Security Aspects of Virtualization in Cloud Computing

Muhammad Kazim, Rahat Masood, Muhammad Shibli, Abdul Abbasi

Security Aspects of Virtualization in Cloud Computing

Muhammad Kazim, Rahat Masood, Muhammad Awais Shibli, and Abdul Ghafoor Abbasi

National University of Sciences and Technology,
Sector H-12, Islamabad - 44000, Pakistan.
{muhammad.kazim,10msccsmmasood,awais.shibli,abdul.ghafoor}@seecs.edu.pk

Abstract. In Cloud computing, virtualization is the basis of delivering Infrastructure as a Service (IaaS) that separates data, network, applications and machines from hardware constraints. Although Cloud computing has been a focused area of research in the last decade, research on Cloud virtualization security has not been extensive. In this paper, different aspects of Cloud virtualization security have been explored. Specifically, we have identified: i) security requirements for virtualization in Cloud computing which can be used as a step towards securing virtual infrastructure of Cloud, ii) attacks that can be launched on Cloud virtual infrastructure, and iii) security solutions to secure the virtualization environment by overcoming the possible threats and attacks.

Keywords: Cloud computing, Cloud virtualization security, Cloud service provider, Hypervisor, Virtual machines, Disk images

1 Introduction

Cloud computing is becoming popular among IT businesses due to its agile, flexible and cost 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 such as computing, network, storage and databases via internet. IaaS is the base of all Cloud services with PaaS and SaaS both built upon it. The primary features of IaaS are elasticity and virtualization [1].

Virtualization enables a single system to concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system (OS). However, there are still open challenges in achieving security for Cloud virtualization. Research has been done to explore major security issues related to virtualization in Cloud. The standard bodies in computing security including National Institute of Standard Technologies (NIST) [2], Cloud Security Alliance (CSA) [3], and Payment Card Industry Data Security Standard (PCI DSS) [4] have issued guidelines on virtualization technologies. These guidelines

discuss security issues related to virtualization in Cloud and provide recommendations for secure virtualization environments. However, the holistic view of virtualization security has not been presented in a composed form. Furthermore, there is need to investigate existing virtualization security solutions proposed in literature to mitigate different attacks.

This paper analyzes the security issues of Cloud virtualization from three different aspects including the security 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 can be launched on different virtualization components (hypervisor, VMs, images), and iii) describes solutions and architectures to provide protection against these different attacks that lead towards a secure virtualization environment.

This paper is organized as follows: Section 2 reviews the security requirements that must be followed to secure virtualization environment. Section 3 describes the major threats and attacks scenarios related to Cloud, section 4 provides existing security solutions for virtualization. Conclusion is given in section 5.

2 Security Requirements of Virtualization

Different virtualization approaches can be applied to various system layers including hardware, desktop, operating system, software, memory, storage, data and network. Full virtualization is a form 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]. Full virtualization can be categorized into two forms: i) bare metal virtualization and ii) hosted virtualization. Bare metal approach is mostly used for server virtualization in large computing systems like Cloud computing as it provides better performance, more robustness and agility. The architecture of bare metal based virtualization generally used in Cloud is shown in Fig. 1.

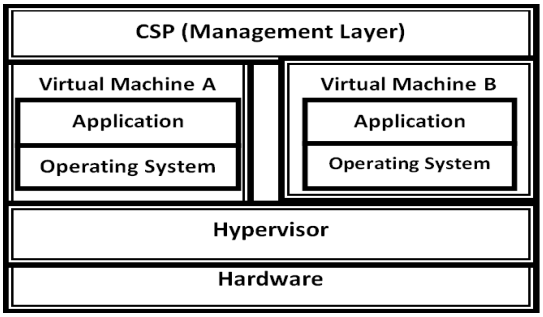

Fig. 1: Bare metal virtualization architecture

The unique characteristics of virtualization along with their benefits also have some drawbacks. Each component of virtualization needs to be secured from the possible threats. In general, before planning and implementing security of any system it is important to understand the security requirements of that environment. This section presents general requirements to prevent virtualization layers attacks in Cloud.

