ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

The Review of Virtualization in an Isolated Computer Environment

Sunanda

Assistant professor, Department of Computer Science & Engineering, Ludhiana College of Engineering & Technology, Ludhiana, Punjab, India

Abstract: The concept of virtualization is expanding into various aspects especially in the field of IT. The networking is relying on the road map of virtualization. The movement of virtualization is originating in servers. The most profound impact on data-centre networks is based on virtualization of the servers. Virtualized servers will support the full array of business applications, multimedia applications, storage, and back-office services. This paper will discuss the role of virtualized architecture explaining the relevant security interior concepts to moderate the risks.

Keywords: Virtualization, VM (virtual Machines), Approaches, Security, Operating System (OS).

I. INTRODUCTION

Virtualization means to create a virtual version of a machine, for instance a network, server, storage device or even an operating system. It is a technique that divides a physical computer into several partly or completely isolated machines commonly known as guest machines or virtual machines (VM). An assortment of virtual machines can run on a host computer, apiece possessing its own applications and OS. This presents an illusion to the processes on these virtual machines as if they are running on a corporal computer, they are sharing the physical hardware of the host machine in reality. The software that allows multiple operating systems to use the hardware of the physical machine is called a control program or a hypervisor. Hypervisors sit between the operating system of the host machine and the virtual environment.

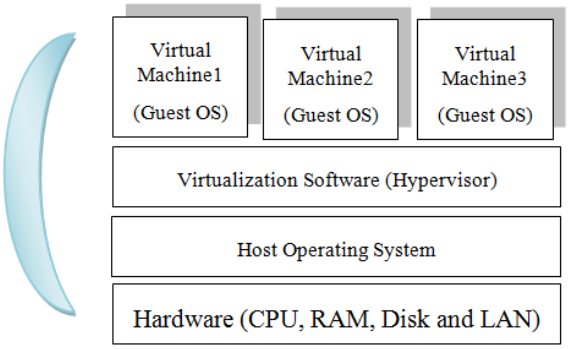


Fig 1: Virtualization

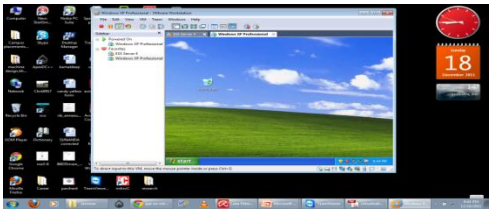


Fig 2: Snapshot of VM

II. BACKGROUND

In 1960's, IBM Corporation was developed Virtualization firstly, formerly to partition large mainframe computer into several logical instances and to run on single substantial mainframe as the host. This feature was invented because maintaining the larger mainframe computers turn dotty about cumbersome. The scientist realized that this capability of partitioning allows multiple processes and applications to run at the one and the parallel time, thus increasing the efficiency of the environment and decreasing the expenses. By day to day development, virtualization technologies have rapidly attains popularity in computing; in fact it is now proven to be a fundamental building block for these days' computing. Two primary benefits offered by any virtualization technology are:

- Resource sharing
- Isolation

➢ Resource sharing - Unlike in non-virtualized environment where all the resources are dedicated to the running programs, in virtualized environment the VMs shares the physical assets as memory, disk and network devices of the core host. The resources allocated on appeal of the VM. Hypervisors plays a significant role in resource allocation.

➢ Isolation - One of the key issues in virtualization provides isolation between virtual machines that are running on the same substantial hardware. Programs running in one virtual machine cannot see programs running in an additional VM.

This is contrast to non-virtual environment where the running programs can see each other and if allowed can communicate with each other.

Virtualization provides a facility of restoring a clean non infected environment even the underlying system is infected by vicious programs.

Since, Virtualization provides an isolated environment this can be used for debugging malicious programs and also to test new applications (Reuben, J. S. (2007).

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

III. VIRUALIZATION COMPONENTS

A. Virtual Machine (VM) It refers to a software computer that, like a PC, runs an operating system and applications. An operating system on a VM is called a guest operating system.

