A survey of virtualization security

Somayeh Sobati moghadam

Abstract—Virtualization is the most rapidly developing technology in IT industry which is cost saving and east for management to deploy. Beside these benefits there are some dark side witch causes the security concerns. Virtualization is an appropriate platform for many potential threats and vulnerabilities that must be addressed. Virtualization brings significant challenges in security such access control failures, vulnerable networks, loss of controlling. Virtualization security should be managed this potential gaps to reduce cost and complexity, thus identifying these challenges plays the important role. In these paper the most common threats in virtualization is presented. We focus on threats that targeted the virtualization.

Index Terms—virtualization security, virtualization security fundamentals, virtualization threats.

1 INTRODUCTION

Virtualization is a revolution in IT world, it offer a lot of benefits for companies and organizations. It provides a framework to use the resources into multiple environments. Separating the applications from hardware, by running multiple OS or applications on a single machine, reducing the amount of cost and providing an isolate environment all are the virtualization benefits. Encapsulating the virtual machines is a reliable way which is used in virtualization. In traditional systems an operating system must be executed in a single machine but in virtualization the management of data is more comfortable. In network configuration, the total infrastructure cost decreases significantly, and make the optimization and best usage of the resources. By creating an abstract layer between hardware and applications, the conflict and ambiguity is diminished. Availability achieved by recovering feature. Decreasing the total ownership's cost, the space required, power and cooling that makes it easier to maintain.Beside all these Strengths, security is a key point. All of this strengths would be meaningless without security. Security in virtual environments means each machines is trusted,warranting that the resources in each machine is encapsulated and cannot pass to another machine. Obviously, it is difficult to trace and monitor all interactions in virtual environment, thus the most important primary requirement is knew and identity the context risks. In this paper, the different type of virtualization will be described and the most important attacks and threat in virtualization will be outlined.

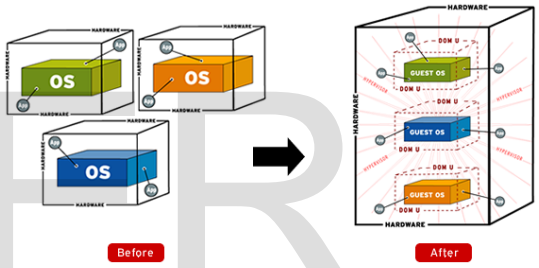

Fig.1 with virtualization multiple OS could be installed on a single

2 TYPES OF VIRTUALIZATION

There are various type of virtualization which is grouped as:

- Desktop virtualization
- Server virtualization
- Storage virtualization
- Network virtualization
- Application virtualization

2.1 Server Virtualization

This is the most important type of virtualization which used to make a mask between users and servers. Server virtualization can be considered as creating virtual servers within a single system. It decreases the number of servers and increases the efficiency of system. Obviously it saves the cost of purchase and maintaining. It provides high amount use of processing power too

.

2.2 Storage Virtualization

• *SomayehSobatimoghadam is obtained mater degree in Information technology at INSA de Lyon university, France. E-mail: s.sobati@hsu.ac.ir*

Storage virtualization resolves the increasing complexity of managing storage by combining multiple storage devices into a single, logical resource with a single view.
Storage virtualization merges storages and logically groping them which decreases archiving, recovery in disasters, backups could be managed easily. Especially it applies to larger SAN or NAS arrays, but it is just as accurately applied to the logical partitioning of a local desktop hard drive [1].

2.3 Network Virtualization

Network virtualization could be defined as ability to manage and prioritize traffic of a network [2]. Network virtualization provide a mechanism to have multiple customized network. It brings more flexibility, scalability, Reliability via optimizing the network speed.

2.4 Desktop Virtualization

Desktop virtualization shares a CPU between several users. Each guest has a separate monitor with a virtual CPU. All guests are connected to a central machine. They are access to all resources and application without necessity of distinct hardware. It could be executed on any type of hardware such as laptop, PCs as well as some smart phones. Desktop virtualization improves management of workstations and their security because it would be ease to keep all guests system up to date and fixed all bugs centrally. Extension of virtual desktop is rapid and easy via copying the original and specifying a special name, so it brings a lot of benefits for big organizations and businesses.

2.5 Application Virtualization

In traditional systems, each user must to install completely the applications, but in application virtualization all applications are available from a remote location. The local user machine provides the CPU and Ram resources and the application is running without installing in user machine. Application virtualization makes a layer between OS and application, so it would be possible to have different version of the same application [3].