2.1 Service Provider Requirements

A report by Alert Logic [5] shows that 50 percent of Cloud users consider service provider security as a major threat. However, the impact of Cloud service provider on Cloud virtualization security has also not been discussed comprehensively in literature.

To secure the virtualization hardware, (Cloud) service provider must limit access of hardware resources to authorized person. Similarly, proper access control should be implemented in the management layer, so that each administrator has access only to its concerned data and software. The service provider also need to provide strong authentication mechanisms to users. Furthermore, security principles for the development of trusted computing system such as economy of mechanism, complete mediation, open design, principle of least privilege, psychological acceptability must also be followed by the service provider.

2.2 Hypervisor Requirements

Hypervisor provides the necessary 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 ensure that no application from any VM can directly take control of it as a host to modify the source code 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 see if it is functioning properly [2].

2.3 Virtual Machine Requirements

Limit on VM resource usage has to be assigned so that malicious VMs can be restricted from consuming extra resources of the system [4]. Moreover, isolation between virtual machines should be provided to ensure that they run independently from each other. To secure the guest OS running in virtual machines, best practices for the security 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 (Dom0) is the first domain started by XEN hypervisor after boot. It is responsible for monitoring the communication between the remote users and guest VMs. Dom0 is also responsible for creating and destroying all guest VMs and providing device drivers to the guest VMs. Dom0 should boot the guest VMs without tampering them. The state of the VM saved as a disk file in Dom0 must remain confidential, and it must not be tampered [8].

2.4 Guest Image Requirements

Hypervisors use disk images (host files used as disk drive for guest OSs) to present guest OSs with virtual hard drives. Guest OS images can be moved and distributed easily, so they must be protected from unauthorized access, tampering and storage. To securely manage the guest OS images they must be examined and updated regularly according to the requirements. Unnecessary images must not be created and if any image is useless it must be removed from system [2]. Whenever VM is migrated from one physical machine to another, images on previous disks should be completely removed. Similarly, data on old broken disks should also be removed before they are discarded. Furthermore, backup of the virtual machines images must be maintained.

VM checkpoint is a feature that allows the users to take snapshot of VM image in the persistent storage. Snapshot records the state of the running image that contains all components of the guest OS. Snapshot is generally captured as a difference between the image and the running state. The major function of checkpoint is to restore VM to its previous state if the VM enters any undesired state. However, the snapshot access should be given to authorized users and checkpoint must be used only to return VM to a stable and non-malicious state [9].

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 in the system to damage the VMs by modifying their source code and changing their functionality. With the help of physical access to system, attackers can also launch cross VM side channel attacks. These attacks

include CPU cache leakage to measure the load of other virtual web server on the network [10]. Moreover, if access control is not implemented properly, different administrators such as network admin and virtualization admin might access the customer data that they are not authorized to access. These activities will result in security compromises such as loss of data confidentiality and unauthorized traffic monitoring.

Service provider has to ensure that software deployed on Cloud are built using proper coding practices. Flawed coding can result in web application attacks such as SQL Injection, Cross Site Scripting, Denial of Service and Code Execution etc. Alert Logic [5] report shows web application attacks to be the most common attacks on Cloud environment, impacting almost 52 percent customers.

3.2 Hypervisor Attacks

A Cloud customer can lease a guest VM to install a malicious guest OS, which attacks and compromises the hypervisor by changing its source code in order to gain access to the memory contents (data and code) of VMs present in the system [7]. With more features in hypervisor its increased code size has resulted in design and implementation vulnerabilities. To control the complete virtualization environment malicious hypervisors such as BLUEPILL rootkit, Vitriol and SubVir and are installed on the fly, which give attacker the host privileges to modify and control VMs [11]. This technique used by malicious software to take complete control of the underlying operating system by hiding itself from administrator and security software is called hyperjacking.

Another attack in which program running in one VM can get root access to the host machine is called VM Escape [2]. It is done by crashing the guest OS to get out of it and running an arbitrary code on the host OS. Therefore, such malicious VMs can take complete control of 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 as well. Fig. 2 shows that the attacker from his virtual machine (VM 2) is able to escape his VM. VM 2 is used to compromise the hypervisor which is further used to launch attacks on other VMs (VM 1) in the system.