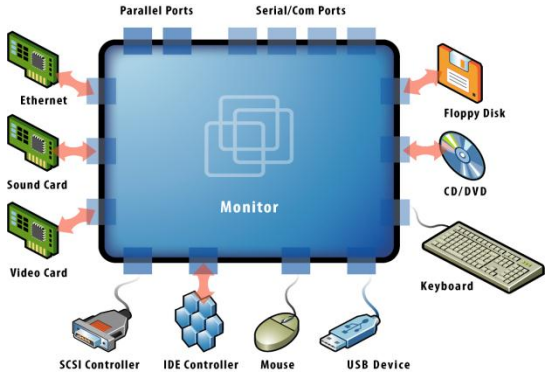


Fig 3: Virtual Machine Anonymous (Dec, 2012)

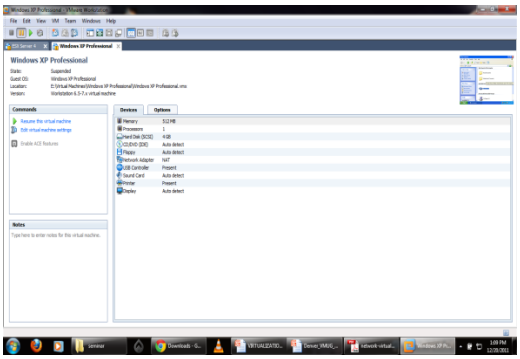


Fig 4: Snapshot of VM

B. Virtual Machine monitor

A layer called a VM monitor or manager (VMM) creates and a control the VM's other virtual subsystems.

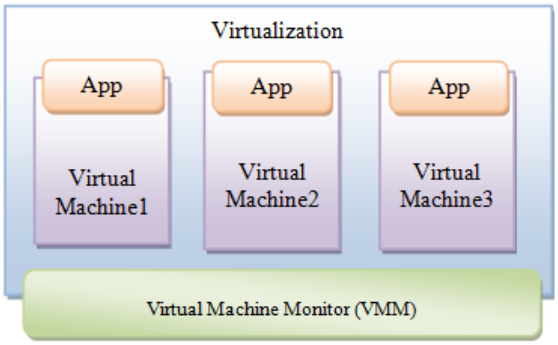


Fig 5: Virtual Machine Monitor

C. Hypervisor

A hypervisor is one of many virtualization techniques which allow multiple OS, termed guests, to run concurrently on a swarm computer, a feature called hardware virtualization. It is so named because it is conceptually one level higher than a superior. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest OS. Multiple instances of a variety of operating systems may share the virtualized resources. Generally, Hypervisor is installed on server hardware whose only task is to run guest operating systems.

IV. VIRTUALIZATION APPROACHES

A. Operating system-based virtualization

Virtualization is enabled by a hosting operating system that supports multiple isolated and virtualized guest OS on a single physical server with this characteristic that all are on the same operating system kernel with has control on Hardware infrastructure Exclusively. The hosting operating system has visibility and control above the VMs. This approach is simple but it has susceptible. For example, an attacker can inject kernel scripts in hosting operating system and this can cause all guest OS have to run their OS taking place this kernel. The result is attacker have control over all VMs that exist or will establish in future.

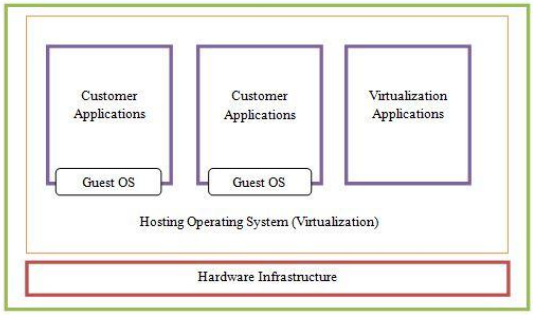


Fig 6: Operating system-based virtualization

B. Application-based virtualization

An application-based virtualization is hosted on top of the hosting OS. This virtualization method emulates each VM which contains its own guest operating system and related relevance's. This virtualization architecture is not commonly used in commercial atmosphere. Security issues of this approach are similar to Operating system-based.

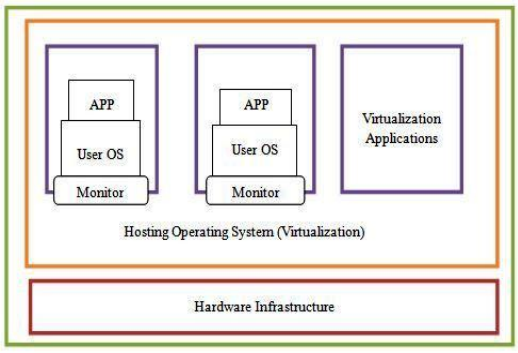


Fig 7: Application-based virtualization

C. Hypervisor-based virtualization

A hypervisor is embedded in the hardware infrastructure or the hosting OS kernel. The Hypervisor is available at the booting time of machine in order to control the sharing of system resources athwart several VMs. Some of these VMs are privileged partitions that they managed the virtualization platform besides hosted VMs. In this architecture, the privileged partitions have visibility and control the VMs. This approach establish most

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

controllable environment and can perform additional security tools such as Intrusion detection systems. But it was vulnerable because of the hypervisor is single peak of failure. If hypervisor crashed or aggressor gets control over it then all VMs are on the assailant control. However, take control over hypervisor from VM level is difficult but not impossible.

