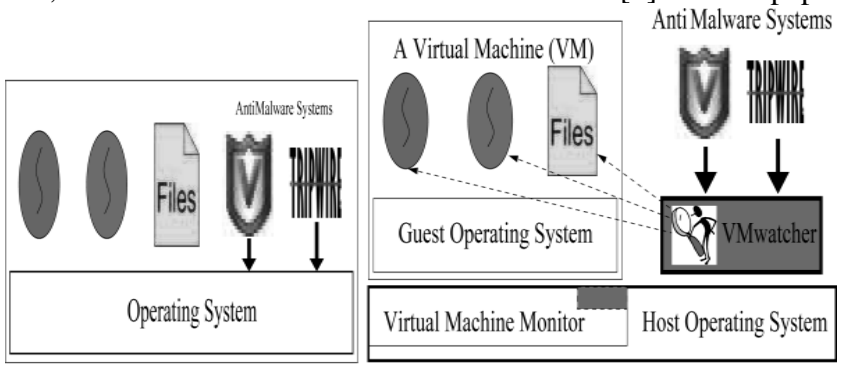
Lee Badger, Tim Grance, RobertPatt-Corner, Jeff Voas [1] have discussed NIST definition and basics of cloud computing. It gives surveys of typical commercial terms of usage for cloud computing systems. It also provides a breakdown of how cloud computing solutions may be deployed and describes general implications for different deployment options. It provides a high-level view of how Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) clouds work. This paper presents open issues and also gives recommendations. One of the appendixes presents a simple worked example illustrating how different kinds of costs may be incurred by using a cloud. Another appendix discusses the sharing of responsibilities between providers and subscribers. One contains a list of acronyms used in this document. Other appendix contains a glossary of terms used in this document and one lists external resources referenced in document. Last appendix lists NIST publications referenced in this document. Bhrugu Sevak [2] in has discussed about the Amazon's Elastic Computing Cloud (EC2) service. He discusses virtual machine placement and extraction policies. He has explained security against side channel attack in cloud computing using combination of virtual firewall appliance and randomly encryption decryption. The security policy discussed in this paper is represented using the above mentioned diagram.



GA´ BOR PE´ K [3] et at. in their paper have given overview of virtualization concepts. They discuss basics of hardware virtualization and different components of virtual environment which are guest OS, host OS, hypervisor, virtual machine monitor, management interface and network. They discussed the adversary model. They discussed in brief how each component in virtual environment that is guest, host, hypervisor, management interface and network can be attacked by adversary. Adversary can compromise guest OS in various ways. He can launch an internet-to-guest, a guest-to-guest, a virtual machine migration network-to-guest, a guest-to-self or a management interface-to-guest attack. Adversary can launch a guest-to-host, a host-to-self or an internet-to-host attack for compromising hosts OS. An adversary can compromise the hypervisor in various ways by launching a guest-to-hypervisor, a host OS-to-hypervisor, and a physical/physical management interface-to-hypervisor attack. Adversary can launch a guest-to-management Interface or a network-to-management attack for compromising management interface. In this paper authors also gives overview of countermeasures for these various attacks discussed above. Amani S. Ibrahim [4] et al in their paper has discussed about Virtualization-Aware Security Solutions [5]. This security approach deploys the security software in a dedicated and privileged VM (SecVM) with privileged access to the hypervisor to secure the other VMs (untrusted VMs) installed in the same physical server. The SecVM utilizes Virtual Machine Introspection (VMI) techniques, to



enable monitoring and observing VMs from outside a VM, and get a view of the VM at the hypervisor level. XUXIAN JIANG, XINYUAN WANG and DONGYAN XU [5] in their paper present the designing, implementation of *VMwatcher - an "out-of-* the-box". This approach helps to overcome the semantic gap challenges.



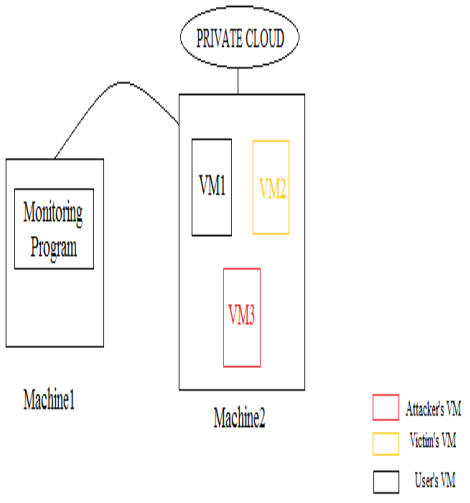
(a) Traditional "in the box" approach (b) VMwatcher approach

4. Proposed Plan of Work

Virtualization is most useful technology in IT industry. The virtual infrastructure is vulnerable to various security attacks it is not secured. The virtual machines are vulnerable to cross-vm attack and in our system we will try to protect vm from cross-vm attack. There are two approaches for providing security to vm one of them is in-the-box view and other is out-of-box view. In out-of-box approach the security is provided to the system from outside the cloud. The security providing program is deployed out of cloud on different physical machine. In our system we will deploy monitoring program out of the cloud that is we will use out of box view. The monitoring program will continuously monitor all the virtual machines on cloud from outside the cloud. If monitoring program will find any malicious activity on any virtual machine in cloud then it will report the cloud provider about that malicious activity and then cloud provider will take suitable action on that malicious virtual machine. This proposed solution can be shown by following diagram:

