A Review of Virtual Machine Attack Based on Xen

Ren xun-yi[1,a], Zhou yu-qi[1]
[1] College of Computer Nanjing University of Posts and Telecommunications, 210023 NanJing, China

Abstract: Virtualization technology as the foundation of cloud computing gets more and more attention because the cloud computing has been widely used. Analyzing the threat with the security of virtual machine and summarizing attack about virtual machine based on XEN to predict visible security hidden recently. Base on this paper can provide a reference for the further research on the security of virtual machine.

1 XEN virtual machine security character

Virtual machine infrastructure is consist of VMM, VM and Domian0, then discussing each of these in the following sections from function that undertaking in the XEN platform. The paragraph show that in terms of security to analyze excising problems

1.1 VMM

VMM belong to the software layer which locating between computer hardware and operating system and running in the privilege level[1]. It is in charge of managing and isolating VM which running at the higher layer to offer security and department running environment. Meanwhile, VMM are valid for a virtual environment that is irrelevant to the real hardware with virtualization, such as monitor, hard disk, CPU, memory, network hard etc[1,3]. In conclusion, VMM is not only a multitasking management tools but also a solution with high security and strong reliability. On the basis of the location of VMM in the computer can divide it into three kinds of modes: independent monitoring mode, host mode and mixed mode. VMM is also called XEN Hypervisor or XEN and VM is called Domain in the XEN[3].

1.2 Domain0

A special virtual machine exist in the XEN called Domain0 by reason of mixed mode used in the XEN.Domian0 is defined as privileged domain, it supervise other Domain(called DomainU) to provide virtual source service, particularly the other Domain access to I/O devices[3].

Domain0 is unique as assistant of XEN, it create with XEN running and become the first Domain which running in the XEN. Domain0. Dom0 possess Native Drive and have privilege to access hardware device. By using of control interface to control other Domain. Control Panel running in the Domain0 can manage creation, destroy, configuration and migration of other Domain. While Device Manager is responsible for initialization of device driver and visit of manage device. Furthermore, Domain0 can empower other Domain to access device, all of these Domain which was equipped with power to access real hardware device by using of Native Device. Thus it can be seen that VMM and Domain0 become the focus of attack object, it is easy to acquire information of DomainU once attacker access to the highest authority of virtual machine.

1.3 VM

VM possess independent ISA structure and veritable hardware device which simulated in the hardware platform. Different operating system can execute in each virtual hardware system, called Guest OS, each one of them access real hardware source via VMM[1].

2 VM attack

The previous section introduced XEN virtualization simply, and point out key character of VM. In this section will introduce all kind of VM attacks at present.

On account of the special of virtual system, it exist more attack point than traditional computer. Mode of VM attack could be divided into four types: gust to host, VM to VMM, VM to VM and outside-attack of VMM.

2.1 VM to Domain0

Domain0 possess the privilege of managing other VM, Attack of VM to Domain mainly attack host via VM to acquire administration of the host. The most famous of which is escape attack of VM, it utilize loophole of software running in the VM to conquer the field of attack or control VM system. VM via leakage of software to bypass VMM monitor, by this way hacker can access Dom0 directly and acquire privilege of

[a] Corresponding author:renxy@njupt.edu.cn

Domian0.Then, attacker can control all the VM in this system.

In 2015, XEN exposed a loophole named Dome Breaking and numbered XSA-148/CVE-2015-7835. This loophole stared to arise in version 3.4 and in version 4.6 have been impacted. It is easy for attacker to come true escape when they utilize a VM running in the mode of PV. Furthermore, attacker can take control of XEN Hypervisor, Domain0 and other VM running in the single physical machine. Dome Breaking exist in memory management facility. On security grounds, XEN set page table page as not be writable. So, PV DomU can not modify its page table directly, it only via Hypercalls to apply for altering page table. XEN Hypervisor will instead of PV DomU to modify page table while request checked off by it. However, XEN provide a quick selection that is to say request is able to skip strict process while the request be verified security by XEN Hypervisor. This strategy cause serious problem that quick update logic allow new Page Directory Table Entry(PDE)to carry the flag of _PAGE_PSE and _PAGE_RW when XEN Hypervisor update item of page table in Page Directory Table(PDT)[4]..

