Secure Virtualization in Cloud Computing using Eucalyptus

[1]M. C Padma, [2]Abdul Jabbar. K

[1]Professor and HOD, Department of CSE, PES College of Engineering, Mandya, Karnataka -571401, India

[2]Department of Computer Science & Engineering, PES College of Engineering, Mandya, Karnataka -571401, India

Abstract: The paper aims to ensure the security for virtual machines in cloud computing using Eucalyptus. Cloud computing is the next generation of networking computing, since it can deliver both software and hardware as on demand resources and services over the Internet. Virtualization plays a special role in cloud computing. After virtualization, it has been possible to present compute resources in the form of Virtual Machine (VM) Images. Security is significant concern in cloud computing. In this paper, the existing security challenges of cloud computing and the security threats in Virtual machine interconnectivity are presented first. Because users who are granted super-user access to their provisioned VMs, without care, may have possibilities that a VM can monitor another VM or access the underlying network interfaces. The paper focuses on the security of virtual machine instances by modifying the existing networking model, which can control the inter-communication among VM instances running in Eucalyptus with higher security.

Keywords: Cloud computing, Virtualization, Virtual machine, Eucalyptus**.**

1. Introduction

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the data centres that provide those services. Cloud providers use virtualization technologies combined with self service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as

Infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure. Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and laaS.

2. Virtualization

Virtualization is technology that facilitates sharing of the common infrastructure and resources of a physical machine (e.g., CPU, storage and network interfaces) between several Virtual Machines (VM), each hosting an entire software stack, including the operating system and applications. Typically VMs are offered in different types, each type have its own characteristics which includes number of CPU cores, amount of main memory, etc. and cost. VMs are controlled by a layer of software called a hypervisor, which resides between the hardware platform and the VMs. The hypervisor supports creating, migrating and terminating virtual machine instances. It is also a very critical component in virtualization environments; when breached, all of the attached virtual machines are compromised.

The hypervisors are often categorized within two groups:

- Type 1: Type 1 managers are installed directly above the hardware and run with the highest level of privileges. Xen and VM Ware ESX are type 1 hypervisors.
- Type 2: Type 2 managers are installed above an operating system, like any other program. QEMU and Virtual Box are type 2 hypervisors.

One of the key issues in virtualization is isolation. Isolation plays a crucial role in VMs in order to guarantee that one VM can not affect the other VMs running in the same host.

Virtual network is a method of creating independent or isolate logical network within a shared physical network. We can find many current hypervisors (i.e., Xen, VMware) offering virtual network mechanism for VMs to access physical network. In this paper we take Xen hypervisor as the example to demonstrate how the virtual network works.

Xen, originated as a research project at the University of Cambridge, is the powerful open source industry standard for virtualization. Today, The Xen hypervisor is becoming the fastest and most secure infrastructure virtualization solution. It supports a wide range of guest operating systems including Windows, Linux, Solaris and various versions of the Free BSD. A Xen system has multiple layers, the lowest and most privileged of which is Xen itself. Xen in turn may host multiple guest operating systems, each of which is executed within a secure virtual machine (in Xen terminology, a domain). The first domain, domain 0, is created automatically when the system boots and has special management privileges. Xen offers two modes for users to configure virtual network:

2.1 Bridge Mode

This mode instructs Xen to attach the VM's interface directly to software Ethernet Bridge connected to the physical network. The administrator can handle VM network DHCP requests the same way as handling common network DHCP requests. Figure 1 illustrates the structure of Network Bridge and Virtual Interface (VIF) Bridge in Xen.

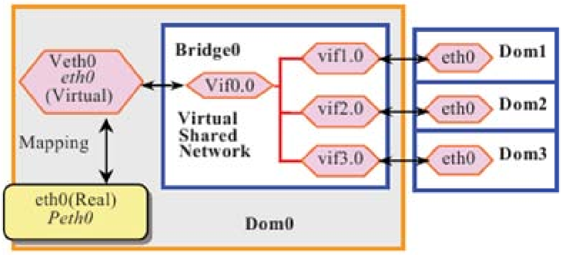

Figure: 1 Structure of Network-Bridge in XEN v.

