AN ASSESSMENT OF VIRTUAL MACHINE ASSAILS

V Venkata Ramana[1], Y. Subba Reddy[2], G. Rama Subba Reddy[3], Dr. Pandurangan Ravi[4]

[1, 2, 3] *Associate Professors, Department of CSE, CBIT, Proddatur, Y.S.R, A.P, (India)*

[4] *Principal, CBIT, Proddatur, Y.S.R, A.P, (India)*

ABSTRACT

Virtual machine plays a typical role in assisting the organizations to decrease the processing cost, pick up the effectiveness, enhanced operation and litheness of accessible hardware. This paper presented an empirical study on security issues in virtualization technologies. Our study focus on various security threads which are common to all virtual machine technologies. The security assails by the intruders have compromised virtual machine infrastructures permit them to way in other virtual machines on the same system and even at the host. Providentially these security apprehensions are being monitored and users can prevent the majority intrusions by taking conventional measures.

***Keywords: Virtual Machine, Hypervisor, Security, Assails*.**

I. INTRODUCTION

Virtual machines are speedily replacing physical machine infrastructure for their abilities to copy hardware environments, share hardware assets and utilize a variety of operating systems. A VM is a software-layer abstraction of hardware that allows a procedure to perform in a followed environment. The hypervisor, also called the virtual machine monitor, runs on the host OS and allocates followed possessions to each guest OS. When the guest makes a system call the hypervisor interrupts and interprets it into the matching system call carried by the host OS. The hypervisor controls each VM's entree to the CPU, memory, continual storage, I/O devices, and the network. The side possessions of virtualization allow VMs to provide security features physical machines do not: isolation, state recording, transience, and mobility. Isolation is the process of encapsulation of each guest OS and idea from the hardware, so that each user accesses file systems and memory blocks separately. In general a VM compromised by intruders will not affect the user host or other VMs on the host. Because each VM is working under the supervision of the hypervisor, the host OS can easily identify and record the changes which have been made to the system configuration and files. This allows users to unwrap system-wide changes to the guest OS [1]. Unfortunately, VMs are a quite new technology with security issues and vulnerabilities. There are three effects of an attack that are adverse to users: 1) the guest OS is compromised, 2) multiple guests OS are compromised, or 3) the host OS is compromised. In addition to these local attacks, there are three other types of attacks on VMs. The attacker may make use of a compromised VM to correspond with other VMs on the same physical host, a desecration of the isolation property of VMs. The second type of attacks are on the hypervisor, which can likely give the attacker access to the host OS and built in hardware [2]. Finally, the third type of attacks is denial of service (DoS), these attacks can be predominantly successful on VMs because they have the capability to guzzle resources from all VMs on the host. Virtual machines are advanced

server infrastructure. They permit emulation of many isolated operating systems, decreasing hardware costs, while providing features such as state restore, transience, and mobility [3]. The three mechanisms of a typical VM setup are: the host OS which communicates with the hardware, the hypervisor which distributes resources and manages the VM, and a guest OS run without contact to the host OS or hardware. VMs are subject to exceptional attacks in addition to attacks that physical machines face, but can be prevented using similar security schemes as applied to normal systems.

II. RESEARCH METHODOLOGY

This paper is a literature survey that classifies various issues regarding security in virtual machine background. Work provides an abstract view of security threats arises in a virtualized environment.

III. CLASSIFICATION OF HYPERVISOR

The hypervisor classification done by its architecture is revealed by the relationship between VMM, guest OS and device drivers.

3.1 Type 1 Hypervisor

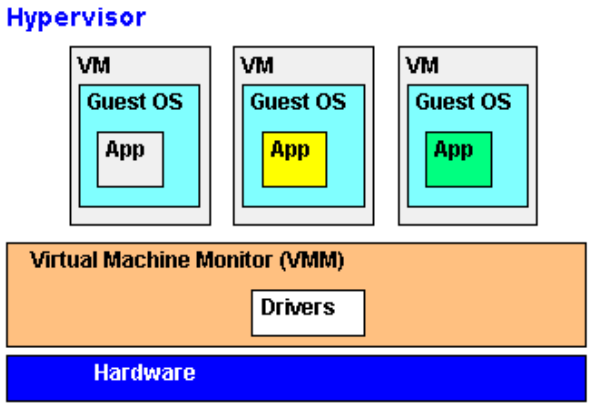
Type 1 hypervisor is software that operates on the host's hardware as a hardware control and guest OS, in which guest OS operates on the layer above the hypervisor as shown in figure 1. It can accomplish higher virtualization by dealing directly with the hardware.

