IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Overview on Information Security in Virtualized Environment

Dr. Rajendra H. Bele
Departmnet of Computer Science,
National Defence Acedemy, Khadakwasla, Pune-23

Abstract. Virtualization is simulation of hardware resources for multiple Applications executing on different virtual machines. Virtualization aims to efficiently utilize existing hardware and reduce the total cost of infrastructure , in addition to that virtualization also enhances availability and scalability of resources, It achieves these features with the help of light weight software called as hypervisor.

Hypervisor produces layer of abstraction between hardware resources and Applications running on VM, Though the aim of virtualization is same there are various types of virtualization exists based on its implementation As hypervisor decouples logical and physical state of system it creates opportunity for researcher to balance ratio of performance between native system and virtualized system in addition to it attracts researchers to focus upon security concerns raised in new virtual environment. This paper throws light on the security issues raised due to virtualized environment and recommends some solution to them.

Keywords:. Para virtualization, Full Virtualization, VM, SAN, NAS, Hypervisor Security

1 Introduction

Virtualization technology involves many components like hypervisor, domain0, domainU, host O.S., guest O.S. Applications, Storage etc. Security in Virtual environment is mainly depends on all these components individual security.

Virtual Machines becomes isolated systems to the user or developers hence traditional security threats needs to be defended using firewalls, antivirus software inside VM. It is also necessary to put into practice other suitable solution to notice and stop attacks in Virtual machines.

As discussed earlier Virtualization can be implemented with different options so the appropriate security model for each position is different to present issues raised in virtual environment, This paper has organized in four sections, section one is abstract, section two presents types of virtualization and its features, section three is about security measures with respective types of virtualization, Section four is conclusions and future work.

2 Types of virtualization technologies and its features

Virtualization is not a new concept it is similar to multiprogramming where resource utilization is improved and size and number of servers are reduced this job is ultimately completed with light weight software called as Virtual machine monitor or hypervisor. Hypervisor allows multiple operating systems and software applications exist on the same physical hardware. The hypervisor controls and manages underlying hardware to many OSs existing as guest systems, and gives each guest system the impression that it is running on its own private hardware [3].

2.1 Types of Virtualization

Many technical details of virtualization are similar, yet various approaches exist with respect to its implementations. There are five main types of virtualization exists based on their architectures like emulation, full virtualization, Para virtualization, operating system virtualization, library virtualization and application virtualization. Emulation simulates the entire hardware resources required to execute unmodified operating system guests for completely different hardware architecture. Examples are PowerPC, Bochs, and Quick Emulator (QEMU). [2]

2.1.1 Full Virtualization

In x86 architecture, virtualization is called as full virtualization if they can run unmodified guest operating system. Major vendors of full virtualization are VMware Workstation, VMware Server; KVM, Xen supports full virtualization with hardware support [2].

2.1.2 Para virtualization

In Para-virtualization, Guest OS needs to modify to make it aware that it is going to be virtualized the; As Compare to full virtualization there are many advantages in Par a virtualization in presentation, size, and administration. The two most common examples of Para virtualization are User-mode Linux (UML) and Open Source Xen.

2.1.3 Operating System Level Virtualization

In this type of virtualization each guest virtual machine runs the same operating system, with different instances. It shows poor isolation across guests. Implementations of operating system level virtualization include Virtuozzo, Linux VServers, OpenVZ, Solaris Containers and FreeBSD.

2.1.4 Library Virtualization

This emulates operating systems or subsystems via a special software library. An example of this type of virtualization is the Wine library available on Linux systems. Wine provides a subset of the Win32 API as a library to allow Windows desktop applications to be executed in a Linux environment.

2.1.5 Application Virtualization

In Application virtualization multiple applications are running inside a virtual execution environment where virtual environment provides a standard Application Programming Interface (API) to execute cross-platform applications .It also manages the application's consumption of local resources. Virtual Machine used in JAVA based applications is one of the examples of Application Virtualization [6].

3. Security Measures in Virtual Environment

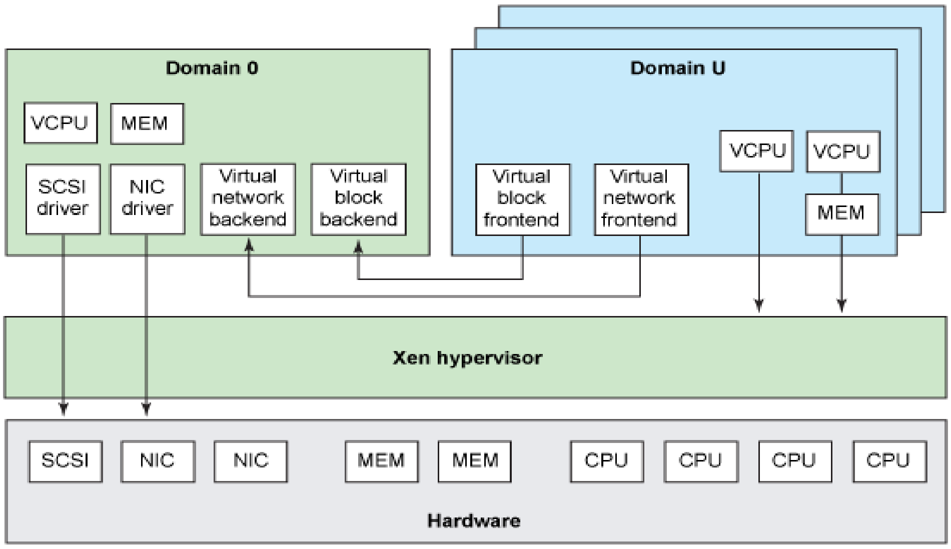

Fig. 1: Scenario of Virtualization [3]

