International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169

Volume: 1 Issue: 1 36 – 39

Cloud Computing Security

Ankur Mishra[1], Ruchita Mathur[2], Shishir Jain[3], Jitendra Singh Rathore[4]

[1,2,4]Asst. Professor, Comp. Science, [3]Student, MCA V Sem., Comp. Science

Lachoo Memorial College of Science & Technology

Jodhpur, Rajasthan, India

ankur.mishra.jodhpur@gmail.com, ruchita.1384@gmail.com, shisaryan@gmail.com, jite2abhay@gmail.com

***Abstract*— Cloud computing has become a growing interest for organizations looking to reduce their IT costs by offloading software costs onto 3rd party organizations who offer software-as-a-service, platform-as-a-service, Security is the key for the Cloud success. There are two technologies Multi-tenancy, Virtualization which provides security about cloud computing.**

Keywords: Virtualization, Multi-tenancy

*****

I. INTRODUCTION

The relative infancy of cloud based computing services, there uncertainty about the level of information security offered by these services. Infrastructure-as-a-service (IaaS) cloud services are largely reliant on virtualization technology, which is seen as providing all the security and process isolation a customer might want. Multi-tenancy and virtualization enable an efficient computing model. Multi-tenancy allows multiple tenants to coexist in the same physical machine sharing its resources (CPU, memory, network...) and, at the same time, creates an isolated environment for each one. Virtualization is the means used to obtain multi-tenancy. Virtualization allows multiple operating systems (OS) to run on the same physical device at the same time. This allows several users to execute their applications on the same physical environment, but isolated from each other. This paper will summarize in the area of cloud security, with a focus on virtualization security.

II. VIRTUALIZATION

Virtualization has been in the IT world for a long time. IBM was the first that introduced the idea in the early 1960's with the term 'Time Sharing'. Virtualization technologies are already established in traditional IT environments, being deployed in many infrastructures. Virtualization of operating systems, also called server virtualization, is defined as "a way of making a physical computer function as if it were two or more computers where each non-physical or virtualized

Computer is provided with the same basic architecture as that of a generic physical computer. Virtualization technology therefore allows the installation of an operating system on hardware that does not really exist." virtualization, resources can be divided or shared through multiple environments, where those environments may be aware of not of the others. These environments are known as virtual machines (VMs), and usually host an OS, which are usually referred as guest Oss.

According to Velte et al., there are two virtualization types that concern cloud computing:

- **Full Virtualization:** In this type of virtualization, a complete installation of one machine is run on another.

- **Paravirtualization:** This type of virtualization allows multiple modified OSs to run on a single hardware device at the same time by more efficiently using system resources

The main difference between them is that in full virtualization the entire system needs to be emulated (BIOS, drive...); but in paravirtualization, the OSs has been modified to work more efficiently with the hypervisor. The use of paravirtualization reduces flexibility since OSs need to be properly modified to run, which means that probably new OSs will need some time before being available on this type of virtualization. Also, there is an increased security impact since the modified OSs have more control over the underlying hardware which can impact on the other virtualized systems and the host OS.

There are also two main types of virtualization architectures:

- **Hosted Architecture:** In this approach, the host OS has a virtualization platform (hypervisor) installed into which one or more VMs run.

- ***Hypervisor Architecture*:** In this approach, the virtualization layer sits on top of the hardware exporting the virtual machine abstraction.

Virtual Machines:-

A **virtual machine** (VM) is a virtualized representation of a physical machine operated and maintained by the virtualization software. VM is a self-contained operation environment. VM is a self-contained operation environment. This environment behaves as a separate computer, emulating the processor, memory, network adapter, removable drives and peripheral devices. VMs provide some benefits over physical machines. VMs are usually compromised by a single or group of files that are read and executed by the virtualization platform. This means that they can be easily migrated from one system to another, copied, or backed up.

Virtual Appliance::-

A virtual appliance (VA) is described as "a pre-packaged software image designed to run inside a virtual machine" Examples of VAs are the virtualized forms of physical network devices such as routers, or switches.
Special type of VAs called virtual security appliance (VSA). A VSA consists of a hardened OS and a single security application, and are usually assigned a higher level of trust to access the hypervisor and other resources like virtual networks running inside the hypervisor. This higher privilege allows the VSA to perform system and management functions. Examples of VSAs are firewalls, anti-virus, or IDS/IPS.