3.2 Type 2 Hypervisor

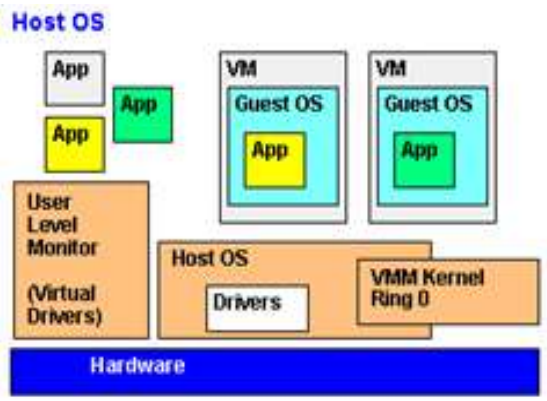
Type 2 hypervisor as shown in figure 1, is software application running within a conventional OS environment. The advantage of Type 2 Hypervisor is the support of a broad range of I/O devices from the Host OS. It is commonly used in client system.

3.3 Type 3 Hybrid Hypervisor

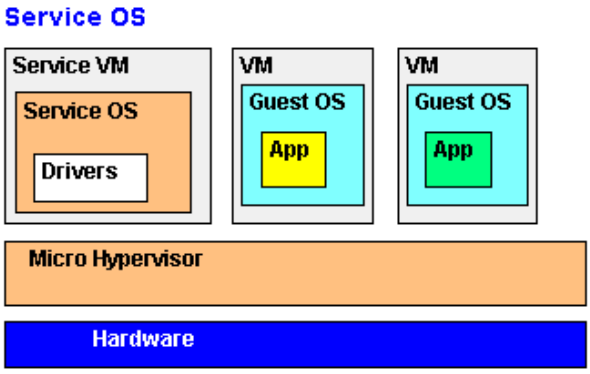
Hybrid Hypervisor combines the robustness of the type 1 model with the flexibility of the type 2 model. One example is Service VM, which is shown in figure 1.



Type 1 Hypervisor



Type 2 Hypervisor



Type 3 Hypervisor

Figure 1: Classification of Hypervisor

IV. SECURITY ASSAILS

The VM layer is secured than any OS, because of its simplicity and strict access management. Compromising the hypervisor offers the prospect of attacker's access to all or any virtual machines controlled by it and presumably the host, that makes the hypervisor a compelling target. The unauthorized communication between guests may be a violation of the isolation principle, however, will doubtless occur through shared memory.

Like physical machines, VMs are a unit liable to thieving and denial of service attacks [4]. The contents of the virtual disk for every virtual machine area unit typically hold on as a file, which might be travel by hypervisors on different machines, permitting attackers to repeat the virtual disk and gain unrestricted access to the digital contents of the virtual machine. Since VMs share resources from the physical machine, VM infrastructures have been notably liable for denial of service attacks [5] that may starve resources from all VMs on the physical machine. As luck would have it, this drawback is well fastened by limiting resource consumption per every VM. Newer merchandise solve several of those issues, but still be issues that hypervisors abundant continue to contemplate in development.

4.1 Communication between VMs or Between VMs and host

One of the first benefits that virtualization brings is isolation. This benefit, if not fastidiously deployed become a threat to the atmosphere. Isolation ought to be fastidiously configured and maintained in an exceedingly virtual atmosphere to make sure that the applications running in one VM don't have access to the applications running in another VM. Isolation ought to be powerfully maintained that housebreaking into one virtual machine shouldn't offer access either to virtual machines within the same atmosphere or to the underlying host machine.

Shared writing board in virtual machine could be a helpful feature that enables knowledge to be transferred between VMs and also the host. However, this convenient feature may also be treated as an entree for transferring knowledge between cooperating worm in VMs. In the worst case, it's accustomed "exfiltrate knowledge to/from the host package ".

In some VM technologies, the VM layer is in a position to log keystrokes and screen updates across the virtual terminals, as long as the host software kernel has given necessary permission. These captured logs area unit hold on come in the host that creates a chance to the host to watch even the logs of encrypted terminal connections within the VMs [6]. Some virtualization avoids isolation, so as to support applications designed for one software to be operated on another software, this answer fully exploits the protection bearers in each the operative systems. this sort of system, wherever there's no isolation between the host and also the VMs provides the

virtual machines a vast access to the host's resources, like file system and networking devices. During which case the host's file system becomes vulnerable.

