SURVEY ON MITIGATION TECHNIQUES OF VIRTUALIZATION TECHNIQUE

Venkata Subramanian N, Saravanan N and Shankar Sriram V S
School of Computing, Shanmugha Arts, Science, Technology and Research Academy University, Tamil Nadu, India
E-Mail: tyrvenkat@mca.sastra.edu

ABSTRACT

Cloud computing is an evolving model to deliver the resources in a convenient way from a pool of resources. With minimal interaction of provider, the resources are assigned to the user as an on-demand basis. For all kinds of web-based services, cloud computing provides a platform. Virtualization plays a major role in the cloud computing environment. Virtualization offers many benefits than real physical machine implementation. Even though plenty of benefits offered by virtualization, it brings several security vulnerabilities. This paper presents the mitigation techniques of various virtualization techniques.

Keywords: virtual machine security, isolation attacks, vm vulnerabilities, vm mitigation techniques.

1. INTRODUCTION

Cloud computing model is used for delivering the resource in a convenient way and on-demand basis from a pool of configurable resources that is being provisioned and released with minimal interaction of service provider [1]. The Virtualization is a software model that separate the operating system from the hardware physically used. These isolated machines are named as Virtual Machines (VM) [2]. Software version of the machine called as VM, which performs all activities similar to physical machine

The virtual machine can be generally classified into two category based on the usage, they are a) system virtual machine b) process virtual machine. Virtual machine performs all activities like traditional OS. More number of virtual machines would be executed on single physical hardware along with various guest operating systems. These operating systems create an illusion on end users that they are working with real physical infrastructure.

Hypervisor is software that provides a chance to run more number of operating systems in a single physical hardware. Virtualization helps the providers to share the resource from common pool. The virtual machines are properly isolated, this leads to a benefit of vulnerability on one VM will not affect the other VM's in the same machine. In Figure-1 the impression of virtual machine environment is given.

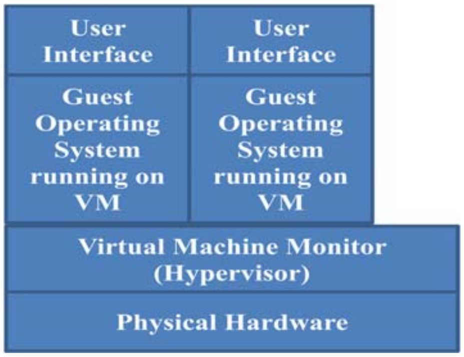
User Interface
User Interface
Guest Operating System running on VM
Guest Operating System running on VM
Virtual Machine Monitor (Hypervisor)
Physical Hardware

Figure-1. Overview of virtual machine environment.

There are several reasons to specify the need for virtualization. The reasons are multiple operating systems and virtual hardware, server consolidation, sandboxing. The physical machine security issues will also be germane for virtualized environment. The virtualization vulnerabilities are hyper-jacking, incorrect VM isolation, VM escapes, unsafe virtual machine migration, VM sprawl, DOS, guest OS vulnerabilities, live VM migration. In this paper we have given mitigation techniques for those security breaches of virtualization techniques. Based on the datacenter, this technology is classified into seven types [3]. They are Application Vitualization (AppV), Presentation Virtualization (PresentV), Desktop irtualization (DeskV), Management Virtualization (ManageV), Network Virtualization (NetV), Storage Virtualization (StoreV).

2. MITIGATION TECHNIQUES

2.1 Hyper-jacking mitigation techniques

The primary technique to secure the hypervisors is to keep it should be kept separate from usual traffic. The access to guest operating system should be delimited by restricting the access to the hypervisors with the intention of avoiding hyper-jacking attacks. Regular patching of the hypervisor is treated as another mitigation technique to overcome hyper-jacking attack. Integrity of virtual machine monitor or the hypervisors can be secured by means of few techniques (Figure. 2) likeHyperSafe [4], CloudVisor [5], HyperSentry [6] [7]. Few other techniques are there to minimize the hyper-jacking attacks such as Secure MMU [8] [9] and H-SVM [9], NoHype [5], HyperWall [6]. In the above stated techniques three techniques will downsize the functionalities of virtual machine monitor can be realized. Few more advanced techniques are there to secure the hypervisors such as NOVA [10], sHype, TrustVisor, SecVisor. Here explanations for few techniques can be explored. With the help of HyperSafe, the security strengthening can be done for VMM and the integrity can also be verified. Based on

"Control Flow Integrity" [11] two techniques are employed in this method.

