SECURITY FOR VIRTUAL MACHINE IN CLOUD COMPUTING

Ms Sindhu S Pandya*

Abstract

Cloud computing is revolutionizing, since its service providers take advantage of virtualization technologies to offer cost-effective access to computing resources via the internet but the revolution comes with new security problems. Among these is the problem of securely managing the virtual-machine and its images that encapsulate each application of the cloud. This paper explains the security concerns arising in cloud computing environments for both administrators and users to maintain compliance integrity and preserve security protection as virtual resources move from on-premise to public cloud environments.

First, we outline the security issues in virtual machines and its images and analyzed using on Update Checker and Online Penetration Suite and an image management system that controls access to images and provides users and administrators with efficient image filters and scanners. Finally this paper presents a novel virtual network framework aimed to control the inter-communication among virtual machines deployed in physical machines with higher security in cloud computing.

Keywords

Cloud Computing, Computer Network Security, Virtual Network, Virtualization

* I/C Principal, Laxmi Institute of Computer Applications(BCA), P.B.- 15, Sarigam P.O., Dist Valsad, Gujarat

1. Introduction:

Cloud computing has emerged as one of the most influential technologies in the IT industry, which can deliver both software and hardware as on-demand resources and services over the internet with lower IT costs and complexities. Many companies such as Amazon, IBM, Google, Oracle, Microsoft, Sales force and HP are rushing to provide cloud solutions in various ways. A Cloud is a pool of virtualized computer resources.

A Cloud can:

- Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications.
- New computer technologies, such as service oriented architecture, virtualization, high power enterprise servers and high band width, support to realize cloud computing platforms.
- Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/ software failures.

To focus on checking the software updates and scans the virtual machines for security vulnerabilities using a component called **Update Checker** for checking the necessity of updates on Linux- Based Virtual Machines. It copies the information about installed packages to database, the check can be executed on the central instance without booting the virtual machine beforehand and shutting it down afterwards. This can also be done using a component called **Online Penetration Suite (OPS)** used to perform periodic online-scanning of virtual machines. One of biggest challenges of security issues in the design of a cloud computing platform is that of virtual machine instance interconnectivity. In this paper, we focus on network security for virtual machines and we select the open source project – Xen hypervisor as the research platform.

1.1 Update checker

The main objective of Update Checker is to detect obsolete software in virtual machines. It has to build a central database that contains all the information required for the task of checking for updates, including the list of installed packages along with its version as well as the list of repositories that are used for each virtual machine. This information has to be imported

into the central database when the virtual machine is first registered, and updated after each change of the virtual machine, i.e., after the installation of new software or the update of already installed software. It can be configured to run the checks at regular intervals, e.g., daily or weekly. Users can be informed about obsolete software in their virtual machines via email.

1.2 Online penetration suite

The main objective of Online Penetration Suite (OPS) is to scan an arbitrary number of virtual machines for security vulnerabilities using multiple security scanners. The OPS combines and interprets the different results and generates a machine-readable and a human-readable report. This allows automatic testing of virtual machines in a virtualized infrastructure to detect known security vulnerabilities, once they are known, the administrators and users can fix them to protect their systems with respect to unwanted attacks. For a scan, the OPS need two input parameters: the names of the target virtual machines and the name of one or more vulnerability scanners. If no scanners are provided, the OPS select all scanners by default. A name uniquely identifies a virtual machine and allows the OPS to obtain further information like the IP and MAC address, path to the disk image(s), etc.

2. Network Security in Virtual Machines:

Security of Virtual Machines:

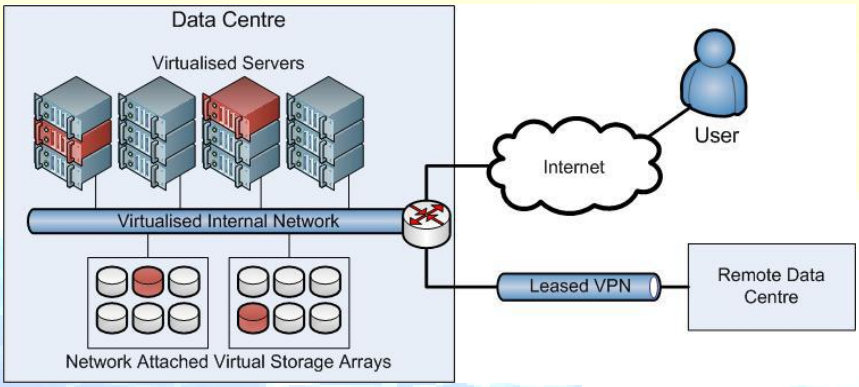
The main purpose of virtualization is to improve the performance of a server by providing users virtual machines within an operating system.