3 SECURITY CONCERNS IN VIRTUAL ENVIRONMENT

4.1 Guest Isolation

Isolation is one of the most important feature of virtualization. This means that the process or application in each VM cannot see or affect the others, which is kind of security in virtual machines. If this secure environment is brokenaccessing to the other machine could be ease. Thus this secure abstract guard must be managed and maintained perfectly. Such isolation prevents the guest from internal attacks such as injection.Additionally it decrease the external treats like DOS attacks too.

4.2 VM Escape attacks

Hosts control VMs and interacts with other guests. By breaking out a guest, attacker could access the other guests or hypervisor. This kind of attack in known as escape. Through escape a guest attacker could access to hypervisor and consequently access to all guests. Thus it could be an important legitimate for attackers and must to have a special attention. This attacks are possible through the VMM bugs. Actually the VMM don't offer a complete isolation to prevent this kind of attacks.

4.3 Side-channel attacks

Another threat vector to virtualization is side-channel attack. Attacker try to access the physical properties of hardware. By means of information about resources like CPU use, he try to gain the cryptographic keys.

4.4 The Revert to Snapshots Problem

Taking an image of guest machine is known as "snapshots". This image allows the administrator to recover in the case of disasters. It seen to be crucial but it could bring some security concerns too. An image or a snapshot can insert an un-secure resources again like an unpatched application. The problem of reusing weak-old security mechanisms or old passwords or other sensitive data, which such problems are more dangerous in snapshot because it contain the data of RAM.

4.5 Virtual machine jumping:

Virtualization offers an encapsulated, isolated environments. The virtual OSs should not be able to break out of virtual machine and interact with host or other guests. If there is a security bug in host, a guest can jumps to another VM and compromises its security.

4.6 Packet sniffing:

In virtual environments each guest shares some resources which could be a suitable point for an attack. The insecure physical links provide a

sniffing platform. The interaction between guests achieve using virtual hub or switch. If a hub is implemented, the attacker can compromise the packets in network communication. In the case of using virtual switch anAddressresolutionProtocol (ARP) could be spoofed [4].

4.7 Remote Management Vulnerabilities

The host manages the virtual systems and other guest. Virtual environments provide this facilitate to manage the machines. Hosts have a management console to manage other guests which help to administrators but it could be an attack goal. By compromising the administrative console, the attacker can control all guests east.

4.8 Denial of Service

The resources in virtualization are shared between the host and the guests. It provide the possibility of denial of service (DoS) attacks. A DoS attack make a barrier in resources availability. In virtual environment a guest could cause a DoS attack against host which could take all the possible resources of the system. There are some DoS vulnerabilities in common virtual systems such as VMware [5].

4.9 Virtual-Machine-Based Rootkit (VMBR)

Rootkits are useful tools for hackers because they hide themselves and it's hard to distinguish them. The goal of a rootkit is to run on operating system kernel (ring0). Virtualization adds another ring (ring -1) which the rootkits try to run in this ring. If it achieve to this goal it can control over whole system. If it succeed it would be a VMBR which is difficult to detect and eliminate it [5].

4 Conclusion

Virtualization is a new powerful technology that brings a lot of benefits. All current efforts in virtualization are focused on implementation and its diver's aspects. The security in virtualization is still a challenge which must be addressed. There are no standard definition of virtualization security because there are different type of virtualization technology. In this paper some threats in virtualization was presented. The security concern in virtual environments is that by compromising a host or a guest it could be east to exploit all virtual systems.

References

[1] A. Mann, "Virtualization 101: Technology, benefits and challenges", White paper, enterprise management associates, 2006.

[2] " IBM systems virtualization", vresion2 release 1, 2005.

[3] Jenni Susan Reuben," A survey on virtual machine security". In Jukka Manner andLaura Tackier, editors, Security of the End Hosts on the Internet, Seminar on NetworkSecurity autumn 2007.

[4] J.C. Carvalho, "Security challenges with virtualization", Master's thesis, Dep. Informatics, LisboaUni. ,December 2009.

[5] P. M. Chen and B. D. Noble," When virtual is better than real", In(HOTOS-VIII), SchlossElmau, Germany, May 2001.