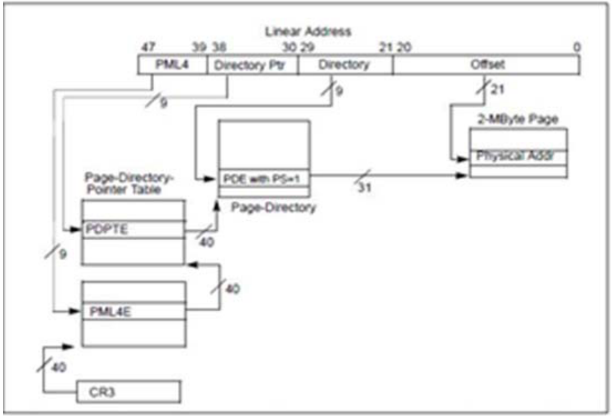

Figure 1. 2M paging mapping in MMU

Flag of _PAGE_PSE in PDE can lead MMU to allow process to use page in the size of 2M.In this case, whether allow to execute quick update operation applying from PDE request will decided by o12e12e_has_changed(o12e, n12e, _PAGE_PRESENT) routine. This function check that physical page frame number in o12e and n12e is consistent with _PAGE_PRESENT flag, if all of them is match well, updating PDE directly via n12e. At the moment, n12e set the flag of _PAGE_PSE which allow process to access physical memory in the size of 2M requested by n12e rather than 4KB stipulated by XEN, superfluous memory may not belong to this VM. Meanwhile, if o12e include the flag of _PAGE_RW at the same time, aforesaid memory can be written willfully. Analyzing form the point of loophole usage, by means of set the flag of _PAGE_PSE and _PAGE_RW in the PDE, users can push through limitation of 4KB and access memory in the size of 2M. In this condition, attacker can read Page Table maliciously which save in 2M memory aforementioned. Using this method to find breaking the limitation of reading Page Tables only for VM in XEN, attacker can read and write physical memory willfully. Finally, attackers can bypass all the security mechanism and execute malicious code in the context of XEN Hypervisor and Dom0[4].

2.2 Outside attack of VMM

Nowadays, there are two major types of outside attack to VMM, Rootkit attack based on VMM (VMBR) and malicious code.

1) VMBR

Attacker via Rootkit to hide and acquire authority of root, they will leave backdoor next. VMBR write program code into memory and running before VMM start. All of VM will be controlled once program running success. Fairly well known VMBR is Blue pill at present.

2) Malicious code

Hacker using long-distance attack to implant malicious code and remote management technology are mostly using HTTP/HTTPS in VM system. On account of these, attacker can exploit loophole of HTTP to implant malicious code. Such as XSS (cross-site scripting) loophole in API HTTP, attack VM by using of browser to execute malicious script[7,8].

2.3 Attack between two VM

VM to VM mode via access common source to attack, covert channel is famous in all of attack ways which implant code into physical machine because of error in process, memory and other information.

Attack between two VM is called cross-VM attack. In this mode, mainly research mode is coresident that means two VM share common source of physical machine. Attacker can obtain information from cache, CPU and shared memory.

