Research on Virtualization Security in Cloud Computing

Lei Chen*†, Ming Xian, Jian Liu and Huimei Wang

1National University of Defense Technology College of Electronic Science and Technology Changsha, China

*corresponding author’s email: 18299927375@163.com

Abstract. Cloud computing services, with its advantages of flexible configuration, efficient utilization of resources and easy management, have achieved rapid development and wide application, in recent years. However, the security issues in cloud computing are also becoming increasingly prominent, at same time, cloud computing security has become an important factor hindering the development of cloud computing. The virtualization technology is one of the core technologies of cloud computing, meanwhile, virtualization security is the core issue of cloud computing security as well. This article introduces the mainstream virtualization technology, reviews the security threats of virtualization in cloud computing, and puts forward the corresponding countermeasures.

1. Introduction
With the rise of cloud computing[1], its technology and concept are becoming mature and popular. In addition, more and more service providers are realizing the great advantages of cloud computing in information processing and use. As a new business service model, it has been recognized and developed rapidly. Virtualization technology is the key technology of cloud computing, but with the wide application of virtualization technology, security issues are also gradually emerging. Its harm degree is far higher than the traditional stand-alone environment, seriously restricted the development of cloud computing industry[2]. The security protection of virtualization in cloud computing is an important measure to promote the safe and orderly development of cloud computing.

2. Virtualization technology
Virtualization[3] is the process by which a computer is virtualized into multiple logical computers, and each logical computer can run a different operating system. What’s more, the applications can run in separate Spaces without affecting each other, thus significantly improve the work efficiency of the computer. VMM is the core software for virtualization and a kind of middle layer software that runs between the physical server and the operating system. It has access to all physical devices on the server, including CPU, memory, disk, and network card. The VMM not only coordinates access to these hardware resources, but also provides protection between the various virtual machines. When the server starts up and executes the VMM, it loads all the virtual machine client operating systems and allocates an appropriate amount of memory, CPU, network, and disk to each virtual machine. The virtualization model is shown in Figure 1.
Depending on the degree and level of virtualization, there are software virtualization and hardware virtualization, full virtualization and paravirtualization. Virtualization technology refers to the technology of realizing virtualization at the software level. On the whole, it can be divided into two camps: open source virtualization and commercial virtualization. Typical examples are Xen, KVM, VMware, Hyper-V and Docker container. Their respective characteristics are shown in Table 1.

| Types       | Characteristics explanation                                                                 |
|-------------|---------------------------------------------------------------------------------------------|
| Xen         | XEN is one of the fastest growing, most stable, and least resource-intensive open source virtualization technologies based on X86 architecture. |
| KVM         | KVM is open source full virtualization that USES QEMU to provide device virtualization, which belongs to the Hypervisor model, supports a variety of hardware platforms. |
| VMware      | VMWare is a global leader in virtualization and cloud computing infrastructure, providing customer-proven solutions that improve IT efficiency by reducing complexity and delivering services more flexibly and nimbly. |
| Hyper-v     | Hyper-v is a hypervisor virtualization technology proposed by Microsoft, can achieve desktop virtualization. |
| Docker container | Docker containers are more portable than traditional virtual machines. Each container has its own file system, processes between containers do not affect each other, and it can distinguish computing word resources. |

3. Security threats to virtualization in cloud computing

3.1. Virtual machine migration

Virtual machine hot migration is done without shutting down the virtual machine, migrate the virtual machine to another physical machine. There are many reasons for performing virtual machine migration, such as maintaining fault tolerance or load balancing. During the migration, the contents of the virtual machine are exposed to the network, which may result in the loss of data privacy and integrity.

3.2. Virtual machine escape

With virtual machines, users can share the resources of the host and achieve mutual isolation. Ideally, a program running in a virtual machine should not affect other virtual machines. However, due to technical limitations and some loopholes in virtualization software, in some cases, programs running in a virtual machine can bypass isolation restrictions and run directly on the host machine, which is called virtual machine escape. When the virtual machine escape attack is successful, it poses a great
threat to both the Hypervisor and the host.

3.3. Rookit attack
Rootkit is a special type of malware that hides itself and specified file processes and network links on the installation target, what is more common is that rootkits are commonly used in combination with other malicious programs such as Trojan and backdoors. Rootkit hides information by loading special drivers and modifying the system kernel.