Virtualization Security:-

Cloud computing, virtualization security is again on the mouth of security practitioners. As a recent study by Gartner [GAR10c] indicates, in 2012 around 60% of the virtualized servers will be less secure than the physical servers they replace, hopefully dropping to 30% by 2015. the security of a VM is dependent upon the OS in use; therefore, it should follow the security practices as if the VM was a physical host. From a security point of view, a VM and a physical server do not differ. There are two main ways to access a VM. One is through the hypervisor, and the other is through the network connections. A compromised VM can be used to affect the host servers and other VMs in the same virtual or physical network. Attacks could be launched against these VMs or a DoS attack could be performed in the host server. In the case of Cloud environments, the risk increases since an attacker does not need to compromise a VM in order to attack other VMs or the network. The attacker just needs to pay for a cloud service and, as a consumer, start the attack avoiding the traditional security network devices.
Lindstrom provides an interesting approach listing five immutable laws of virtualization security:

- Law 1: All existing OS-level attacks work in the exact same way.
- Law 2: The hypervisor attack surface is additive to a system's risk profile.
- Law 3: Separating functionality and/or content into VMs will reduce risk.
- Law 4: Aggregating functions and resources onto a physical platform will increase risk.
- Law 5: A system containing a 'trusted' VM on an 'untrusted' host has a higher risk level than a system containing a 'trusted' host with an 'untrusted' VM.

Lindstrom continues and explains that, in a broad sense, the vulnerability level of a system is a measure of the attack surface. An attack surface can be defined as the nature and extent of resources on a system that are exposed and, therefore, attackable. Virtualization increases the vulnerability by adding the attack surface of the hypervisor and the VMM. In cloud computing, virtualization technologies still share the same security issues, but those are increased by the multi-tenant architecture and the erosion of the perimeter. CSA is primarily concern about the impact that virtualization has on network security. Because VMs can now communicate through the hypervisor instead of through the physical network, the traditional network security controls become useless; and express the necessity of these controls to take a new form in the virtual environment.
Another important aspect of the security is the sharing of resources between VMs with different sensitivities, security, and owners. Unless a new security architecture is developed that does not require any network dependency for protection, this risk will always be present
A list of security challenges of virtualization in the Cloud that summarize almost all the problems:

- **Inter-VM Attacks:** The new communication channel created between VMs cannot be monitored using traditional network security controls.
- **Instant-on gaps:** Provide up-to-date security to dormant VMs becomes a difficult task. A compromised image of a VM could potentially create a security breach when instanced.
- **Mixed Trust level VMs:** Several VMs with different security levels could potentially be placed on the same host machine. This is especially concerning when coexisting with unknown tenants.
- **Resource contention:** Accidental or unauthorized use of shared resources can potentially lead to a denial of service.
- **Complexity of management:** Management of the VMs becomes harder than before, requiring more complex patching and configuration policies.
- **Multi-tenancy**: VMs now coexist with other unknown and potentially malicious VMs.
- **Lack of audit trail:** The process of monitoring and log VMs activities becomes more difficult on virtualization environments.

Several issues arise from virtualization in cloud environments, but this can actually become an advantage for organisations. The absence of a security perimeter and the highly volatile nature of VMs will force organisations to adopt robust security processes which can result in a high-security computing infrastructure according to Reese.
This thesis will focus on the threats exposed by a malicious tenant coexisting in the same host system with other tenants in a public IaaS Cloud. More precisely the following threats will be analyzed:

- Virtual machine to virtual machine attacks (VM-to-VM).
- Virtual machine to hypervisor attacks (VM-to-Hypervisor).