Proposed System

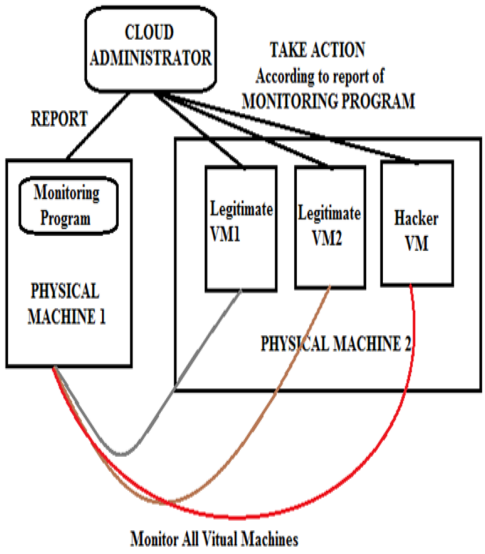
In our system we will have two physical machines. On one machine we will show virtual environment using VMware workstation. On this system we will create 3virtual machines. On all these three virtual machines we will install different operating systems (Windows XP, Windows7, Windows8). One of these machines will be a normal user, one will be attacker and one will be a victim which will be attacked by attacker. All these 3 machines will be interconnected using WAMP server. On other physical machine we will install the monitoring program. This program will continuously monitor all the virtual machines on other system. This program will be connected to the virtual machines through LAN/Internet.



As we mentioned that one of the three virtual machines will be a attacker. This attacker vm will read all the functions done by the victim machine. The attacker will passively monitor the victim. Now the monitoring program installed outside the cloud will be monitoring the activities of all the virtual machines and it will find the activity done by the attacker. When monitoring program find this activity of attacker it will inform the cloud provider about this activity and will block the attacker. As per our planned work our proposed system will be as shown in following diagram:

5. Conclusion

Virtualization is emerging and useful technology in IT sector. Even though it is most useful technology it has many security challenges and we have to focus on these challenges. So in our work we are trying to provide security to virtual systems. In this survey paper we have discussed the basics of virtualization, its types, its components, various security attacks on the virtual environment. The virtual environment is vulnerable to various security attacks and in our system we will try to work on providing security against cross vm side channel attack. In this paper we have discussed our proposed plan of work and also have given our proposed system. With our proposed system we try to make the virtual machines on our system secured from cross channel attack and will try to improve the system.



6. Future Work

The system which we have explained in this paper is working with two virtual machines. We are trying to work with three virtual machines. In this system, with monitoring program we have linked only delete option. But further we can try to develop a program which access the data contained in host machine. When any virtual machine, access data from the host machine then this activity must also be noticed by the monitoring program. So we can also be linked with the monitoring program. If we link this program with monitoring program then we can notice the malicious activities done with host machine.

References

[1] Lee Badger, Tim Grance, Robert Patt-Corne, Jeff Voas "DRAFT Cloud Computing Synopsis And Recommendations", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-146 May 2011.

[2] Bhrugu Sevak "Security against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012.

[3] Gabor Pek, Levente Buttyan, Boldisar Bencsa´ TH "A Survey of Security Issues in Hardware Virtualization" Accepted on ACM Computing Surveys, Vol. V, No. N, Article Y, Publication date: January 20XX.

[4] Amani S. Ibrahim, James Hamlyn and John Grundy "Emerging Security Challenges of Cloud Virtual Infrastructure**"** In Proceedings of APSEC 2010, Cloud Workshop, Sydney, Australia.

[5] XUXIAN JIANG, XINYUAN WANG and DONGYAN XU "Stealthy Malware Detection and Monitoring through VMM-Based "Out-of-the-Box" Semantic View Reconstruction" ACM Transactions on Information and System Security,Vol. 13,No. 2, Article 12, Publication date: February 2010.

[6] Tyson T. Brooks, Carlos Caicedo, Joon S. Park "Security Vulnerability Analysis in Virtualized Computing Environments" International Journal of Intelligent Computing Research (IJICR), Volume 3, Issues 1/2, Mar/Jun 2012.

[7] Bryan D. Payne Martim Carbone Monirul Sharif Wenke Lee "Lares: An Architecture for Secure Active Monitoring Using Virtualization" IEEE 2008.

[8] Steve Mansfield-Devine "Danger in the clouds" Network Security December 2008.

[9] Kuai Xu, Feng Wang, Lin Gu "Profiling-as-a-Service in Multi-Tenant Cloud Computing Environments"

[10] M. Armbrust, A. Fox, Armando, R. Griffith, A. D. Joseph, R. Katz,Randy, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.

[11] S. S. L. Ertaul and G. Saldamli, "Security Challenges in Cloud Computing," in Proceedings of International Conference on Security and Management, July 2010.