In Server Virtualization there are two types of virtualization. Type I and Type II Virtualization. Type I virtualization is called as bare metal virtualization also called as native virtualization where hypervisor directly runs on the underlying hardware, without a host OS.

Type II form of virtualization, known as host based virtualization where hypervisor runs on top of the OS called as host operating system, this host Operating System can be any general operating system such as Windows, Linux, or MacOS etc.

3.1 Bare Metal Virtualization verses Hosted Virtualization and Security

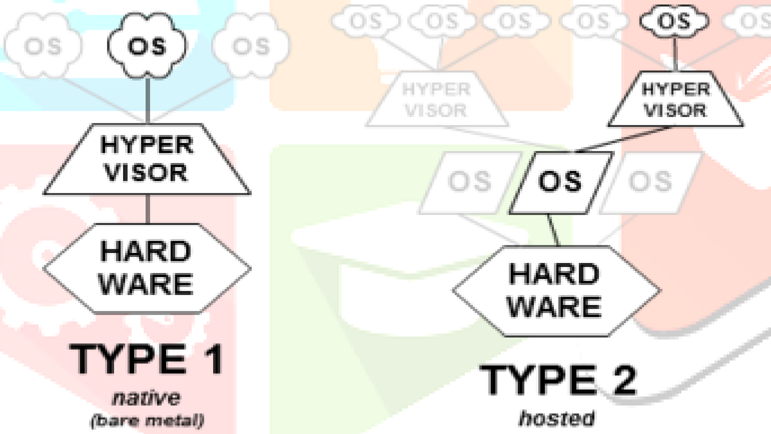

Fig.2. Basic Types of Virtualization [7]

Usually Servers are virtualized using bare metal virtualization (Type I) and Desktops are virtualized with host based virtualization (Type II). In both native and host based virtualization, each Virtual Machine having its own operating System called as guest OS, each guest have its own set of virtual hardware, like a native computer system. This hardware device includes Processor, Memory, Disk and Network devices like bridges and switches .In set of devices includes Storage controllers, Ethernet cards, Display and sound devices, Keyboard and mouse. Some Virtualization setups provides USB drives, parallel ports for printing, and serial ports as part of virtual hardware. [4]

Decision between bare metal and hosted virtualization plays crucial role while making security decision for overall system. Introduction of a VMM on top of an OS adds more complication and weaknesses to the domain0 because hypervisor is small light weight peace of software. It is not full-fledged operating System, so it becomes simple target for attackers. Selecting Type I (Bare Metal) virtualization instead of Type II (host based) will improve security if security in hypervisor not be compromised. Type I and Type II virtualization technologies having its own features with respect to performances .Individual organisation should optimise their security policies with respect to performance and then decide whether or not a host OS should be used under a hypervisor or above hypervisor in a server or desktop virtualization.

3.2 Security in Virtualized Network

Virtual Machines can communicate with each other through virtualized network environments. Virtualized network provides networking facilities to Guest O.S. existing in different virtual machines. In virtual environment on virtual Machine can communicate with other Virtual Machine through virtual network devices like witches, routers etc. These VM's also has limited admittance to the outside substantial network. The network interfaces that the virtual machines having are either virtual, physical, or both. [10]

Hypervisor creates a virtual private network for All VMs existing guest OSs. In virtual environment hypervisor may implement virtual network devices like switches, hubs, bridges etc. This hypervisor's networking environment speeds up for interactions among multiple guests on a only host. It boosts the speed of communication because data packet will transmit through virtual networking devices and it will not strike hardware devices used in networking because internal networking can be implemented with several ways by hypervisor. Sometimes it is Virtual switch network or it could be virtual LAN (VLAN).

Many networks depend on tools that watch traffic as it flows across routers and switches. Some hypervisors provide APIs that allow a privileged VM to have full control to the network traffic. Network traffic monitoring tools may be available at hypervisor level or at privileged domain that is Host OS which can create additional loop holes for security attackers due to network monitoring system. Network monitoring tools existing at hypervisor can impact on system performance due to heavy network traffic faces by hypervisor as hypervisor is light weight software. [9]

Hence the security concerns related to networks internal to a Virtual Machine Monitor must not be compromised while designing hypervisors, developer should consider security measures in it. In addition to performance security must be focused in Hypervisor (VMM) design and implementation. Multiple Virtual Machines created in virtualized environment plays different roles like database server, web server, file server etc. Organizations also monitor the switch that connects the virtual machines, watching for traffic that would indicate attack on virtual servers.