"Non-by passable memory lockdown" will be treated as first technique, which endues a VMM with self protection. It protects the memory pages and their attributes from malicious modification. "Restricted pointer indexing" is considered as the second technique, which supplements the first one. Along with memory pages, the control data is encompassed to its protection umbrella, which is the primary usage of this technique. Without claiming specialized add-ons to basic hardware the implementation of HyperSafe can be done. In a level below the VMM, software layer is represented by CloudVisor, which intervene the VMM and the VM. The nested virtualization architecture takes care of the segregation of VMM and the VMs for the sake of securing the guest's resources and protect against the infected VMMs. Since Trusted Computing Base is diminished, rest of the VM and any manager VMs are not included, and CloudVisor has highest privileges as compared to VMM. For running hypervisors a novel security framework called HyperSentry [12] (Figure-3) has been developed. From the hypervisor a software component is separated and that has been setup by the HyperSentry to provide stealthy and in-context measurement for precisely measuring integrity.

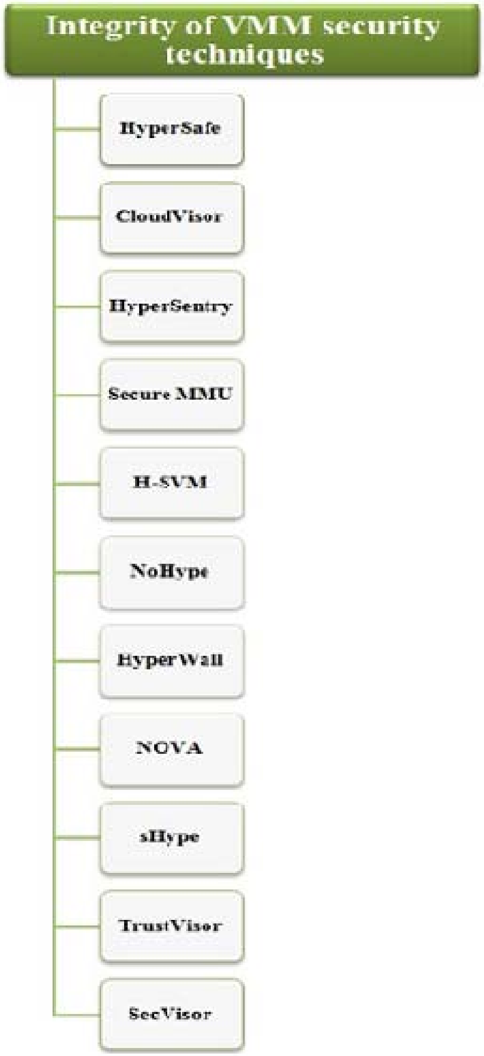

Figure-2. Integrity of VMM security techniques.

To trigger stealthy measurement this HyperSentry adopts out-of-band channel. To secure its vital data and base code it adopts System Management Mode. In order to overcome SMM's limitation, a set of novel techniques is being adopted by HyperSentry, which provides an integrity measurement agent with identical relevant information which is made available to the hypervisor, overall secured execution and evidence to the obtained output. Based on the experimental analysis this solution is considered to be having minimal overhead as compared to the existing solutions in practice. The overall architecture of HyperSentry is depicted in the following diagram and the trusted components are shown in gray [12]. In order to minimize the security breaches due to the abundant functionalities of virtual machine monitor, the following techniques are introduced with minimal functionality for the virtual machine monitors.

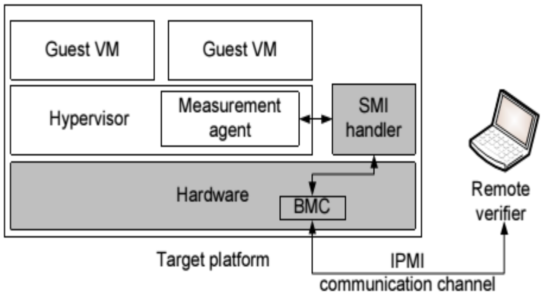

Figure-3. Architecture of hyper sentry.