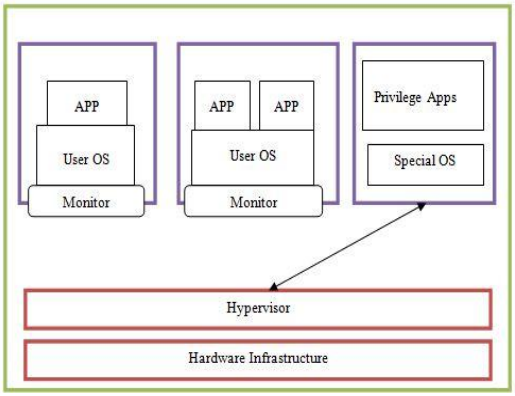


Fig 8: Hypervisor-based virtualization

D. virtual infrastructure

It provides a layer of abstraction surrounded by computing; networking hardware and, storage, and the applications running on it (see Figure 9). The deployment of virtual infrastructure is being disorderly, since the user experiences are fundamentally unchanged. However, virtual infrastructure gives administrators the advantage of managing pooled resources athwart enterprise, allowing IT managers to be more responsive to dynamic organizational needs and to better leverage infrastructure investments.

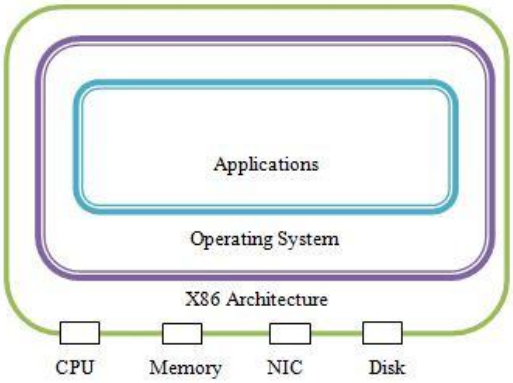
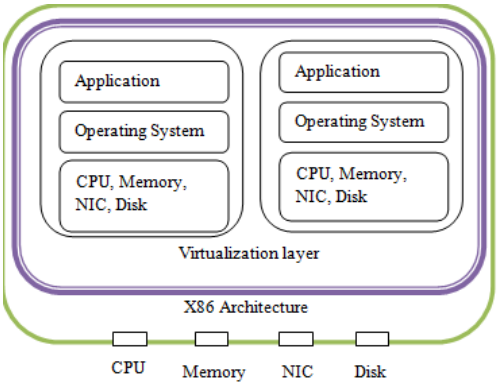


Fig 9: Before Virtualization



after Virtualization

V. TYPES OF VIRTUALIZATION

Server virtualization enables multiple virtual operating systems to run on a single substantial machine, yet remain logically distinct with consistent hardware profiles (burry & nelson, 2004). To the contrary, server virtualization can often take the place of the costly practice of manual server consolidation, by combining many physical servers keen on one server. "the idea is to present the illusion of one huge machine that's substantially powerful, reliable, robust and manageable - whether it's one machine that looks like many, or multiple machines tied together to seem to be like a single system" (brandel, 2004). The focus of server virtualization is on maximizing the efficiency of server hardware in order to increase the return on investment for the hardware.

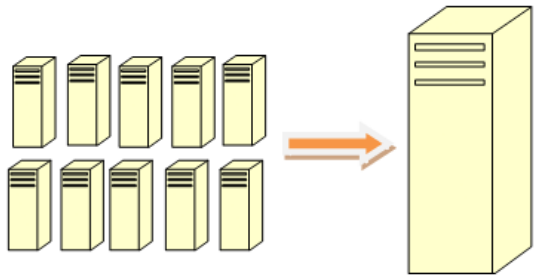


Fig 10: Server Virtualization

B. Desktop Virtualization

It is used to move end user desktops from their local PC, "to the cloud". In other words, end user desktops are virtualized and they are accessed using thin client devices.