2.2 Route Mode

The second mode offered by Xen for the configuration of virtual network is route. This configuration allows the administrator to create a point-to-point link between dom0 and each VM. A set of MAC and IP addresses must be defined in advance because routes to each VM should be added to dom0's routing table before a VM is started. So, in this mode, each VM instance created by Xen is assigned a free MAC/IP tuple and released when the VM is terminated. DHCP doesn't work in route mode. Figure 2 presents the structure of route in Xen.

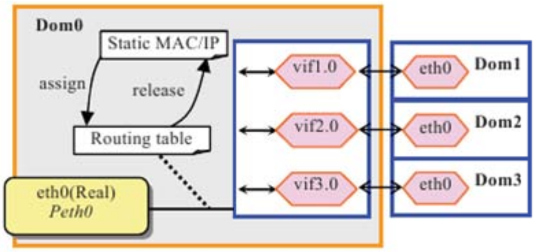

Figure 2: Structure of route in XEN

2.3 Virtualisation Challenges in Cloud Computing

a. The break of isolation. A VM can monitor another one or even have access to the host machine.
b. Data segregation: one instance of customer data has to be fully segregated from other customer data.
c. Privacy: exposure of sensitive information stored on the platforms implies legal liability and loss of reputation;

Remote management vulnerabilities: Commercial hypervisors normally have management consoles as new facilities for administrators to manage VMs. Xen, for instance, uses Xen Centre to manage their VMs. These consoles also open new vulnerabilities, such a Cross-site scripting, SQL injection, etc.

Denial of service (DOS) vulnerabilities: In virtualization environment, resources such as CPU, memory, disk and network are shared by VMs and the host. So it is possible that a DOS will be imposed to VMs which correspondingly take all the possible resources from the host. As a result, the system will deny any request from the guests because of no resources available.

2.4 Dynamic Virtual Machines: VM State and Sprawl.

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

2.5 Vulnerability Exploits and VM-To-VM Attacks

Cloud computing servers use the same operating systems, enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition, co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems need to be able to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualized cloud environment.

3. Eucalyptus Method

In the cloud, VM instance network solution must address connectivity, isolation, and performance. Connectivity means every virtual machine in the same NC or in different NC under Eucalyptus control must be able to communicate with each other. But besides connectivity, the network also has to fulfil the isolation between instances. It is important because users are granted super user access to their provisioned VMs and they may have super user access to the underlying network interfaces. This ability can cause security concerns, in case that if two instances are running on one physical machine, a user of one VM may have the ability to snoop and influence network packets belonging to another. Note that current hypervisor do not support this. This work is done incorporation with the EUCALYPTUS.

The public interface is assigned for communication outside of a given set of VM instances. For example, in an environment that has available public IP addresses, these addresses may be assigned to VM instances at instance boot time. In environments where instances are connected to a private local network and this local network has a router that supports external communication through network address translation (NAT). In this case, the public interface may be assigned with a valid private IP address given by the router.

The private interface is used only for inter VM communication across zones, where VM instances are running inside separate private networks (zones) but need to communicate with one another. Figure 3 illustrates that the instance's private interface is connected via a bridge to a virtual software Ethernet system called Virtual Distributed Ethernet (VDE). VDE is an Ethernet protocol, where users can specify and control virtual Ethernet switch and cable abstractions that are implemented as programs. When a system is initiated, it sets up a VDE network overlay that creates one VDE switch per CC and NC component and many VDE wire established between switches. The VDE switches support a spanning tree protocol, which allows redundant links to exist while preventing loops in the network.