[6] Randy Perry Al Gillen, Tim Grieser," Business value of virtualization: Realizing thebenefits of integrated solutions", Technical report, IDC, July 2008.

[7] Christopher Strachey," Time sharing in large fast computers", In International Conferenceon Information Processing, pages 336–341. UNESCO, June 1959.

[8] VMware, Inc. Vmware milestones, 2009. URL http://www.vmware.com/company/mediaresource/milestones.html. Retrieved November 22,2009.

[9] Amit Singh," An introduction to virtualization",URL http://www.kernelthread.com/publications/virtualization/.

[10] Nadir Kiyanclar," A survey of virtualization techniques focusing on secure on-demandcluster computing",ArXiv Computer Science e-prints, November 2005.

[11] J. Smith , R. Nair,"Virtual Machines: Versatile Platforms for Systems and Processes",The Morgan Kaufmann Series in Computer Architecture and Design, MorganKaufmann Publishers Inc., San Francisco, CA, USA, 2005.

[12] M.Rosenblum, T. Garfinkel," Virtual machine monitors: Current technologyand future trends", Computer, 38(5):39–47, 2005.

[13] G. Milos, D. G. Murray, S. Hand, and M. Fetterman. Satori: Enlightened Page Sharing.In Usenix, 2009.

[14] J. S. Robin , C. E. Irvine," Analysis of the intelpentium's ability to supporta secure virtual machine monitor", In SSYM'00: Proceedings of the 9th conferenceon USENIX Security Symposium, pages 10–10, Berkeley, CA, USA, 2000.

[15] J. S. Reuben," A survey on virtual machine security", Seminar on NetworkSecurity Autumn 2007. Helsinki University of Technology, TelecommunicationsSoftware and Multimedia Laboratory, 2007..

[16] X. Jiang , D. X. Collapsar," a VM-based architecture for networkattack detention center", In SSYM'04: Proceedings of the 13th conference on USENIXSecurity Symposium, pages 2–2, Berkeley, CA, USA, 2004.

[17] K.Kourai, S. Chiba,"HyperSpector: virtual distributed monitoring environmentsfor secure intrusion detection", In VEE '05: Proceedings of the 1st ACM/USENIXinternational conference on Virtual execution environments, pages 197–207,New York, NY, USA, 2005.

[18] E. Siebert," A brief history of VMware", IT Knowledge Exchange, February2009. URLhttp://itknowledgeexchange.techtarget.com/virtualization-pro/a-brief-history-of-vmware-2/. RetrievedAugust 6, 2009.

[19] D. Duchamp , G. De Angelis," A hypervisor based security testbed", In DETER:Proceedings of the DETER Community Workshop on Cyber Security Experimentationand Test on DETER Community Workshop on Cyber Security Experimentation andTest 2007, pages 3–3, Berkeley, CA, USA, 2007.

[20] N.M.Donald," Security considerations and best practices for securing virtual machines",Gartner, Inc., March 2007.

[21] J.Kirch," Virtual Machine Security Guidelines Version 1.0",The Center for InternetSecurity, September 2007.

[22] VMware Security Advisory. VMSA-2009-0006, April 2009. URL http://www.vmware.com/security/advisories/VMSA-2009-0006.html, RetrievedAugust 06, 2009.

[23] S. T. King, P. M. Chen, Yi-M. Wang, C.Verbowski, H.J. Wang, J. R. Lorch,"Subvirt: Implementing malware with virtual machines", In SP '06:Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 314–327,Washington, DC, USA, 2006.

[24] H.Fritsch," Analysis and detection of virtualization-based rootkits", Master's thesis,TechnischeUniversitatMunchen, 2008.

[25] M. Carbone, D. Zamboni, and W. Lee," Taming virtualization", IEEESecurity and Privacy, 6(1):65–67, 2008.

[26] T.Garfinkel, M.Rosenblum," When virtual is harder than real: securitychallenges in virtual machine based computing environments", In HOTOS'05: Proceedingsof the 10th conference on Hot Topics in Operating Systems, pages 20–20,Berkeley, CA, USA, 2005.

[27] R. Naraine. "Vm rootkits: The next big threat.eWeek", March 2006

[28] J. Kirch," Virtual machine security guidelines",The center for Internet Security, http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf,2007.

[29] B. Huston,"Secuirty tip: 3 steps towardssecuring virtual machines.Security",http://security.itworld.com/4367/nlssecurity071009/page_1.html, 2007.