4.2 VM Escape

Virtual machines area unit allowed to share the resources of the host machine however still will give isolation between VMs and between the VMs and also the host. That is, the virtual ma- chines area unit designed during an approach that a program running in one virtual machine cannot monitor, or communicate either with programs running in different VMs or with the programs running within the host. However really the organizations compromise isolation. They configure flexible isolation to satisfy their organization desires that exploits the safety of the systems. New package bugs were already introduced to compromise isolation [2]. One such example of this type of attack is VM escape. VM escape is one in every of the worst case happens if the isolation between the host and between the VMs is compromised. In VM escape, the program running during a virtual machine is ready to utterly bypass the virtual layer (hypervisor layer), and find access to the host machine. Since the host machine is that the root, the program that gain access to the host machine conjointly gains the foundation privileges primarily escapes from the virtual machine privileges [8]. This lead to complete breakdown within the security framework of the surroundings [7]. This drawback is solved by properly configuring the host/guest interaction.

4.3 VM monitoring from the host

Host machine within the virtual atmosphere is taken into account to be the management purpose and there are a unit implications that modify the host to monitors and communicate with the VM applications up running. Thus it's additional necessary to strictly shield the host machines than protective distinctive VMs. totally different virtualization technologies have different implications for the host machine to influence the VMs up running within the system. Following area unit the attainable ways that for the host to influence the VMs [7],

- The host will begin, shutdown, pause and restart the VMs.
- The host will able to monitor and modify the resources offered for the virtual machines.
- The host if given enough rights will monitor the applications running within the VMs.
- The host will read, copy, and certain to switch the info keep within the virtual disks appointed to the VMs.

And notably, generally all the network traffic to/from the VMs tolerate the host, this allows the host to observe all the network traffic for all its VMs. within which case if a bunch is compromised then the safety of the VMs is under question. essentially altogether virtualization technologies, the host machines area unit given some kind of basic rights to manage some actions like resource allocations of the VMs running on prime. However care ought to be taken once configuring the VM atmosphere in order that enough isolation ought to be pro- vided that avoids the host being an entree for assaultive the virtual machine [7].

4.4 VM Monitoring From another VM

It is thought-about as a threat once one VM with none difficult is also allowed to observe resources of another VM. Because of today's trendy CPUs, that comes with an in-built memory protection feature. The hypervisor who is chargeable for memory isolation will build use of this feature; this memory protection feature prevents one VM seeing the opposite VM's memory re- sources. And additional over the VMs doesn't have the likelihood to directly access the file system of the host machine, thus it's not possible for a VM to access the virtual disk allotted to a different VM on the host. Once involves the network traffic, isolation utterly depends

on the affiliation (network) setup of the virtualized atmosphere. If the host machine is connected to the guest machine by suggests that of physical dedicated channel, then it's unlikely that the guest machine will sniff packets to the host and the other way around. But really the VMs area unit joined to the host machine by suggests that "virtual hub" or by a virtual switch [9].

4.5 Denial of Service

In virtual machine design the guest machines and therefore the underlying host share the physical resources like mainframe, memory disk, and network resource. Therefore it's attainable for a guest to impose a denial of service attack to alternative guests residing within the same system. Denial of service attack in virtual atmosphere is de- scribed as associate in attack once a guest machine takes all the attainable resources of the system. Hence, the system denies the service to alternative guests that area unit creating request for resources, this is often as a result of there's no resource accessible for alternative guests. The simplest approach to forestall a guest intense all the re- sources is to limit the resources allotted to the guests. Current virtualization technologies supply a mechanism to limit the resources allotted to every guest machines within the atmosphere [10]. So the underlying virtualization technology ought to be properly configured, which might then forestall one guest intense all the accessible resources, there by pre- emission the denial of service attack.

4.6 Guest-to-Guest attack

As mentioned in Sec. 4.3 it is important to prevent the host machine than the individual VMs. If an attacker gains the administrator privileges of the hardware then it's likely that the attacker can break-in into the virtual machines. It is termed as guest-to-guest attack because the attacker can able to hop from one virtual machine to another virtual machine provided that the underlying security framework is already broken [4].

4.7 External Modification of a VM

There are some sensitive applications exists which rely on the infrastructure of the VM environment. These applications running inside a virtual machine requires the virtual machine to be a trusted environment to execute that applications if a VM is modified for some reason, the applications can still be able to run on the VM but the trust is broken. Sudhakar and Andrew [3] in their paper emphasis more at- tacks on application virtualization. A best solution for this problem is to digitally sign the VM and validating the signature prior to the execution of this sensitive application [7].