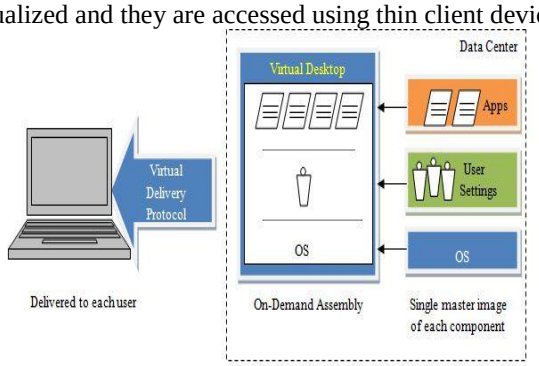


Fig 11: Desktop Virtualization

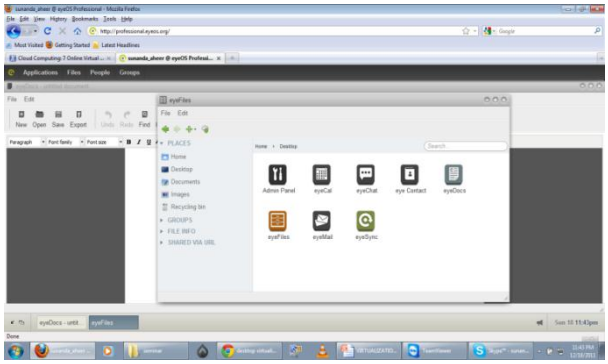


Fig 12: snapshot of virtual Desktop

C. Application Virtualization

While most of the rampant virtualization strategies focus on the hardware infrastructure. With application

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

virtualization (also commonly referred to as service virtualization) end-user software is "packaged", stored and distributed in an on-demand trend athwart a network. This virtualization strategy goes hand in hand with unvarying web services initiative that is making waves in the IT industry today. Virtualized application uses a common abstraction layer, which defines a protocol, allowing them to communicate with one another in a standard messaging format. Thus, application can invoke one another in order to perform request functions. A virtualized application is not only capable of remotely invoking requests and revisit results, but also ensuring that the application's state and other data are available and consistent on all resource nodes executing the application across a grid.

D. Storage Virtualization

It is used to run virtual storage appliances which can be easily moved from one hardware platform to another .Storage virtualization attempts to maximize the efficiency of storage devices in information architecture.

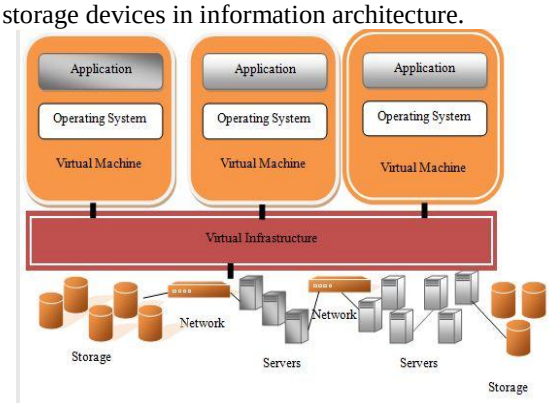


Fig 13: Storage Virtualization

E. I/O Virtualization

It is used to reduce the number of I/O cables that go to a server and gain flexibility. I/O Virtualization enables discrete I/O resources to be shared and dynamically allocated across many physical servers with no loss of throughput. This optimization can result in improved performance of the computer system. I/O Virtualization physically removes I/O components – adapters, cables, network ports and storage – from servers, leaving them as pure compute and memory engines. It pools these resources behind the I/O Virtualization (IOV) switch and allocates them to the servers through 'virtual' adapters. In some products, Direct Attached Storage (DAS) is also virtualized. Servers are connected to the IOV switch by one or more high-speed interconnect cables – PCI Express. No other network or storage cable is required to connect directly to the server. All network connectivity is provided through the IOV switch, vitalizing each I/O device with an image which looks to the server software exactly the same as the original physical I/O device. Profiles of I/O configuration and bandwidth requirements are created for each server in software. These profiles can then be applied and changed with simple commands, remotely and can also be automated. Any server can be connected to any network or storage port, dynamically, without changing any physical connections or taking the server down – and with no loss of bandwidth. Network and storage aggregation switches are eliminated. Figure 14 illustrates the functions of I/O Virtualization.

