ISSN:0975-9646

Securing the Virtual Machines in Cloud Environment Using Hypervisor-based Technology

Gaurav Mhatre[#1], Harshali Mhatre*[2]

[#]Information technology Department, Mumbai University, Atharva college of Engineering,
Malad (w), Mumbai-400095, Maharashtra, India

[*]Information technology Department VIVA College, Virar (W),
Palghar-401303, Maharashtra, India

***Abstract*— The term “cloud computing" is a recent buzzword in the IT world. Behind this fancy poetic phrase there lies a true picture of the future of computing for both in technical perspective and social perspective , because it can reduce the cost and complexity of applications, and it is flexible and scalable. Virtualization technology has security issues that must be addressed before cloud technology is affected by them. In addition, the virtualization technology has limit security capabilities in order to secure wide area environment such as the cloud. Therefore, the development of a robust security system requires changes in traditional virtualization architecture. This paper proposes to summarize virtualization level of cloud computing security in detailed view.**

***Keywords* — Virtualization Technologies, Cloud Computing, architecture, security, components, hypervisor**.

I. INTRODUCTION

Cloud computing, an emerging IT delivery model, is the next generation of networking computing which can deliver both software and hardware as on demand resources and services over the internet with lower IT costs and complexities. Actually, in cloud there are abundant users and their application that are running but security is important for all of them. A cloud computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. A virtual appliance relieves some of the notable management issues because most of the maintenance, software updates, configuration and other management tasks are automated and centralized at the data center by the cloud provider responsible for them. Because virtualization is not a new technology and it has not enough security capabilities for wide network such as cloud.

This paper is organized as following. Section 2 describes the cloud computing and virtualization technology. Section 3 introduces virtualization approaches. Section 4 introduces issues and attacks in security and reliability of virtualization. Section 5 presents a novel approach in order to secure virtualization technology for cloud computing. Finally, Section 6 presents the conclusions.

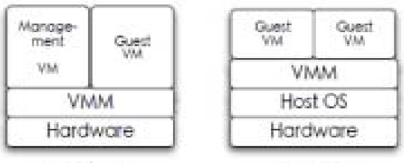
II. VIRTUALIZATION COMPONENTS

Virtualization is one of most important elements that makes cloud computing. Virtualization is a technology to helping IT organizations optimize their application performance in a cost-effective manner, but it can also present its share of application delivery challenges that cause some security difficulties. Most of the current interest in virtualization revolves around virtual servers in part because virtualizing servers can result in significant cost savings. The phrase virtual machine refers to a software computer that, like a physical computer, runs an operating system and applications. An operating system on a virtual machine is called a guest operating system. In addition, there is a management layer called a virtual machine monitor or manager (VMM) that creates and controls the all virtual machines' in virtual environment. A hypervisor is one of many virtualization techniques which allow multiple operating systems, termed guests, to run concurrently on a host computer, a feature called hardware virtualization. It is so named because it is conceptually one level higher than a supervisor. Hypervisor is a firmware or low-level program that acts as a Virtual Machine Monitor. The Virtual Machine Monitor (VMM) or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised, its virtual machines may potentially be compromised as well. The VMM is low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws [7]. Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it will be easier to find and fix any vulnerability. Virtualization introduces the ability to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance [8]. This useful feature can also raise security problems [2][3]. An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Also, it is clear that VM migration exposes the content of the VM to the network, which can compromise its data integrity and confidentiality. A malicious virtual machine can be migrated to another host (with another VMM) compromising it.

There are two types of hypervisor:

Type 1 hypervisor runs on bare system.

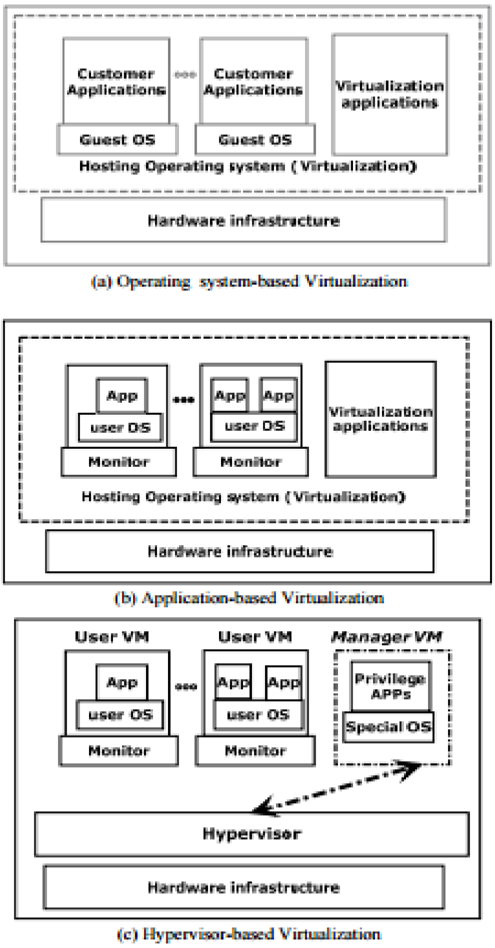
Lynx Secure, RTS Hypervisor, Oracle VM, SunxVM Server, Virtual Logic VLX are examples of Type 1 hypervisor. "The type1 hypervisor does not have any host operating system because they are installed on a bare system." Type 2 hypervisor is a software interface that emulates the devices with which a system normally interacts. Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMware workstation 6.0 are examples of Type 2 hypervisor.