The following security issues:

- The break of isolation. A VM can monitor another one or even have access to the host machine.
- Remote management vulnerabilities. Commercial hypervisors have management consoles as new facilities for administrators to manage VMs. Xen, for instance, uses XenCenter to manage their VMs.
- 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.
- Revert to snapshots problem. Snapshot is a mechanism to allow the administrator to make a snapshot of the machine in a certain point and to revert to the snapshot in case of necessity.

Snapshot also brings some security problems such as using old security policies, re-enabling previous disabled accounts and passwords.

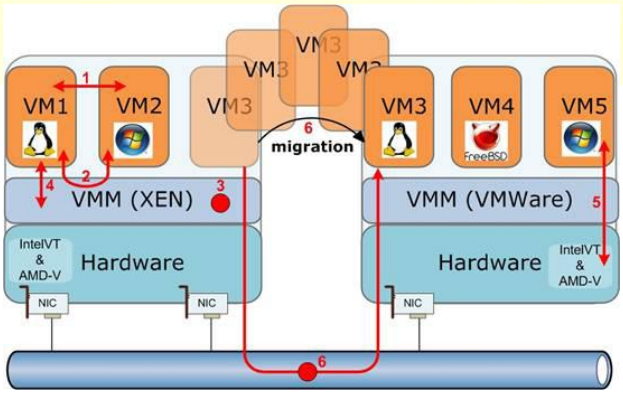
Infrastructure-as-a-service (IaaS) is built on server virtualisation (virtual machine hypervisors such as Xen), network virtualisation and storage virtualisation. The IaaS business model drives infrastructure providers towards a centralised architecture, as depicted in Figure 1.



Connectivity between data centres owned by a single provider is implemented by leased virtual networks providing guarantee, but static quality of service for the IaaS owner. Connectivity between the data centre and the IaaS user is handled by the Internet.

2.1 Virtualisation Environment Threats

Analysis of security threats in virtualisation environments provides some challenges raised by virtualisation of computing resources and networking. Figure 1 represents 6 different security threats that might emerge when a hypervisor is used.

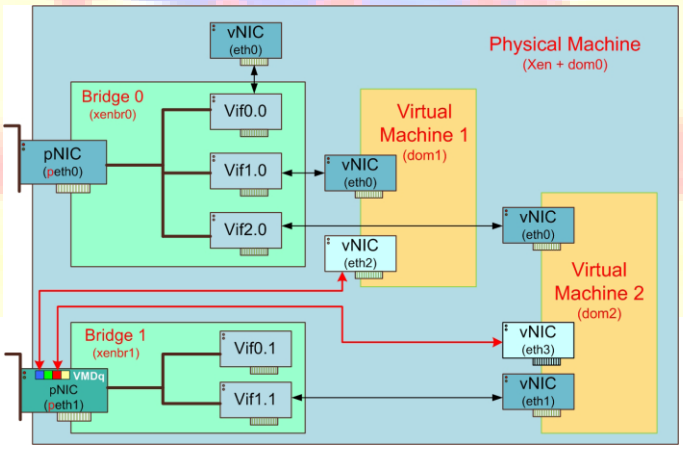


2.2 *Isolation between Virtual Machines*

In isolation each virtual machine uses and reads only its allocated resources. For example, the memory management is subdivided into multiple levels (Hypervisor level, Host VM level and Guest VM level). The Hypervisor can read all the physical memory space. The Host Virtual machine (dom0 for XEN) can read all the memory except the memory allocated to the hypervisor. Guest Virtual Machines (domU for XEN) can only read their allocated memory.