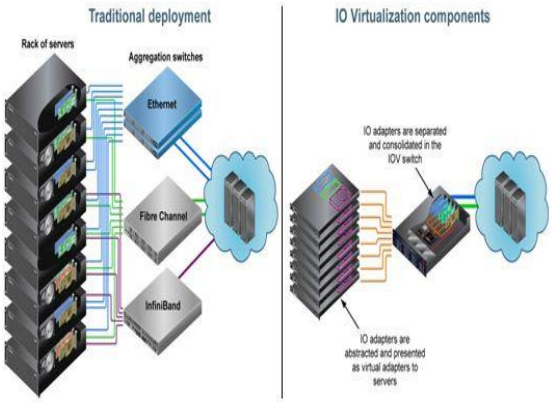


Fig 14: I/O Virtualization (2009)

F. Network Virtualization

It is used to create virtual networks inside a server to connect VM's together and create virtual security zones. A common practice it to create implicit LANs, or VLANs, in order to more effectively manage a network.

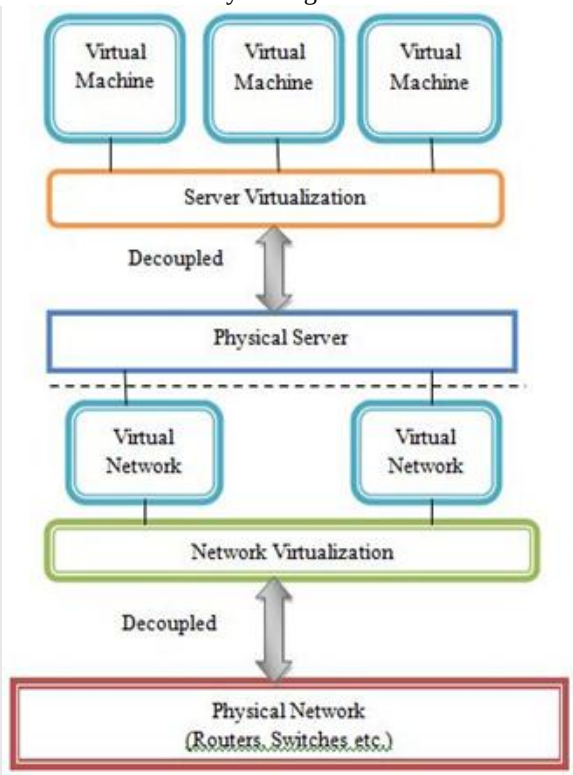


Fig 15: Network Virtualization

VI. SECURITY VULNERABILITIES IN VIRTUALIZATION

A. Communication between VMs or Between VMs and host

One of the primary benefits that virtualization bring isolation. This benefit, if not carefully deployed become a threat to environment. Isolation should be carefully configured and maintained in a virtual environment to ensure that the applications running in one VM don't have

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

access to the applications running in another VM. Isolation should be strongly maintained that break-in into one virtual machine should not provide access either to virtual machines in the same environment or to the underlying host machine.

Some virtualization circumvents isolation, in order to support applications designed for one operating system to be operated on another OS, this solution completely exploits the security bearers in both the operating systems. This kind of system, where there is no isolation between the host and the VMs gives the virtual machines an unlimited access to the host's resources, such as file system and networking devices. In this case the host's file system becomes vulnerable.

B. VM Escape

VM's are allowed to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host. That is, the virtual machines are designed in a way that a program running in one virtual machine cannot monitor, or communicate either with programs running in other VMs or with the programs running in the host. But in reality the organizations compromise isolation. They configure flexible isolation to meet their organization needs which exploits the security of the systems. New software bugs were already introduced to compromise isolation. One such example of this kind of attack is VM escape. VM escape is one of the worst case happens if the isolation between the host and between the VMs is compromised. In VM escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer), and get access to the host machine. Since the host machine is the root, the program which gain access to the host machine also gains the root privileges basically escapes from the virtual machine privileges. This result completely breakdown in the security framework of the environment. This problem can be solved by properly configuring the host/guest interaction.

C. VM monitoring from the host

Host machine in the virtual environment is considered to be the control point and there are implications that enable the host to monitors and communicate with the VM applications up running.

Therefore it is more necessary to strictly protect the host machines than protecting distinctive VMs. Different virtualization technologies have different implications for the host machine to influence the VMs up running in the system. Following are the possible ways for the host to influence the VMs.

- The host can start shutdown, pause and restart the VMs.
- The host can able to monitor and modify the resources available for the virtual machines.
- The host if given enough rights can monitor the applications running inside the VMs.
- The host can view, copy, and likely to modify the data stored in the virtual disks assigned to the VMs.

