Security Aspects of Virtualization in Cloud Computing

Payal Jingare, Prof. Priyanka Sorte

Abstract- In Cloud computing, virtualization is that the basis of deliveringInfrastructure as a Service (IaaS) that separates data, network, applications and machines from hardware constraints. Although Cloud computing has been a focused area of research within the last decade, research on Cloud virtualization security has not been extensive. During this paper, different aspects of Cloud virtualization security are explored. Specifically, we've got identified: i) security requirements for virtualization in Cloud computing which might be used as a step towards securing virtual infrastructure of Cloud, ii) attacks that may be launched on Cloud virtual infrastructure.

Index Terms— Cloud Computing, Cloud virtualization security, Cloud service provider, Attacks on virtualization, hypervisor, virtual machines, disk images.

INTRODUCTION

Cloud computing is becoming popular among IT businesses thanks to its agile,flexible and value effective services being offered at Software, Platform and Infrastructure level. Software as a Service (SaaS) allows users to access applications hosted by different vendors on Cloud via internet. Platform as a Service (PaaS) enables developers to code, test and deploy their applications on IaaS. In Infrastructure as a Service (IaaS) model, Cloud providers offer services like computing, network, storage and databases via internet. IaaS is that the base of all Cloud services with PaaS and SaaS both built upon it. the first features of IaaS are elasticity and virtualization [1]. Virtualization enables one system to concurrently run multiple isolated virtual machines (VMs), softwares or multiple instances of one operating system (OS). However, there are still open challenges in achieving security for Cloud virtualization. This paper analyzes the safety problems with Cloud virtualization from three different aspects including the safety requirements, attacks and security solutions of virtualization. Therefore, the contribution of this paper is three-fold. This paper: i) presents general requirements for securing Cloud virtualization environment, ii) describes possible attacks that may be launched on different virtualization components (hypervisor, VMs, images).

2 Security Requirements of Virtualization

Different virtualization approaches are often applied to varied system layers including hardware, desktop, OS, software, memory, storage, data and network. Full virtualization could be a variety of hardware virtualization that involves complete abstraction of underlying hardware and provides better operational efficiency by putting more work load on each physical system [2].

- *Payal Jingare is currently pursuing masters degree program in Information technology in PHCACS, Rasayani in Mumbai University, India, PH-7057640590. E-mail: payaljingare1212@gmail.com*
- *Priyanka Sorte is currently a professor in masters degree program in PHCACS, Rasayani in Mumbai University, India, PH-8097770691. E-mail:.psorte@mes.ac.in*

Full virtualization is often categorized into two forms: i) bare metal virtualization and ii) hosted virtualization.

Bare Metal (Hypervisor)

- Virtualization Engine Installs Directly on Hardware
- No reliance on an underlying OS
- VMware ESX Server, XEN, MS Hyper-V

Hosted

- Relies on an underlying OS
- More security implications because of the reliance on the Underlying
- VMware Workstation, VMware Server, VMware Player, MS Virtual PC and Server [13]

Bare metal approach is usually used for server virtualization in large computing systems like Cloud computing because it provides better performance, more robustness and agility. The architecture of bare metal based virtualization generally employed in Cloud the unique characteristics of virtualization together with their benefits even has some drawbacks. Each component of virtualization has to be secured from the possible threats. In general, before planning and implementing security of any system it's important to know the protection requirements of that environment. This sections attack in Cloud in presents general requirements to forestall virtualization layers attacks in cloud.

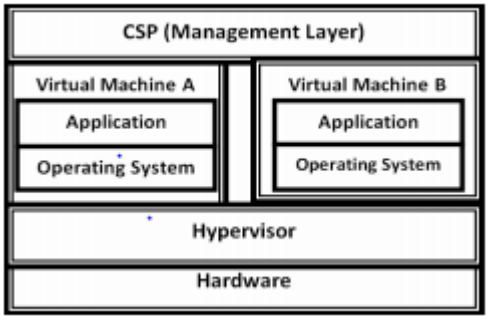

Fig.2 security requirements of virtualization

2.1 Service Provider Requirements

A service provider (SP) provides organizations with con-

sulting ,legal,real estate,communications,storage,processing although a service provider can be an organizational sub-unit,it is usually a third party or outsourced supplier,including telecommunication service provider (tcsp) ,application service providers(ASPS),storage provider(SSPS),and internet service providers (ISPS)[11] report by Alert Logic [5] shows that one-half of Cloud users consider service provider security as a big threat. To secure the virtualization hardware, (Cloud) service provider must limit access of hardware resources to authorized person. Similarly, proper access control should be implemented within the management layer, so each administrator has access only to its concerned data and software.