2.3 *Information Theft through Malicious Use of Hypervisor*

To share physical resources, the hypervisor uses different techniques depending on the shared physical components. For example, to share physical network cards, the hypervisor can use Bridged or Routed networking. In Figure below, there are two bridges (xenbr0 and xenbr1) that virtualize two physical network cards (peth0 and peth1). The bridge xenbr0 connects physical interface peth0 to three virtual interfaces (vif0.0, vif1.0 and vif2.0). Each virtual interface is connected to a virtual machine. To ensure that a virtual machine cannot read the packets sent to other VM by introducing Virtual Machine Device Queues (VMDq) and Single Root Input Output Virtualisation (SR-IOV).



2.4 *Untrusted Hypervisors*

If the owner of the physical machine wants to read and steal the data of virtual machines, they can do it using the untrusted hypervisor. For this each user of a virtual machine should have a good contract with the owner of the physical machine, but it is imperative that virtual machines use their own mechanisms to secure themselves.

2.5 U*ntrusted Virtual Machines*

It is possible to have a good contract between the virtual machine user and the hypervisor. A virtual machine can try to get control of the hypervisor using software related security holes without informing the hypervisor. Then, this virtual machine can get control of the physical machine.

2.6 *Unsecure Network Transfer on Inter Device Migrations*

A virtual machine can migrate from a physical machine to another by using traditional or new protocols. It is imperative to protect this migration by using or adapting existing techniques to prevent attacks on migration control mechanisms, transactions, and protocols.

3. Communication Security

3.1 *Secure Virtual Networking*

Virtual networking introduces new security challenges by enabling communication between different virtual components. From a virtual network user's perspective the network might be private but in reality the communication occurs via a public infrastructure. Therefore, mechanisms to secure this communication have to be established. One way is to do it is that the virtual network customer has to care for securing the communication. Another way is to provide secured communication as a service by the virtual network provider, which means that the communication is secured by default and transparent to the customer.

3.2 *Secure Management of Cloud Networking*

For the management of cloud networking, access to the physical infrastructure and to the network properties is needed which should be implemented as a single interface, where a user can specify several parameters on-demand.

3.3 *Security management features for VM images:*

- An access control framework that regulates the sharing of VM images reducing the publisher's risk of unauthorized accesses to the images.
- Image filters that are applied to an image at publish and retrieve time to remove unwanted information in the image. Unwanted information could be information that is private to the user, such as passwords, or malicious, such as malware, or illegal, such as pirated software. Filters address the security risks of all three parties. Filters reduce the publisher's risk of inadvertently releasing private information, the retriever's risk of consuming illegal or harmful content, and the administrator's risk of assuming liability for hosting such content. A provenance tracking mechanism that tracks the derivation history of an image and the associated operations that have been performed on the image. Security functionality like auditing can be built on top of this provenance tracking layer. Provenance tracking provides accountability and discourages the intentional introduction of malicious or illegal content, which in turn reduces the administrator's risk of hosting images that contain such content. We also use the provenance to track modifications to the image that result from applying filters.
- A set of repository maintenance services, such as periodic virus scanning of the entire repository, that detect and fix vulnerabilities discovered after images are published. These reduce the retriever's risk of running malicious or illegal software and the administrator's risk of hosting them.

REFERENCES

1. Sun Microsystems, Inc. Introduction to Cloud Computing Architecture. White Paper, 1st edition, June 2009.
2. Cloud Computing, http://www.ibm.com/ibm/cloud/
3. J. Geelan. Twenty one experts define cloud computing. Virtualization, August 2008. Electronic Magazine, article available at http://virtualization.sys-con.com/node/612375.
4. Virtualization Concept and History (Jan 24, 2010), http://www.remoteitservices.com/content/virtualization-concept-andhistory.
5. Virtualization: What are the security risks? (Jan 22, 2008), http://www.zdnet.com/blog/security/virtualization-what-are-thesecurity-risks/821.
6. Xen Hypervisor (July 2010) - Leading Open Source Hypervisor for Servers, http://www.xen.org/products/xenhyp.html.
7. Cloud Security Is Not (Just) Virtualization Security (Nov 2009), http://whitepapers.zdnet.com/abstract.aspx?docid=1621585.
8. Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.
9. Amazon. Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2.
10. J. Heiser and M. Nicolett. Assessing the Security Risks of Cloud Computing, June 2008.