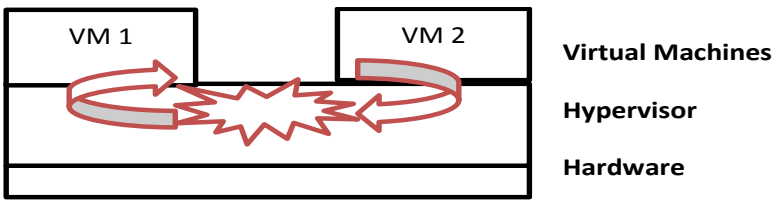

Fig. 2: VM Escape attack (Source: [7])

3.3 Virtual Machine Attacks

Malicious programs in different virtual machines can achieve required access permissions to log keystrokes and screen updates across virtual terminals [12] that can be exploited by attackers to gain sensitive information. If isolation is not properly implemented covert channels can be used for unauthorized communication with other VMs in 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 examples of such attacks that result in data destruction, information gathering and creation of backdoors for attackers. Attacks through buggy software, viruses and worms can exploit the guest OS in VMs. Furthermore, unpatched VM operating systems can be exploited by zero day attacks.

The privileged host virtual machine Dom0 can be compromised by attacker to either tamper boot process of guest VMs or access all guest VMs including their memory, disk space and network traffic. By controlling Dom0 attacker can create too many virtual machines to consume all resources of the system or destroy any virtual machine containing important data by launching DOS attack at Cloud. Furthermore, the saved state of guest virtual machine as a disk file appears in plaintext to Dom0. Attacker can compromise the integrity and confidentiality of the saved VM state and when restored VM may not function as desired [8].

3.4 Guest Image Attacks

Unnecessary guest OS images in Cloud can result in different security issues if the security of each image is not maintained [2]. If a malicious guest OS image is migrated to another host, it can compromise the other system as well. Furthermore, creating too many images and keeping unnecessary images can consume resources of the system which can be used as a potential 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 might also recover some data from old broken disks [3]. The security of image backup is also an issue. By gaining access to the backup images attacker can extract all information and data.

Attacker can access VM checkpoint present in the disk that contain VM physical memory contents and can expose sensitive information of VM state. A new checkpoint can be created by attacker and loaded in system to take VM to any state desired by attacker. If all the checkpoints in storage are accessed, information about previous VM states can be obtained [9].

4 Security Solutions for Virtualization

To cater the attacks on virtualization environment different security solutions have been proposed in literature. This section discusses those security solutions

for each component of virtualization architecture. By implementing these security solutions the attacks discussed in section 3 can be mitigated or at least the impact of those attacks on virtualization environment can be minimized.

4.1 Service Provider Security

Unauthorized person should not have physical access to the virtualization hardware of the system. In order to protect VMs from unauthorized access by Cloud administrators, each VM can be assigned access control that can only be set through Hypervisor. The three core principles of access control namely identification, authentication and authorization will restrict admin access from unauthorized data and system components. Moreover, if any administrator is involved in security compromise, access control implemented in Cloud can help identify that person. Web application attacks can be prevented by installing an application layer firewall infront of web facing applications and by having the customer code reviewed for common vulnerabilities [4].

An online identity management community OpenID has been integrated with an open source Cloud platform OpenStack to provide identity management in Cloud [13]. Sandra R. et al. [14] proposed an architecture using SELinux, XEN, IPsec as tools to enforce Mandatory Access Control (MAC) policies at VM, OS and network layers. These MAC policies control the communication between VMs based on application templates that can be configured by administrators dynamically. Furthermore, the security requirements of virtualized environment differ from that of physical system, Cloud service provider must make sure that the security tools for vulnerability assessment also include the virtualization tools used [3].

4.2 Hypervisor Security

Hypersafe is a system that maintains code integrity of the Hypervisor. It extends the hypervisor implementation and prevents its code modification by locking down the write-protected memory pages. It secures the Hypervisor against the control-flow hijacking attacks by protecting its code from unauthorized access [15]. VM Escape attack can only be executed through a local physical environment. Therefore, the physical Cloud environment must be prevented from insider attacks. The interaction between guest machines and host OS must also be properly configured [12].