The restriction of the functions and the role of VMM are promoted by the scheme called Hardware assisted virtual machine (H-SVM). Memory isolation is the ultimate motto, since the other party cannot access the physical pages that are assigned earlier. Information deletion from any existing pages that are assigned, swapping of pages and a degree of page sharing restriction are considered to be additional functions. It shows similar means of functionality over CloudVisor [13].

The second downsizing technique of VMM is NoHype that deals with the elimination of the attack surface by the hackers. In this method, the VM exist as a potential source, which negatively impacts security that results in injection of code and further versioning of VMM. The physical location, which is used to mount the hardware, is well secure from attacks, but the possible threats reside in guest operating systems. At the booting time, a temporary VMM is used to handle system configuration data, which declines customer code from execution.

Another architecture, which is used to endorse security in virtual environment, is HyperWall. The combination of HyperWall with any other model results in more secured architecture. HyperWall promotes the use of “Confidentiality and integrity protection” tables. It protects the VM’s memory based on user preferences. This is accomplished by VMM or DMA with hardware assistance is ascertained as a vital component in a secured architecture. The commodity VMMs is utilized with minor hardware alterations. Hyperwall exhibits multi-facilitated functions as compared to others.

2.2 VM escape mitigation techniques

The operating system that are installed and running on the virtual machines should run the regular software patch. The host should run only the required resource-sharing functionalities or services. In the guest operating system should install the genuine and lesser number of applications, so that those applications will not cause any kind of penetration attacks.

2.3 Unsafe VM migration mitigation techniques

To overcome the unsafe VM migration attack only restricted services and protocols alone to be permitted, to and from virtual machines. Proper guard should be enforced between virtual machines when the data exchanges are happening. Separate virtual NIC should be provided for management and production on each virtual machine with separate VLANs.

2.4 VM Sprawl mitigation techniques

Virtual infrastructures should be provided access based on the role. To create new virtual machines there should be some strict procedures to be made. Periodic verification should be done on the already created virtual machines. The identified idle virtual machines are to be destroyed properly or should be properly turned off.

2.5 Guest OS vulnerabilities mitigation techniques

Operating system running on the virtual machine should perform the patching process periodically. Have to adopt firewall applications and traffic isolation applications. On-demand or really needed applications should be installed on the operating system that is running on the virtual machine to overcome malicious attacks from unknowing applications running on the virtual machines.

2.6 Denial of service mitigation techniques

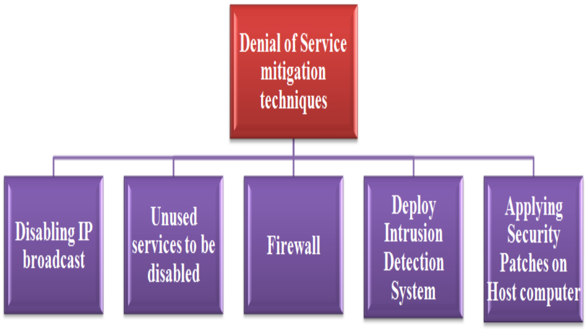
Denial of Service mitigation techniques
Disabling IP broadcast
Unused services to be disabled
Firewall
Deploy Intrusion Detection System
Applying Security Patches on Host computer

Figure-4. DoS mitigation techniques.

2.6.1 Disabling IP broadcast

IP broadcasting should be disabled to prevent the host computers to acts as amplifiers in Smurf and Fraggle attacks. All the nearing networks should disable broadcasting so that this attack can be tackled.

2.6.2 Unused services to be disabled

UDP echo or some other services are not required then those services should be disabled to defend from the attacks through unused services and unused ports.

2.6.3 Firewall

Effective filters to be installed to monitor all transactions and filtering all the packets from private address that are getting in and coming out from the networks so that the network can be prevented neighboring networks that may perform attacks and from remote attacks.

2.6.4 Deploy intrusion detection system

Deploying intrusion detection on the host computer to monitor all kind of net-flow and other activities so that host computer can be guarded from all kind of intrusion attacks on the another network.

2.6.5 Applying security patches on host computer

Host computer should be updated with recent security patches so that the host computer can be protected against the denial of service attack.

2.7 Live VM migration mitigation techniques

In order to secure the virtual machine before and after the migration process the following techniques are used i) Source virtual machine monitor level virtual firewall, ii) destination virtual machine monitor level virtual firewall.