(a) Type I (b) Type II

III. Virtualization Approaches

In a traditional environment consisting of physical servers connected by a physical switch, IT organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management is not typically provided from a virtual switch. Basically, the virtual switch has links from the physical switch via the physical NIC that attaches to Virtual Machines. The resulting lack of oversight of the traffic flows between and among the Virtual Machines on the same physical level affects security and performance surveying. There are several common approaches to virtualization with differences between how each controls the virtual machines. The architecture of these approaches is illustrated in Figure 1.



(a) Operating system-based Virtualization

(b) Application-based Virtualization

(c) Hypervisor-based Virtualization

Fig. 1. Virtualization approaches

A. Operating System-Based Virtualization

In this approach (Figure 1.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the Virtual Machines. This approach is simple, but it has vulnerabilities, such as when an attacker injects controlling scripts into the host operating system that causes all guest OS's to gain control over the host OS on this kernel. The result is that the attacker will have control over all VMs that exist or will be established in the future.

B. Application-Based Virtualization

An application-based virtualization is hosted on top of the hosting operating system (Figure1.b). This virtualization application then emulates each VM containing its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based.

C. Hypervisor-Based Virtualization

The hypervisor is available at the boot time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions which manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines. This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems [1]. However, it is vulnerable because the hypervisor has a single point of failure. If the hypervisor crashes or the attacker gains control over it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level is difficult, though not impossible.

IV. Virtual Machines Security

As mentioned before, there are at least two levels of virtualization, Virtual Machines and the hypervisor. Virtualization is not as new a technology as cloud, but it contains several security issues that have now migrated to cloud technology. Also, there are other vulnerabilities and security issues which are unique to cloud environment or may have a more critical role in cloud.

A. Hypervisor Security In a virtualization environment, there are several Virtual Machines that may have independent security zones which are not accessible from other virtual machines that have their own zones. A hypervisor has its own security zone, and it is the controlling agent for everything within the virtualization host. Hypervisor can touch and affect all acts of the virtual machines running within the virtualization host [3].There are multiple security zones, but these security zones exist within the same physical infrastructure that, in a more traditional sense, only exists within a single security zone. This can cause a security issue when an attacker takes control over the hypervisor. Then the attacker has full control over all data within the hypervisor's territory. Another major virtualization security concern is "escaping the Virtual Machine" or the ability to reach the hypervisor from within the Virtual Machine level. This will be even more of a concern as more APIs are created for virtualization platforms [4]. As more APIs are created, so are controls to disable the functionality within a Virtual Machine that can reduce performance and availability. The reasons for choosing this technology: 1. Hypervisor controls the hardware, and it is only way to access it. This capability allows hypervisor-based virtualization to have a secure infrastructure. Hypervisor can act as a firewall and will be able to prevent malicious users to from compromising the hardware infrastructure. 2. Hypervisor is implemented below the guest OS in the cloud computing hierarchy, which means that if an attack passes the security systems in the guest OS, the hypervisor can detect it. 3. The hypervisor is used as a layer of abstraction to isolate the virtual environment from the hardware underneath. 4. The hypervisor-level of virtualization controls all the access between the guests' OSs and the shared hardware underside. Therefore, hypervisor is able to simplify the transaction-monitoring process in the cloud environment. There are three major levels in security management of hypervisor as mentioned below: 1. Authentication: users must authenticate their account properly, using the appropriate, standard, and available mechanisms. 2. Authorization: users must secure authorization and must have permission to do everything they try to do. 3. Networking: the network must be designed using mechanisms that ensure secure connections with the management application, which is most likely located in a different security zone than the typical user. Authentication and Authorization are some of the most interesting auditing aspects of management because there are so many methods available to manage a virtual host auditing purpose [5]. The general belief is that networking is the most important issue in the transaction between users and the hypervisor, but there is much more to virtualization security than just networking. But it is just as important to understand the APIs and basic concepts of available hypervisor and virtual machines and how those management tools work. If security manager can address Authentication, Authorization, and Virtual Hardware and hypervisor security as well as networking security, cloud clients well on the way to a comprehensive security policy [6]. If a cloud provider at the virtualization level depends only on network security to perform these tasks, then the implemented virtual environment will be at risk.