In order to stop one VM from affecting or communicating with other VMs isolation must be properly implemented and maintained by hypervisor. Moreover, further possible attack vectors on hypervisors can be reduced by hardening the hypervisor [4]. These techniques include separating the duties of administrative functions, restricting the hypervisors administrator access to modify, create or delete hypervisor logs, and monitoring the hypervisor logs regularly.

4.3 Virtual Machine Security

Administrator must deploy a software or application that stops VMs from using extra resources unless authorized. Moreover, a light weight process must run on a virtual machine that collects logs from the VMs and monitors them in real time to fix any tampering of VMs. The guest OS and applications running on it must be hardened by using best security practices. These practices include installing security software such as anti-viruses, anti-spyware, firewall, Host Intrusion Prevention System (HIPS), web application protection, and log monitoring in guest OS [4]. Protection of VMs by different security practices is shown in Fig. 3.

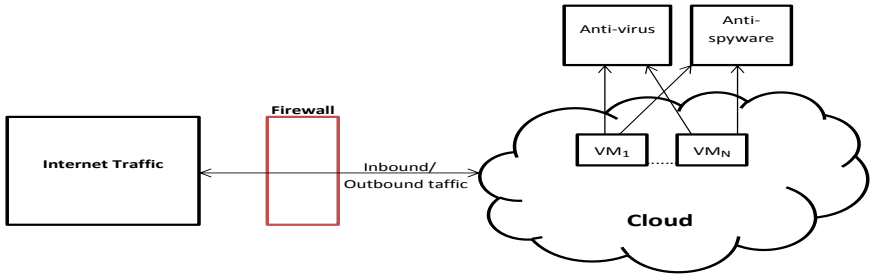

Fig. 3: VM security by firewall, anti-virus and anti-spyware

To identify the faults in guest OS Dan P. et al. [16] proposed a system called "Vigilant". It utilizes virtualization and machine learning methods to monitor VMs through hypervisor without putting any monitoring agent in VMs (out-of-band detection). Flavio L. et al. [17] proposed Advanced Cloud Protection System (ACPS) that monitors and protects the integrity of OS in guest VMs. The periodic monitoring of executable system files is done to check the behavior of Cloud components. It uses virtual introspection techniques to deploy guest monitoring machine in system without being noticed by attacker on guest VM. Hence any suspicious activity on the guest OS can be blocked.

To protect the newly created virtual machines for users (guest VMs) from compromised privileged virtual machine Dom0, a protocol is designed by Jinzhu Kong [8]. Hypervisor generates a pair of secret keys, Kernel and the initrd image are kept encrypted all the time with the secret key Kimg. First the user attests the Cloud server through Trusted Platform Module (TPM), if attestation succeeds then user sends a boot request to the Dom0 which then boots the guest domain. The guest VM executes the wrapping code and requests Hypervisor to decrypt kernel and initrd images. Hypervisor encrypts this request with its private key and asks user for key to decrypt kernel so that a VM can be created. The user sends private key Kimg encrypted under the public key of Hypervisor. Hypervisor decrypts the user message, and the private key Kimg is used to decrypt the kernel, initrd images and to launch the guest virtual machine. In this

way the newly created VM is secured from compromised Dom0. The complete workflow is shown in Fig. 4.

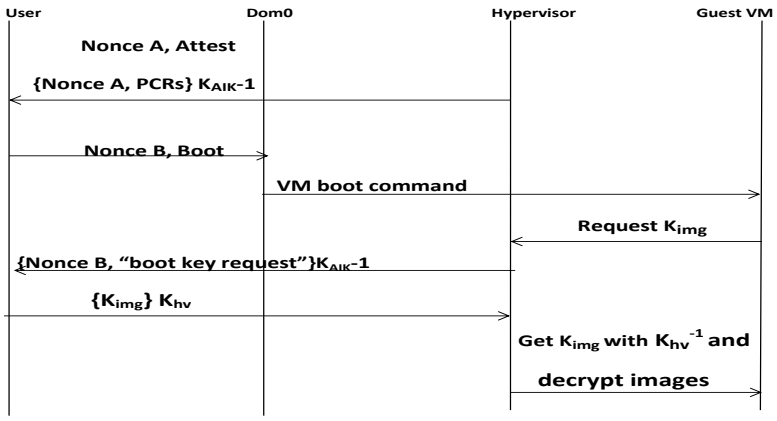

Fig. 4: Secure VM boot protocol (Source: [8])