3.4. Denial of service attack
Virtual machines on the same physical machine share resources. If an attacker USES one virtual machine to obtain all the resources of the host machine, the resources of other virtual machines will also be disturbed, or even crash because there are no resources available, which will result in a denial of service attack in the virtual environment.

3.5. Virtual machine monitor problem
Virtual machine monitor is the key module of virtualization, virtual machine monitors are responsible for both managing and isolating virtual machines and generating or managing virtual resources. If the virtual machine monitor is compromised, all the virtual machines it manages will be controlled by the attacker, and the virtual machine metadata stored by the virtual machine monitor will be exposed to the attacker.

3.6 Decoupling attacks on virtualization platforms
Under the traditional working environment, a single vulnerability can only attack the physical machine with system vulnerability, and the attack scope is very narrow and limited. Multiple rent users based on cloud computing virtualization platform are able to share information of the entire system, and then attack the entire virtual vulnerability platform through a single virtual machine.

4. Countermeasures for virtualization security problems in cloud computing

4.1. Security regime of Hypervisor
At present, the mainstream virtualization software[4], such as Xen, VMware and KVM, all have security holes, It can destroy the Hypervisor's integrity and defenses, the security of the Hypervisor is critical to the security of the virtualization platform.Currently, there are three main aspects of Hypervisor security hardening, the first is to build a lightweight Hypervisor, the second is to protect the integrity of the Hypervisor based on trusted computing technology, the third is to improve the defense capability of Hypervisor by configuring virtual firewall and reasonably allocating host resources.

4.2. Virtual machine security isolation
Through the virtual machine security isolation mechanism, the virtual machines of the users with interests run independently and do not interfere with each other. It is mainly realized from two aspects: first, SMM security memory management model is applied to encrypt the memory through SMM controller, second, SIOM security I/O management model is used to weaken Dom 0 for Xen.

4.3. Virtual machine access control
Security models such as sHype, Chinese wall and BLP are used to reduce the risk of hidden information flow in the virtual machine system, and to control the use of resources and event behavior inside the virtual machine to improve the security of the system.

4.4. Virtual machine security monitoring
To ensure the healthy operation of each virtual machine, virtual machine security monitoring is indispensable[5]. There are two mainstream virtual machine security monitoring architectures. One is
the monitoring architecture based on virtual machine introspection technology, which puts the monitoring module in the Hypervisor and detects other virtual machines through virtual machine introspection technology. The other is the security active monitoring architecture based on virtualization, which intercepts the change of system state by inserting some hook functions into the monitored virtual machine and jumps to a separate secure virtual machine for monitoring and management.

4.5. Virtual trusted computing technology

Through the trusted measurement trusted storage and trusted report mechanism provided by trusted computing, the computing environment of terminals is purified, the trusted connection between terminals is built, and the virtual space of honest mutual trust is built. The dynamic integrity of the virtual machine is guaranteed by the trusted measurement mechanism, the trust communication between different virtual environments is realized by the trusted report mechanism, and the data migration storage and access control is guaranteed by the trusted storage mechanism.

Strengthen the virtualization security protection in cloud computing from the above five aspects can effectively promote the virtualization security of cloud computing, so as to improve the security and reliability of cloud computing services. The overall virtualization security protection model is shown in Figure 2.

![Figure 2. Virtualization security protection model](image)

5. Conclusion

Virtualization plays a major role in reducing administrative costs and increasing the availability and flexibility of hardware resources. As the core of the cloud computing technology, virtualization is facing security threats hindered the rapid development of cloud computing and widely used. It is of great significance to analyze the main security threats faced by virtualization technology and strengthen the security protection of virtualization.

References:

[1] Sharma, S., Soni, S., Sengar, S., (2012) Security in cloud computing National Conf. on Security Issues in Network Technologies, 1-6.
[2] Sen, J., (2013) Security and privacy issues in cloud computing Retrieved from arxiv.org/pdf/1303.4814.
[3] Khurana, S., Verma, A.G., (2013) Comparisons of cloud computing service model: SaaS, PaaS, IaaS International Journal of Electronics & Communication Technology (IJECT), 4 3 29-32.

[4] Ashraf, I., (2014) An overview of service model of cloud computing Int. J. of Multidisciplinary and Current Research 2, 779-783.

[5] Zhang, T., Lee, R.B., (2016) Monitoring and Attestation of Virtual Machine Security Health in Cloud Computing [J]. IEEE Micro, 36(5): 28-37.