B. Traditional Intrusion Detection Techniques in VMs .The IDSs can use in hypervisor level, because all the communication between the VMs and the hardware is under the control of hypervisor. If there is an IDS in the hypervisor, it can detect attacks better than the same IDS, running on the guest OS. The guest OS cannot monitor events in cloud, only events within its VM. However, it is possible for the guest OS to monitor VM events if the cloud provider performs this feature or if the cloud is IaaS [7]. Using IDSs, the HIDS has more performance than the NIDS. However, there are direct attacks against the IDS, and if the attack succeeds, the whole cloud is at risk, because the attacker can access all the information that NIDS has gathered, which can include a lot of important and useful data about the cloud users. In traditional networks, this is achievable by NIDS, however. In addition, if the attacker is in the same cloud as his victim is, the NIDS is unable to detect him. It seems NIDS may be best solution for cloud environment but using NIDS has serious problems that one of the main problems when using NIDS for monitoring is the encrypted data.

V. Future Scope

In this paper, we added some features to virtualization architecture in order to improve security for cloud environment. The proposed architecture are based on this truth:

"When the workload of the VM increases abnormally, the VM may be a victim or an attacker" Therefore, in the architecture, we included additional units for monitoring the events and activities in VMs, while trying to prevent attacks without knowing what type of data is being transmitted between VMs or VMs and hypervisor.

Description of Proposed Architecture

Generally, encryption is used by most of users and it is not possible to ask users not to encrypt their data. In our proposed architecture, there are not any requirements to reveal user data or encryption key to cloud providers. We have also added some new features to increase security performance in virtualization technology such as security and reliability monitoring units (VSEM and VREM). HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them, but HSEM decides if the VM is an attacker or a victim. Actually, HSEM receives behavioral information from VSEM and HREM and never collects any information itself. Figure 2 illustrates the new secure architecture and the new units in VMs level, VSEM and VREM, which is available for all VMs (and also in Management VM) In addition, There are two other new units, HSEM and HREM, which is available in the hypervisor level. VSEM and VREM consume low resources of the VM, but they help to secure VMs against attacks.

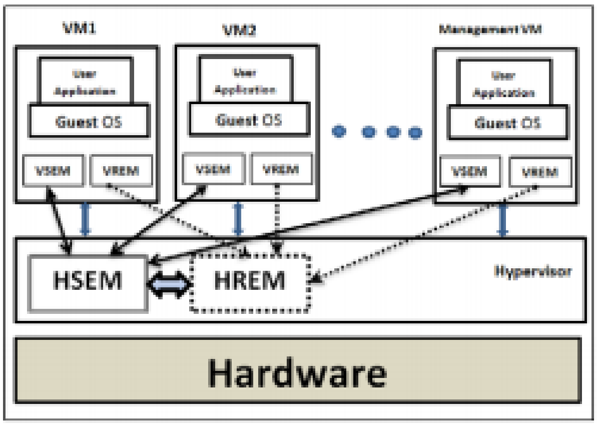


Fig 2 Architecture of secured virtualization

VI. Conclusion

In this paper, we propose virtualization architecture to secure cloud. In the proposed architecture, we try to reduce the workload, decentralize security-related tasks between hypervisor and VMs, and convert the centralized security system to a distributed one. The distributed security system is a very good way to reduce the workload from hypervisor-based virtualization, but this distribution may inject vulnerabilities to cloud. The cloud must work properly and creates an immune environment against attacks, no matter what application is running on the cloud. Moving toward cloud computing requires the consideration of several essential factors, and the most important of them is security.

References

[1] L. Litty, "Hypervisor-based Intrusion Detection," M.S. thesis, Dept. Computer Science, University of Toronto, 2005.

[2] G. Rowel, "Virtualization: The next generation of application delivery challenges," 2009.

[3] G. Texiwill, Is Network Security the Major Component of Virtualization Security?, 2009.

[4] D. E. Y. Sarna, Implementing and Developing Cloud Computing Applications: Taylor and Francis Group, LLC, 2011.

[5] T. Ristenpart and e. al, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the 16th ACM conference on Computer and communications security, Chicago, IL, November 9-13, 2009.

[6] "Securing Virtualization in Real-World Environments," White paper, 2009.

[7] F. Sabahi, "Intrusion Detection Techniques performance in Cloud Environments " in Proc. Conf. on Computer Design and Engineering, Kuala Lumpur, Malaysia, 2011, pp. 398-402.

[8] G. Texiwill, Is Network Security the Major Component of Virtualization Security?, 2009

[9] "Securing Virtualization in Real-World Environments," White paper, 2009.

[10] Cloud Computing, http://www.ibm.com/ibm/cloud/

.