To avoid the VM storage attacks, before saving the state of the virtual machine in Dom0 its encryption can be done using AES-256, where key can be any random initialization vector. The hash of the encrypted state can be taken using MD5. When the virtual machines are to be restored, the new hash can be taken to verify the integrity of saved virtual machine. If the hash of the restored state and hash of the saved state match it means that the virtual machine state is not altered [8]. Fig. 5 shows the secure storage of saved VM state.

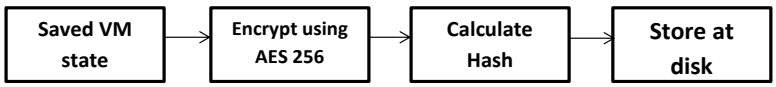

Fig. 5: Securing the saved VM state

4.4 Guest Image Security

Organizations using virtualization must have a policy to manage the creation, usage, storage and deletion of images. Image files must be scanned for the detecting viruses, worms, spyware and rootkits that hide themselves from security software running in guest OS. J. Wei et al. [18] proposed an image management system to efficiently manage images in Cloud and detect security violations in images. It proposes the use of filters, virus scanners and rootkit detectors to provide protection against potentially compromised images. Nuwa [19] is a tool designed

to apply efficient patching to VM images in Cloud. By analyzing patches, Nuwa rewrites the patching scripts so that they can be applied offline. As a result, the installation scripts for online patching can be applied to images when they are offline.

When VMs are to be migrated from one physical machine to another, Cloud admin must recheck and ensure that all data is removed from previous or broken disks. To protect the backup VM images cryptographic techniques such as encryption may be employed to encrypt all backup images. If any VM is deleted then its backup must also be removed from system. Furthermore, to protect VM images from storage attacks, Cloud provider must encrypt the complete VM images when not in use [3].

Checkpoint attacks can be prevented by encrypting the checkpoint files. Another mechanism to provide security to Checkpoints is SPARC. SPARC is a mechanism designed to deal with security and privacy issues resulting from VM checkpoint. SPARC enables users to select applications that they want to checkpoint so sensitive applications and processes cant be checkpointed. Table 1 shows the summary of different security aspects of virtualization discussed in the paper.

5 Conclusion

The security of cloud cannot be maintained unless its virtualization environment is secured. Although different virtualization approaches exist, bare metal virtualization approach is commonly used in large computing systems such as Cloud for server virtualization. This paper presents general architecture of bare metal virtualization and covers security aspects of its different components. Cloud virtualization environment can be compromised by different attacks at service provider, hypervisor, virtual machines, guest operating system and disk images. The attack scenarios at these components are discussed in the paper. To provide security to the virtualization environment, general requirements for virtualization security and different existing security schemes that provide security to virtualization environment have also been discussed. Therefore, the holistic picture of virtualization security in Cloud is provided through structured analysis in which security requirements, attacks and solutions correspond to each other.