At instance run time, the NC responsible for controlling the VM creates a new Ethernet bridge that is connected to the local VDE switch and configures the instance to attach its private interface to the new bridge. At this point, our requirement of instance connectivity is satisfied, because any VM started on any NC will be able to contact any other VM over the virtual Ethernet. Currently, Eucalyptus allows the administrator to define a class B IP subnet that is to be used by instances connected to the private network, and each new instance is assigned a dynamic IP address from within the specified subnet.

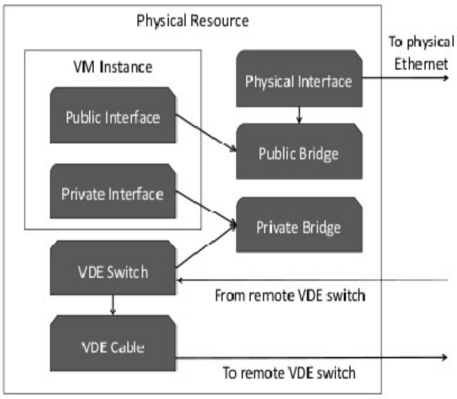

Figure: 3 Each VM instance is assigned a public interface for external network connections, and a private interface connected to a fully virtual Ethernet network for inter VM Communication.

Now the second requirement of the virtual network is network traffic isolation between instances. As mentioned from the beginning, we want that if two instances, owned by separate users, are running on the same host or on different hosts connected to the same physical Ethernet, they do not have the ability to inspect or modify each other's network traffic. To solve this problem, simply use the concept of a virtual local area network (VLAN). In VLAN every set of instances owned by a particular user is assigned a tag, inserted into every communicated frame header that is then used as an identifier assigned to that user's instances. VDE switch ports then only forward packets that have the same VLAN tag. So a set of instances will only be forwarded traffic on VDE ports that other instances in the set are attached to, and all traffic they generate will be tagged with a VLAN identifier at the virtual switch level, thus isolating instance network traffic even when two instances are running on the same physical resource. Figure 4 illustrates this scenario.

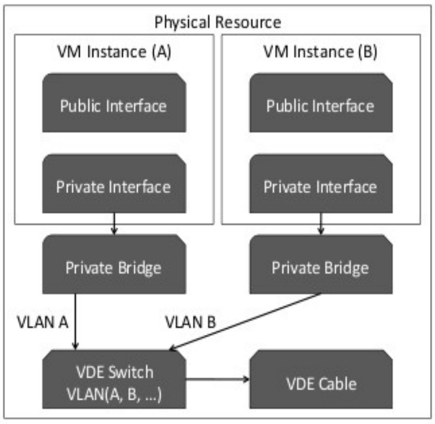

Figure 4: Two instances owned by user A and user B running on the same physical resource are connected to the VDE network through ports configured to only forward traffic based on a particular VM's assigned VLAN.

4. Measures to Control VM Security

A variety of distinct security technologies should be deployed to achieve comprehensive VM-level security that increases protection and maintains the compliance integrity of servers and applications, whether in virtual or cloud environments. These include security layers such as firewalls, intrusion detection and prevention; file integrity monitoring, log inspection, and anti-malware protection.

- A firewall decreases the attack surface of virtualized servers in cloud computing environments. A bi-directional stateful firewall, deployed on individual VMs, can provide centralized management of server firewall policy. It should include pre-defined templates for common enterprise server types.
- Intrusion detection and prevention systems (IDS/IPS) intervene against attacks that attempt to exploit known vulnerabilities long before patches are published or deployed. Implementing IDS/IPS within the virtualized environment can shield applications and operating systems from newly discovered vulnerabilities. This achieves timely protection against known and zero day attacks. In particular, vulnerability rules shield a known vulnerability– for example, those disclosed monthly by Microsoft – from an unlimited number of exploits.
- File integrity monitoring inspects files, systems, and registry for changes. Integrity monitoring of critical operating system and application files (e.g., files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes that could signal a compromise of virtual and cloud computing resources.
- Log inspection provides visibility into important security events captured in log files. Log inspection rules optimize

the identification of important security events buried in multiple log entries from numerous sources. These events can be aggregated and sent to a stand-alone security system, or forwarded to a security information and event management (SIEM) system for correlation with other infrastructure events, reporting, and archiving.