4.8 External Modification of the Hypervisor

As mentioned earlier in Sec. 4.4 hypervisor is responsible for providing isolation between the guest machines. The VMs are said to be completely isolated or "self-protected" [7, 2] only if the underlying hypervisor behaves well. A badly behaved hypervisor will break the security model of the system.

V. CONCLUSION

The paper has bestowed a number of the safety flaws within the virtual machine atmosphere. A number of the threats bestowed here could also be thought of as benefits in some things, however, they're bestowed here in order that the correct care ought to be taken whereas planning and implementing the virtual atmosphere. Virtualization brings little additional security to the ambiance [11]. Ace with all the central issues is that everybody ought to digest in mind of the very fact that virtual machines represent the logical instance of Associate in underlying system. Numerous of the standard PC threats apply a similar to the virtual machines

additionally. Another issue that produces the safety consequences difficult to grasp is that, there is a unit numerous differing types of virtualization technologies on the market within the market. Every of its own deserves and demerits, every virtualization preparation is completely different looking on the necessity for the virtualization. It's common that any single virtualization technology won't offer protect to any or all the safety problems arise [12]. However, the key to form a decent virtualization atmosphere is to check fastidiously the atmosphere that's to be fertilized, the requirements and goals of the organization, and taking into thought all the doable security problems that puts the virtual machines in danger? Finally fastidiously style the virtual atmosphere with the assistance of corrective virtualization technology that matches the goals. The majority of the safety problems bestowed here issues the safety of the host and therefore the hypervisor. If the host or the hypervisor is compromised, then the total security model is broken. Attacks against the hypervisor changing into a lot of commonality among the attackers realm [11]. Thus, once fitting the atmosphere, care ought to be taken to confirm that the hypervisor is secure enough to the fresh rising threats, if not patches should be done. Patches ought to be done often in order that the dangers of hypervisor being compromised are avoided [5]. Virtualization may be a powerful resolution to scale back the operational prices in today's computing, however if done wrong, it be- return as a threat to the atmosphere. Whereas implementing, exaggerate the safety model to withstand the attacks. And as mentioned earlier keeping observance for brand spanking new developments that emerges during this field and still stay awake to this point.

REFERENCES

[1] P. Ferrie. Attacks on virtual Machine Emulators. SYMANTEC ADVANCED THREAT RESEARCH. http://www.symantec.com/avcenter/ reference/Virtual_Machine_Threats. pdf.

[2] T. Garfinkel and M. Rosenblum. When Virtual is Harder than Real: Security Challenges in Virtual Machine Bases computing Environments. Stanford University Department of Computer Science. http: //www.stanford.edu/~talg/papers/ HOTOS05/virtual-harder-hotos05.pdf%.

[3] S. Govindavajhala and A. W. Appel. Using Memory Errors to Attack a Virtual Machine. Princeton Univer- sity. http://www.cs.princeton.edu/sip/ pub/memerr.pdf.

[4] K. J. Higgins. Vm's create potential risks. Tech- nical report, darkREADING, 2007.http://www.darkreading.com/document.asp? doc_id=117908.

[5] B. Huston. Secuirty tip: 3 steps towards securing virtual machines. Security, Septem- ber 2007. http://security.itworld.com/ 4367/nlssecurity071009/page_1.html.

[6] M. Jones. Discover the Linux Kernel Virtual Machine. IBM. http://www-128.ibm. com/developerworks/linux/library/ l-linux-kvm/.

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

[8] A. Mann. The pros and cons of virtualization. BTQ, 2007. http://www.btquarterly.com/ ?mc=pros-cons-virtualization\&page= virt-view%research.

[9] D. Marshall. Whitepaper: Virtual machine security guidelines. InfoWorld, September 2007. http://weblog.infoworld.com/ virtualization/archives/2007/09/ whitepaper_%virt.html.

[10] E. Messmer. Security in the 'virtual ma- chine'? NETWORKWORLD, April 2006. http://www.networkworld.com/weblogs/ security/012014.html.

[11] R. Naraine. Vm rootkits: The next big threat. eWeek, March 2006. http://www.eweek.com/ article2/0,1759,1936666,00.asp.

[12] R.P.Goldberg. Architecture of virtual machines. In Proceedings of the workshop on virtual computer sys- tems, pages 74 – 112. THE ACM, 1973.