The virtual machine can also be attacked during the migration process due to lack of proper mechanism to secure at the time of migration process. Virtual machine virtual firewall plays a vital role in granting security during the migration process. Firewall rules should be kept intact during the migration in order to restrict an attacker to invoke migration, introducing malicious code in to the virtual machine to exploit the data or to crash the virtual machine itself [14].

The Total Migration Time (TMT) and virtual machine Down Time (DT) are the effective measures for evaluating the intactness of the virtual machine virtual firewall. During virtual machine mobility, the Up Time of virtual machine level virtual firewall is calculated by the differences between the TMT and DT. The period between the migration initiation and migration completion is termed as Total Migration Time, which ranges from 21sec to 250sec [15]. The unresponsive time of virtual machine at the time of migration is referred as Down Time which varies between 0.3 secs to 14 secs [15]. At the migration time when the virtual machine is not down could be used by the attacker to exploit virtual machine, this is situation where the virtual firewall safeguards the virtual machine. This duration is often referred to as virtual firewall Up Time (UT). By sending the ICMP packets without break to the migrating virtual machine, the UT for the virtual firewall is obtained. The ping commands are used for calculating the TMT and DT [15].

To secure the live Virtual Machine migration, Internet Protocol Security tunnel [16] can be used (Figure-5). But the disadvantage of using this approach is that the downtime of Virtual Machine will be getting increased, the reason is that the processing power that requires for migration will be very much higher comparing to the normal operation. This will cause the break in service, but data will be secured due to the face that, through the IPSec if the transmission is happening then the data will be encrypted. IPSec tunnel can also be used in securing the data flow from one server to another server or from one edge router to another edge router. The below diagram depicts how actually the live virtual machine migration happening though the IPSec tunnel.

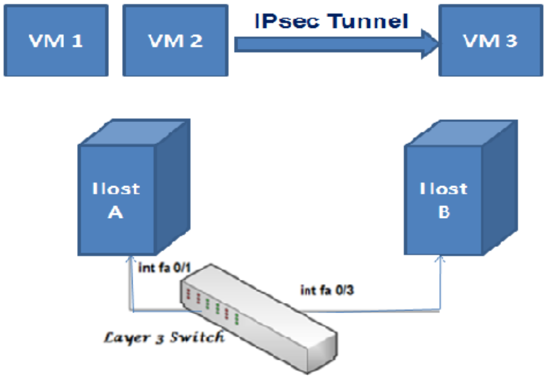

Figure-5. Live vm migration using IPSec tunnel.

Another approach to secure the live virtual machine migration is that performing the encryption of data by the hypervisor. If the hypervisor itself encrypts the data using strong encryption keys then the chance of hacking will be minimized much. The remote host's hypervisor should perform the decryption process using proper key to determine the integrity and confidentiality. If the hypervisor has done the encryption and decryption then the downtime, migration time, overhead of virtual machine will be less.

2.8 Analyze virtual machine

Virtual Machine Introspection is the activity done by hypervisor in order to analyze the virtual machine allocated memory content from outside. LibVMI is a framework to do this kind of Virtual Machine Introspection activity. Virtual Hub or Virtual Switch will be utilized to bring down the network traffic and to minimize the cost involved in provisioning the dedicated physical path to each guest machines. Sniffing attacks or ARP Poisoning may also happen if the dedicated physical path has been provisioned. The solution to this kind of problem is that authenticating all the network traffic.

To overcome the Denial of Service issue is that limit the resource allocations to the guest machines because if the attacker guest attacks then rest guest machine will not be in a position to get any resources. There are three broad classifications of virtual machine security solutions [17], they are Virtual Machine based, Server based, and Network based (Figure-6).

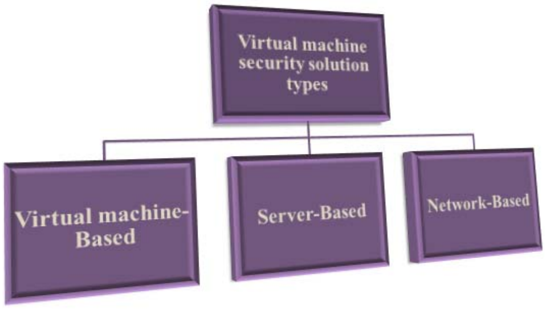

Figure-6. Virtual machine security solution types.