- Anti-malware protection defends against viruses, spyware, Trojans and other malware. It should detect malware in real time and incorporate cleanup capabilities to help remove malicious code and repair any system damage caused by the malware.

5. Results and Discussion

The paper focuses on the security of virtual machine in cloud computing. Virtualization is a key feature of cloud computing. After virtualization, it has been possible to present compute resources in the form of Virtual Machine (VM) Images. Security is significant concern in cloud computing. One of biggest challenges of security issues in the design of a cloud computing platform is that of virtual machine (VM) instance interconnectivity. Because users who are granted super-user access to their provisioned VMs, without care, may have possibilities that a VM can monitor another VM or access the underlying network interfaces

The proposed method is implemented using Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems). The Experiment using the existing architecture shows that the virtual machines are vulnerable to attacks such as spoofing and sniffing. The enhanced novel model can be effectively used for virtual machine interconnection without further security threats.

6. Conclusion and Future Work

The inability of physical segregation and hardware-based security to deal with attacks between virtual machines on the same server highlights the need for mechanisms to be deployed directly on the server, or virtual machines. Deploying a line of defence including firewall, intrusion detection and prevention, integrity monitoring, log inspection, and malware protection as software on virtual machines is the most effective method to maintain integrity of compliance and preserve security policy protection as virtual resources move from on-premise to public cloud environments

Eucalyptus is still young and under development. Eucalyptus 1.5.1 doesn't support a http POST request, so when we tried to implement a POST request, it returns undefined errors. Although Eucalyptus has the same interface as Amazon, it has some differences too. Eucalyptus uses hypervisors to control life cycles of instances. The hypervisors may have their special networking configurations, or hypervisor like Xen needs a xenified kernel to run with (but KVM not). Or Xen currently doesn't get support from Ubuntu with a xenified kernel. So the work can be expanded to support all the hypervisor such as Xen, etc.

References

[1] Z. Pervez, Sungyoung Lee, Young-Koo Lee. Multi-Tenant, Secure, Load Disseminated SaaS Architecture. In proceedings of the 12th Advanced Communication Technology (ICACT) International Conference. Phoenix, USA, 2010, pp. 214 – 219.

[2] Hanqian Wu, Yi Ding, Chunk Winer, Li Yao - Network security for virtual machines in cloud computing, International Conference on Services Computing , 2011, pp. 564-520.

[3] B. R. Kandukuri, R. P. V. and A. Rakshit, "Cloud Security Issues ," in Proceedings of the 2009 IEEE International Conference on Services Computing , 2011, pp. 517-520

[4] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," Cloud Computing, IEEE International Conference on, vol. 0, pp. 109-116, 2010.

[5] Neil MacDonald. Security considerations and best practices for securing virtual machines. Gartner, Inc., March 2011

[6] J. Kirch. Virtual Machine Security Guidelines Version 1.0. The Centres for Internet Security, September 2010.

[7] Xen Networking (July 2010), http://wiki.xensource.com/xenwiki/XenNetworking.

[8] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.

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

Author Profile

Dr. M. C. Padma received her B.E. Degree in Computer Science and Engineering and M.Sc. Tech. by Research degree from University of Mysore, Mysore, India and Ph.D. from Visvesvaraya Technological University, Belgaum. She is currently working as Professor in the department of Computer Science and Engineering, PES College of Engineering, Mandya, Karnataka. Her main research interests are in the area of image processing, pattern recognition, database management system, data structures, natural language processing, data mining, document image processing, network security and cryptography.

Abdul Jabbar. K born in 1987. He received his graduation in computer Science and engineering from Institution of Engineers India (IEI), Kolkata. Now pursuing M Tech degree in Computer Science and Engineering from PES College of engineering, Mandya, Karnataka, India. He is currently doing training on cloud computing from HASH Solutions, Cochin. His research interests are cloud computing, web services and networking.