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 can analyze the effectiveness of security solutions of virtualization against the specific 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. ALERTLOGIC: 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. Kong, J.: Protecting the confidentiality of virtual machines against untrusted host. In: Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on, IEEE (2010) 364–368
9. Gofman, M.I., Luo, R., Yang, P., Gopalan, K.: Sparc: a security and privacy aware virtual machinecheckpointing mechanism. In: Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, ACM (2011) 115–124
10. Jin, S., Ahn, J., Cha, S., Huh, J.: Architectural support for secure virtualization under a vulnerable hypervisor. In: Proceedings of the 44th Annual IEEE/ACM International Symposium on Microarchitecture, ACM (2011) 272–283
11. Ibrahim, A.S., Hamlyn-harris, J.H., Grundy, J.: Emerging security challenges of cloud virtual infrastructure. (2010)
12. Reuben, J.S.: A survey on virtual machine security. Helsinki University of Technology (2007)
13. Khan, R.H., Ylitalo, J., Ahmed, A.S.: Openid authentication as a service in openstack. In: Information Assurance and Security (IAS), 2011 7th International Conference on, IEEE (2011) 372–377
14. Rueda, S., Sreenivasan, Y., Jaeger, T.: Flexible security configuration for virtual machines. In: Proceedings of the 2nd ACM workshop on Computer security architectures, ACM (2008) 35–44
15. Wang, Z., Jiang, X.: Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. In: Security and Privacy (SP), 2010 IEEE Symposium on, IEEE (2010) 380–395
16. Pelleg, D., Ben-Yehuda, M., Harper, R., Spainhower, L., Adeshiyan, T.: Vigilant–out-of-band detection of failures in virtual machines. Operating systems review **42**(1) (2008) 26
17. Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and Computer Applications **34**(4) (2011) 1113–1122
18. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P.: Managing security of virtual machine images in a cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud computing security, ACM (2009) 91–96
19. Zhou, W., Ning, P., Zhang, X., Ammons, G., Wang, R., Bala, V.: Always up-to-date: scalable offline patching of vm images in a compute cloud. In: Proceedings of the 26th Annual Computer Security Applications Conference, ACM (2010) 377–386

Table 1: Summary of security aspects of virtualization described in paper

Category	Requirements	Attacks	Solutions
Service Provider	Limit access to hardware	Malicious code execution	Develop and implement policy to limit access to hardware
	Implement access control	Stealing of customer data through unapproved access	Implement MAC policies at VM, OS and network layers
	Provide strong authentication mechanisms to users	Unauthorized access to Cloud system and data	OpenID integration with OpenStack Cloud to provide secure authentication
Hypervisor	Maintain isolation between VMs	VM Escape attack	Properly configure the interaction between guest machines and host VM
	Hypervisor should monitor functionality of guest VMs	Customers can lease a guest VM to install a malicious guest OS	Encrypt the VMs to protect them from compromised hypervisor and VMs
	Programs controlling the hypervisor must be secured using best software security practices	Malicious hypervisors attacks including BLUEPILL, Vitriol and SubVir	Hypersafe is a system designed to maintain the integrity of Hypervisor
			Use techniques to harden the hypervisor security
Virtual Machines	There must be limit on VMs resource usage	Using a malicious VM to consume extra resources of the system, resulting in DOS attack	Administrator must deploy a software or application that limits VMs from using extra resources unless authorized
	Isolation between virtual machines should be implemented properly	Malicious programs use covert channels to communicate with other VMs in unauthorized way	Vigilant can monitor faults in guest OS of VM
	Update the OS regularly and use anti-virus software, secure internet and restrict remote access	Malicious programs can monitor traffic, steal critical data, and tampering the functionality of VMs	Security features such as firewall, HIPS, log monitoring must be provided in guest OS
	Guest OS must be monitored regularly for updates and errors	Attacks through worms, viruses, botnets can also be used to exploit the VMs	Use anti-viruses, anti-spyware programs in guest OS to detect any suspicious activity
			Advanced Cloud Protection System (ACPS) can monitor and protect the integrity of guest OS
	Securely boot the guest VMs	Attacker can tamper boot process of guest VMs	Security protocol by J. Kong can be to ensure secure boot of guest VMs
	Saved VM state must not be tampered by Dom0	Attacker can compromise the integrity and confidentiality of the saved state of guest virtual machine	Use encryption and hashing of VMs state before saving VM
Guest Images	Snapshot access must be prevented from authorized access	VM checkpoint attacks	Checkpoint attacks can be prevented by encrypting the checkpoints or using SPARC
	Make a policy to remove unnecessary images	Security issues from unnecessary images can compromise system	J. Wei et al. proposed an image management system to manage images in Cloud
	Apply updates and patches to maintain images secure	Old images are vulnerable to zero day attacks	Nuwa is a tool designed to apply efficient patching to VM images in Cloud
	There must be policy to remove images from old disks after VM migration	Attackers can access and recover data from old and broken disks	After VM migration, Cloud admin must ensure that data is removed from old disks
	Backup of the virtual machines images must be maintained	Unauthorized access to the backup data can result in leakage of sensitive information	Backup of VM images must be encrypted. If any VM is removed then its backup must also be removed