Virtual Machine-Based security solutions will have some security software installed in all the running virtual machines. In the scalability perspective it will protects one running virtual machine image at a time. Server-Based security solution will have virtual security appliance installed on the server. In the scalability perspective it will provides traffic protection for the specific virtualization server. Network-Based security solution will have off-line appliance deployed in network. One appliance will be enough to secure the whole virtualized environment. In the scalability perspective it will protects and enforces security policies on all virtual servers on the network.

3. CONCLUSIONS

In order to accomplish many numbers of activities like the physical machine, virtualization technology is used in cloud computing. The virtualization technology is not implemented properly then it leads to several security threats. Virtual machine is the resemblance of physical machine, so that the attacks possible in physical machine also applicable for virtual machine. Also the virtualization technology itself is having some security issues. This paper provides mitigation techniques for most of the frequent threats. Hyper visor will monitor every virtual machine that is running in the architecture, so that attacks are minimized. The virtualization technique is not entirely unsecure and few number of security breaches if that have not been implemented properly. The host operating and guest operating systems are to be secured. Still more unexplored susceptible areas are there in the technology and those to be explored.

REFERENCES

[1] Definition of Cloud computing, http://www.nist.gov/itl/cloud/.

[2] Danielle Ruest. 2009. Nelson Ruest Virtualization: A Beginner's Guide McGrawHill publication. p. 30.

[3] Danielle Ruest. 2009. Nelson Ruest Virtualization: A Beginner's Guide McGrawHill publication. p. 25.

[4] Z. Wang and X. Jiang. 2010. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow. in Proceedings of the 2010 IEEE Symposium on Security and Privacy SP. pp. 380-395.

[5] J. Szefer, E. Keller, R. B. Lee and J. Rexford. 2011. Eliminating the hypervisor attack surface for a more secure cloud. in Proceedings of the 18th ACM conference on Computer and communications security CCS. pp. 401-412.

[6] J. Szefer and R. B. Lee. 2012. Architectural Support for Hypervisor-Secure Virtualization. in Proceedings of the seventeenth international conference on Architectural Support for Programming Languages and Operating Systems ASPLOS. pp. 437-450.

[7] A. M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang and N. C. Skalsky. 2010. HyperSentry: enabling stealthy in-context measurement of hypervisor integrity. in Proceedings of the 17th ACM conference on Computer and communications security CCS. pp. 38-49.

[8] S. Jin and J. Huh. 2011. Secure MMU: Architectural support for memory isolation among virtual machines. in IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops. pp. 217-222.

[9] S. Jin, J. Ahn, S. Cha and J. Huh. 2011. Architectural support for secure virtualization under a vulnerable hypervisor. in Proceedings of the 44th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO-44 '11).

[10] Brosig, F, Gorsler, F. Huber, N. Kounev, S. Modeling. 2013. Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS). 2013 IEEE 21st International Symposium on. 404-408.

[11] M. Abadi, M. Budiu, Ú. Erlingsson and J. Ligatti. 2009. Control-flow integrity principles, implementations, and applications. ACM Transactions on Information and System Security (TISSEC). 13(1).

[12] Ahmed M. Azab, Peng Ning, Zhi Wang, Xuxian Jiang. 2010. HyperSentry: Enabling Stealthy In-context Measurement of Hypervisor Integrity. ACM 978-1-4503-0244-9/10/10, CCS'10.

[13] F. Zhang, J. Chen, H. Chen and B. Zang. 2011. CloudVisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. in Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles SOSP. pp. 203-216.

[14] J. Shetty, A. M R, and S. G. 2012. A Survey on Techniques of Secure Live Migration of Virtual Machine. International Journal of Computer Applications. 39(12): 34-39.

[15] F. Salfner, P. Tr and A. Polze. 2011. Downtime Analysis of Virtual Machine Live Migration. The Fourth INternational Conference on Dependability (DEPEND 2011). pp. 100-105.

[16] John R. Vacca. 2013. Computer and Information Security Handbook (Second Edition) Chapter 6 - Securing Cloud Computing Systems.

[17] Vimal Vaidya RedCannon Security, Inc. Virtualization Vulnerabilities and Threats: A Solution White Paper, 2009.