2.2 Hypervisor Requirements

Hypervisor provides the mandatory resource management functions that enable sharing of hardware resources between the VMs. Hypervisor must maintain the isolation between VMs and support multiplexing of multiple VMs on single hardware platform [6]. It must make sure that no application from any VM can directly take control of it as a number to change the ASCII text file of hypervisor and other VMs in the network. Hypervisor should also monitor the guest OS and applications in VMs to detect any suspicious behavior [7]. Programs that control the hypervisor must be secured using similar practices used for security of programs running on servers. Similarly access to the hypervisor must be restricted. Other security measures to secure hypervisor include installing updates to the hypervisor, restricting administrator access to the hypervisors management interfaces and analyzing hypervisors logs to work out if it's functioning properly.

2.3 Virtual Machine Requirements

Limit on VM resource usage must be assigned so as that malicious VMs is also restricted from consuming extra resources of the system [4]. Moreover, isolation between virtual machines should be provided to create sure that they run independently from each other. To secure the guest OS running in virtual machines, best practices for the protection of physical machines must be followed that include updating the OS regularly for patches and updates, using anti-virus software, securing internet and email and monitoring of guest OS regularly [3]. Privileged VM (Domo) is that the primary domain started by XEN hypervisor after boot. it's in command of monitoring the communication between the remote users and guest VMs. Dom0 is additionally in command of creating and destroying all guest VMs and providing device drivers to the guest VMs. Domo should boot the guest VMs without tampering them. The state of the VM saved as a disk file in Domo must remain confidential, and it must not be tamperory.

2.4 Guest Image Requirements

Whenever VM is migrated from one physical machine to different, images on previous disks should be completely removed. Similarly, data on old broken disks should even be removed before they're discarded. Furthermore, backup of the virtual machines images must be maintained. VM checkpoint may be a feature that enables the users to require snapshot of VM image within the persistent storage. Snapshot records the state of the running image that contains all components of the guest OS. Snapshot is mostly captured as a difference between the image and therefore the running state. the main function of checkpoint is to revive VM to its previous state if the VM enters any undesired state. However, the snapshot access should be to authorized users and checkpoint must be used only to return VM to a stable and non-malicious stat**e.**

3. Attacks on virtualization

Each component of virtualization layer can act as an attack vector to launch multiple attacks on the system. Attacks that target different components of virtualization environment may result in security issues such as compromise of complete Cloud infrastructure, stealing of customer data and system hacking. This section discusses different attack scenarios at virtualization environment in Cloud.

3.1 Service Provider Attacks

If the attacker has physical access to the Cloud hardware, he may run malicious application or code within the system to wreck the VMs by modifying their source code and changing their functionality. With the assistance of physical access to system, attackers also can launch cross VM side channel attacks. These attacks include CPU cache leakage to live the load of other virtual web server on the network [10]. It will result in security compromises like loss of information confidentiality and unauthorized traffic monitoring. Service provider has got to make sure that software deployed on Cloud are built using proper coding practices

3.2 Hypervisor Attacks

A Cloud customer can lease a guest VM to put in a malicious guest OS, which attacks and compromises the hypervisor by changing its ASCII text file so as to gain access to the memory contents (data and code) of VMs present within the system [7]. With more features in hypervisor its increased code size has resulted in design and implementation vulnerabilities. to manage the entire virtualization environment malicious hypervisors like BLUEPILL rootkit, Vitriol and SubVir and are installed on the fly, which give attacker the host privileges to modify and control VMs [8]. this method utilized by malicious software to take complete control of the underlying software package by hiding itself from administrator and security software is termed hyperjacking. Another attack within which program running in one VM can get root access to the host machine is termed VM Escape [2]. It's done by crashing the guest OS to get out of it and running an arbitrary code on the host OS. Escaping the guest OS allows the VMs to interact with the hypervisor and provides them access to other guest OS on the system still. Fig. 3.2 shows that the attacker from his virtual machine (VM 2) is in a position to flee his VM. VM 2 is employed to compromise the hypervisor which is further accustomed launch attacks on other VMs (VM 1) in

the system.

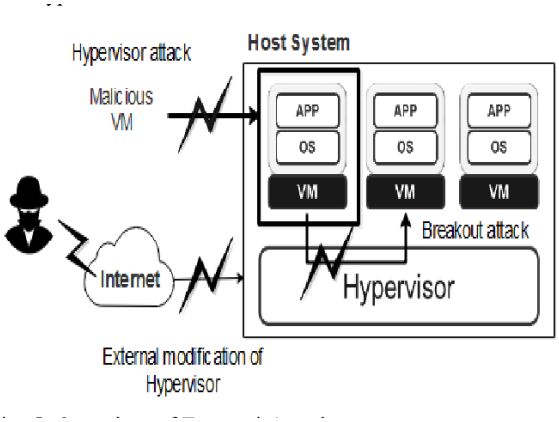

Fig 3.2 hypervisor attacks in cloud computing

3.3 Virtual Machine Attacks

Malicious programs in numerous virtual machines can do required access permissions to log keystrokes and screen updates across virtual terminals [9] that can be exploited by attackers to realize sensitive information. If isolation is not properly implemented covert channels will be used for unauthorized communication with other VMs within the system. Attackers can use Trojans, malwares and botnets for traffic monitoring, stealing critical data and tampering the functionality of guest OS. Conficker, Zeus botnet, command and control botnet communication activity are the samples of such attacks that end in data destruction, operation and creation of backdoors for attackers. Attacks through buggy software, viruses and worms can exploit the guest OS in VMs.