3.3 Virtualized Storage

Main foundation for cloud computing is virtualization any cloud solution is combination or collection of various virtualization technologies, web technologies and Network technologies and much more. In Storage virtualization, there are many ways to deal with storage in virtual environment.

- It can simulate disk storage to different guest OS.
- All most all hypervisors have virtual hard drives
- Storage Area Network and Network Attached Storage

If large volume of data produced and maintained in the industry, Virtualized system can utilize advanced storage technologies, such as network-attached storage (NAS) and storage area networks (SAN), to store a data compiled and processed by guest OSs. [11]

Virtualized system has access to NAS and SAN, either through their network or through virtual devices available in Virtual environment. Hypervisors can make available SAN and NAs with help of additional management software's in it; there are certain technologies available in the market which can provide complete abstraction for SAN and NAS for data centers where those systems appear as virtual drives. Virtualization is leading at each level from desktop to device virtualization and Software Defined Network hence new Hybrid type of virtualization solutions are being added into hypervisors technology regularly. [11]

Security in storage virtualization is similar to the security in traditional storage systems. While partitioning storage area for various virtual servers, complete isolation needs to implemented .While migrating Application from one Virtual machine to other Virtual Machine its disk image and memory image should be protected and secularly managed. Though the various types of storage are shared among different Virtual machines it should be managed in such a way that they are always under control of security protocols defined by the system. Redundant Copies of data backups which are part of protection in a security strategy in virtualized system is similar to native systems, hence organization should set up backup of virtualized storage into their regular backup strategy. Contact to the virtual storage can be controlled at the privileged domain and UN Privileged domains (Guest OS). One can understand that hacker could access information if they gain physical access to the system while it is running and the files in use are in decrypted form. So it is very important to have controlled access to physical access to the system appropriately. File system encryption will keep away unauthorized person from booting up system. Complete implementation of Confidentiality, Authenticity and Authorization mechanisms are implemented to control user access to files and other assets according to the group policy. [9]

4. Conclusions

Virtualization is root to reduce size of infrastructure of data centres in the organisation, not only this it also comes along with many other befits like live migration, disaster recovery, high availability, clustering etc. Virtualization facilitated these benefits to its users so that it becomes a large and very exciting field of research, with new research and threats coming out daily, hence many solutions are exists in the market and continuous efforts are made to enhance performance which creates opportunities to take review on security in virtualization.

In Virtual environment security in normal system must be implemented first in addition to that security with threats affecting to the Hypervisor, VMs, OSs in VMs, Applications running on different virtual Machines , and the Administrative tasks such as network management , storage management etcetera need to be implemented .

Security in the context of virtualization refers to security in hypervisor, security to virtualized network system and security to virtualized storage etc. Security to access various components and data in virtualized environment is essential in the area of virtualization. Sensitive data must be protected by implementing confidentiality, integrity, and authorisation policies for software data ,program data in memory, on disk, or in other forms of storage, As well as data in software and hardware operational state like resource allocation levels, program execution etc. While implementing security solutions in virtual environment organisation has to plan the security policy with respect to the design of infrastructure for example changes to Type One VMMs may not (necessarily) be applicable to Type Two VMMs.

As many components are involved in virtualization it is essential to analyse the existing software and hardware infrastructure as well size and workload of applications to be executed in virtual environment and define appropriate security policy and should be implemented to maintain persistent security in the virtualization.

References

1. Umar Farooq Minhas, Jitendra Yadav, Ashraf Aboulnaga, kenneth Salem University of Waterloo, “Database Systems on Virtual Machines: How Much do You Lose”, 2007
2. Prabhakar Chaganti ,”Xen Virtualization practical guide to supporting multiple operating system”
3. http://www.ibm.com/developerworks/library/l-multipath-xen/index.html.
4. Jeanna N. Mathews; Eli M.Dow; Todd Deshane; Wenjin Hu;Running Zen: A Hands on Guide to the Art of Virtualization April, 2008.
5. Ashraf Aboulnaga University of Waterloo prepared jointly with Cristiana Amza Kenneth Salem University of Toronto University of Waterloo” Virtualization and Databases: State of the Art and Research Challenges”, 2006.
6. Tutorial by Jeanna Mathews and Zach Shepherd Clarkson University on “Introduction to the open Source Xen”
7. http://en.wikipedia.org/wiki/Hypervisor.
8. Pearce, M., Zeadally, S., and Hunt, R. 2013. Virtualization: Issues, security threats, and solutions. ACM Comput. Surv. 45, 2, Article 17 (February 2013), 39 pages.
9. Guide to security for full virtualization Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 ,January 2011
10. Kirk L. Kroeker “The Evolution of Virtualization” ACM Technical News Centre.2010
11. September/October 2007 ACM QUEUE