III. MULTI-TENANCY

The CSA goes further and states that "multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies" Multi-tenancy has different definitions and importance depending on the services model and deployment models respectively. There are some differences between a SaaS and an IaaS multi-tenant architecture. Depending on the different deployment models, a multi-tenant environment will provide different security concerns. According to IBM, the term multi-tenant means the ability to provide computing services to multiple customers by using a common infrastructure and code base. In a multi-tenant environment, tenants would have a private space and a common space shared amongst all tenants. By sharing resources and creating standard offerings, multi-tenancy reduces costs and improves efficiency of operations. Multi-tenancy makes use of virtualization technologies to increase resource utilization, load balancing, scalability, and reliability; and the use of automation reduces complexity, decrease operation costs, and increase provisioning speed.
Multi-tenancy can be applied to different levels. Depending on the level, the multi-tenancy architecture will lead to different concerns. According to IBM these levels can include:

- **Application level.** Multiple tenants use an application which provides logical separation between users, access controls, and customization.

- **Middleware level**. Multiple applications use the same middleware which provides logical separation, access controls, and resources.
- **Operating system** (OS) level. Multiple middleware runs under the same OS which provides access controls, logical separation, and resources to the middleware.
- **Hardware level.** The hardware provides logical separation, access control and resources to each OS instance. In this level, each OS is considered a tenant.

The most typical components that can be shared across multiple tenants are:

- Storage.
- CPU processing.
- Memory.
- Network bandwidth
- Management.
- Provisioning.
- Complexity.
- Power Usage.
- Billing or chargeback.

Virtualization technologies are the key to solve these problems. Virtualization provides a mean to maximize the efficiency of sharing these resources through several mechanisms

Multi-Tenancy Security:-

The capability of multi-tenancy to share resources is a key element for cloud computing. However, multi-tenancy is

also one of the main security concerns according to CSA and ENISA.

Virtualization is the means used to achieve multi-tenant environments, so they share many of security risks. From a high point of view the idea of sharing resources and the coexistence of different tenants that are unknown to each other, enables all the security risks.

In order to avoid tenants affecting each others' operations when running on the same host machine, it is necessary to employ a strong compartmentalization; and it is of utmost importance that consumers cannot access other consumer's data, network traffic, or any other information related

Multi-tenancy architectures allow servers that were under used until now to be efficiently managed to reallocate the spare resources. Multiple tenants can coexist in the same host machine making the most of their CPU, memory, and networking capabilities. In public clouds, organisations put at risk their data and operations sharing 'houses' with other unknown tenants, which can perfectly be malicious attackers with thirst of get some rewards.

IV. CONCLUSION

Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.

Cloud computing several technologies and architectures should be mixed to enhance the features, in particular multi-tenancy and virtualization; but they bring their own security concerns to the already large list of cloud computing. As multi-tenancy, virtualization comes with its own issues. The hypervisor provides a new attack surface to be compromised; and the virtual network enables a malicious VM to perform attacks on other VMs avoiding traditional network security controls. This requires a new form to approach network security like using privileged VMs; but this also generates new security risks if being compromised.

CSA accurately states that "the lowest common denominator of security will be shared by all tenants in the multi-tenant virtual environment unless a new security architecture can be achieved that does not 'wire in' any network dependency for protection".

The movement to the Cloud could mean an improvement in security to many organisations. New robust security controls will be required in order to assure proper security with the de-perimeterization, and to be compliant with the everyday more strict laws and regulations.

V. REFERENCES

[1] Amazon EC2, http://aws.amazon.com/ec2/

[2] Google App Engine, http://code.google.com/appengine/

[3] Google Apps, http://docs.google.com/

[4] Nessus, http://www.nessus.org/

[5] Amazon Web Services, Zeus Botnet Controller, Accessed on July 2011, http://aws.amazon.com/es/security/zeus-botnet-controller/

[6] A. Cargile, Hypervisor Security Concerns, December 2009, http:// thecoffeedesk. com/ news/ index.php/ 2009 / 12 / 01/hypervisor-security-concerns/

[7] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009, https://cloudsecurityalliance.org/wp-content / uploads / 2011 / 07/csaguide.v2.1.pdf

[8] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March 2010, https:// cloudsecurityalliance.org/ topthreats/ csathreats.v1.0.pdf

[9] Common Vulnerabilities and Exposures, CVE-2007-1744, Accessed on July 2011, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1744

[10] Gartner, 2011 CIO Agenda Findings, Accessed on July 2011, http://www.gartner.com/technology/cio/ cioagenda_findings.jsp