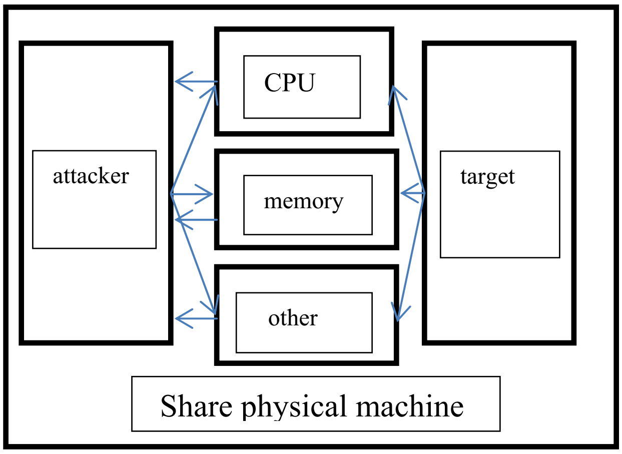

Figure 2. coresident attack mode

Theory of covert channel: Running program with changing in the time, energy and memory. Because the program is different, take time, memory size will be different too. With the number of program running increasing, the leakage of possibility of information increasing too, such as usage of shared memory, CPU utilization, IP address and other information. Different program need different running time, CPU occupancy and memory utilization, large program is able to make the shortage of CPU resource, CPU will always in the condition of high load operation. Attackers can collect changing of utilization to analyse data, transfer regular data through covert channel to acquire valuable information[6].

Take XEN for example, Hypervisor save a table called M2P, it store a relation of machine addresses to pseudo physical addresses. Each Domain can read M2P and via HYPERVISOR_MMU_UPDATE to update table item in the scope of its address. This feather was proved to be used in creating convert channel between two VM. Communication on both of the VM share a structure data, one of the first domain as a flag (two side know each other), and the last domain contains hidden message of actual transmission. In the process of actual transmission, one side update shared data structures to list item in the range of address, the other side traverse M2P items to find opposite side flag, then, according to the excursion in the structure to find hidden message.

CPU load changes can also be used to construct hidden channels. Assume two VCPU in the two VM is mapped to the same physical CPU (or CPU kernel) and running same task, VM as a hidden message receiver execute this task always, as transfer via execute and not execute this task to acquire temporal variation in the receiver. Both of side can agree that the sender does not perform this task transfer 0 bit, and execute this task transfer 1bit. So the receiver analyse bit string form opposite side to grasp utilization of CPU[5].

3 Security of VM

Security of VM can be divided into four types:

1) Security of Hypervisor, ensure hypervisor security, prevent attacker take control of Hypervisor, isolate source between VM, assure security of data storage and confidentially and integrity of machine communication.

2) Trusted computing, establish a credible security domain or trusted computing platform to ensure upper security.

3) Access control, improve access control mechanism constantly.

4) Security application, via security of sand box, intrusion detection and honeypot system for protection.

4 Conclusion

This paper talk about security of XEN mainly and introduce attack mode of VM at present, guest to host, VM to VMM, VM to VM and outside attack to VM. On account of para-virtualization, XEN include two privilege level, VMM and Domain. It is easy for attacker to control other VM and access memory, once they acquire management of VMM and Domain. Attack VMM and Domian0 more frequent than other, second is covert channel or system loophole. Analyse usage of memory or load of CPU and collect running information of other VM. So, when consider to attack a VM, firstly attack host to acquire management of it, this way is easy and difficult. In XEN, possible loophole still threat security, what can we do is improve it in the use constantly.

Acknowledgement

Supported by National Natural Science Foundation of China (61073188), China Postdoctoral Science Foundation (20100471355), the Talent Project of Nanjing University of Posts and Telecommunications (NY208006)

References

1. Lei Shi, Deqing Zou,Hai Jin, M.XEN virtualzation,Wuhan: Huazhong University of Science and Technology Press (2009)
2. Zhongyuan Qin, Risheng Sheng, Qunfang Zhang, Yuxing Di, J. Summarize of security of VM pl. Application Research of Computers(2012)
3. Yingxu Lai, Shaolong Hu, Zheng Yang, J. Research for Security of VM pl. Journal of University of Science and Technology of China(2011)
4. http://xenbits.xen.org/xsa/advisory-148.html
5. Ke Ai, J. Discuss security of virtualization based on cloud pl. Information&Communication, 12(2015)
6. Hang Li, D. Research for security of VM pl. Xidian University(2014)
7. Olivier Heen, Christoph Neuamam, Luis Montalvo, Serge Defrance, D. Improving the Resistance to Side-channel Attacks On Cloud Storage Service pl. IEEE, 6(2012)
8. K. Suzaki, K. Iijima, T. Yagi etc, J. Memory deduplication as a threat to the guest pl. In Proceeding of the Fourth European Workshop on System Security, 1-6(2011)