3.4 Guest Image Attacks

Unnecessary guest OS images in Cloud may result in numerous security issues if the security of every image isn't maintained [2]. If a malicious guest OS image is migrated to a different host, it can compromise the opposite system still. Furthermore, creating too many images and keeping unnecessary images can consume resources of the system which might be used as a possible attack vector by attacker to compromise the system [2]. When VMs are moved from one physical machine to other, data of VM images might still exist on previous storage disks that attacker can access. Similarly, attackers may also recover some data from old broken disks [3]. the safety of image backup is additionally a problem. By gaining access to the backup images attacker can extract all information and data. Attacker can access VM checkpoint present within the disk that contain VM physical memory contents and might expose sensitive information of VM state. A new checkpoint may be created by attacker and loaded in system to require VM to any state desired by attacker. If all the checkpoints in storage are accessed, information about previous VM states may be obtained.

4. Conclusion

The paper has presented some of the security flaws in the virtual machine environment. Some of the threats presented here may be considered as benefits in some situations, but they are presented here so that proper care should be taken while designing and implementing the virtual environment.Virtualization is a powerful solution to reduce the operational costs in today's computing but if done wrong it become as a threat to the environment.

The security of cloud can not be maintained unless its virtualization environ-ment is secured. Although different virtualization approaches exist, bare metal virtualization approach is usually utilized in large computing systems like Cloud for server virtualization. This paper presents general architecture of bare metal virtualization and covers security aspects of its different components. Cloud virtualization environment will be compromised by different attacks at service provider, hypervisor, virtual machines, guest software package and diskimages. The attack scenarios at these components are discussed within the paper. to supply security to the virtualization environment, general requirements for vir-tualization security and different existing security schemes that provide security to virtualization environment have also been discussed. Addressing these security aspects will lead towards more extensive research on secure Cloud virtualization environment. In future, an assessment criteria needs to be proposed by which we are able to analyze the effectiveness of security solutions of virtualization against the precise attacks.

References

[1]Orlando, D.: Cloud computing service models. http://www. ibm.com/developerworks/cloud/library/cl-cloudservices1iaas/ cl-cloudservices1iaas-pdf.pdf Last Accessed: 2012-10-27.

[2].Hoffman, P., Scarfone, K., Souppaya, M.: Guide to security for full virtualization technologies. National Institute of Standards and Technology (NIST) (2011) 800– 125

[3].Brunette, G., Mogull, R., et al.: Security guidance for critical areas of focus in cloud computing v2.1. Cloud Security Alliance (2009) 1–76

[4] Council, V.S.I.G.P.S.S.: Pci dss virtualization guidelines v2.0. (2011) 1–39

[5] State of cloud security report: Targeted attacks and real world hacks. http:// www.alertlogic.com/resources/cloud-security-report/ last Accessed: 2013- 04-14.

[6].Szefer, J., Keller, E., Lee, R.B., Rexford, J.: Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM conference on Computer and communications security, ACM (2011) 401–412

[7].Szefer, J., Lee, R.B.: A case for hardware protection of guest vms from compromised hypervisors in cloud computing. In: Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on, IEEE (2011) 248– 252

[8]Ibrahim, A.S., Hamlyn-harris, J.H., Grundy, J.: Emerging security challenges of cloud virtual infrastructure.

(2010)
[9]Reuben, J.S.: A survey on virtual machine security. Helsinki University of Technology (2007)
[10] Zhou, W., Ning, P., Zhang, X., Ammons, G., Wang, R., Bala, V.: Always up-todate: scalable offline patching of vm images in a compute cloud. In: Proceedings of the 26th Annual Computer Security Applications Conference, ACM (2010) 377– 386
[11] https://en.wikipedia.org/wiki/Service_provider
[12]https://www.juniper.net/documentation/en_US/learn-about/LA_SecurityVirtualization.pdf
[13]http://www.cpd.iit.edu/netsecure08/ROBERT_RANDELL.pdf
[14]https://www.researchgate.net/publication/252065709_SPARC_A_Security_and_Privacy_Aware_Virtual_Machine_Checkpointing_Mechanism