And particularly, in general all the network traffic to/from the VMs pass through the host, this enables the host to monitor all the network traffic for all its VMs. In which case if a host is compromised then the security of the VMs is under question. Basically in all virtualization technologies, the host machines are given some sort of basic rights to control some actions such as resource allocations of the VMs running on top. But care should be taken when configuring the VM environment so that enough isolation should be provided which avoids the host being a gateway for attacking the VM.

D. Denial of Service

In VM architecture the guest machines and the underlying host share the physical resources such as CPU, memory, network resource and disk. So it is possible for a guest to impose a denial of service attack to other guests residing in the same system. Denial of service attack in virtual environment can be described as an attack when a guest machine takes all the possible system's resources. Hence, the system denies the service to other guests that are making request for resources; this is because there is no resource available for other guests. The best approach to prevent a guest consuming all the resources is to limit the resources allocated to the guests. Current virtualization technologies offer a mechanism to limit the resources allocated to each guest machines in the environment. Therefore the underlying virtualization technology should be properly configured, which can then prevent one guest consuming all the existing resources, thereby preventing the denial of service attack.

E. Guest-to-Guest attack

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. If the hacker could also get control of the hypervisor and he owns all data transmitting between the hypervisor and VMs and he can perform a spoofing attack.

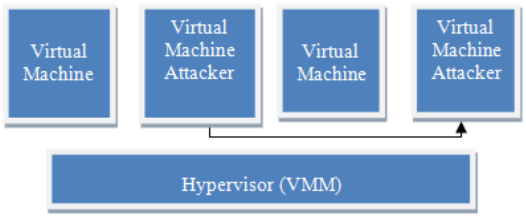


Fig 16: Guest-to-Guest attack

F. Hypervisor Security

In a virtualization environment there are several VM that may have their independent security zones which can't accessible from other VMs which have their own zones. In a virtualization environment a hypervisor has own security zone and it is the controlling agent for everything within the host of virtualization. Hypervisor can touch and affect all acts of the VMs running within the virtualization host

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

(Sabahi, F.2011).There are multiple security zones but these security zones exist within the same physical infrastructure that in more traditional senses generally only exists within a single security zone. This can cause a security issue when an attacker can take control over hypervisor then the attacker have full control on all works within hypervisor territory. Another major virtualization security concerns is "escaping the VM" or being able to reach the hypervisor from within the VM level.

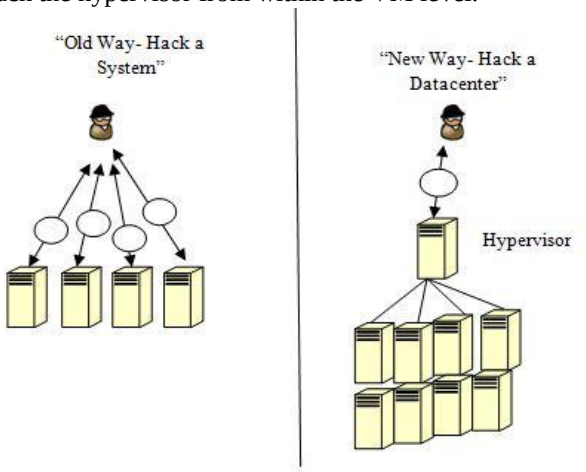


Fig 17: Attack on virtualized environment

VII. BENEFITS OF VIRTUALIZATION

A. Save Hardware Cost and Footprint

Virtualization provides the ability to take advantage of multiple operating systems on one embedded controller or PC, without investing in a separate computer for all OS. This allows engineers to buy less hardware and reduce overall system footprint (which is especially important in deployed applications).

B. Take Advantage of Operating System Services

With virtualization it is possible to take advantage of the capabilities offered by different operating systems on just one situate of hardware. For example, a designer may wish to use graphics services provided by Windows in conjunction with deterministic processing provided by a real-time OS such as Lab VIEW Real-Time.

C. Make Use of Multi-core Processors

Virtualization software can allow users to directly assign groups of processor cores to individual OS's. For example, if an engineer wishes to use Linux and a more CPU, real-time OS and memory resources can be allocated to the real-time OS so that performance can be optimized. Running virtualization software on a given computer allows designers to make the most of their processing resources by keeping processor cores busy.

D. Test Beta Software and Maintain Legacy Applications

The ability to run two or more OS's side-by-side means that programmers can test new releases of software without the need of dedicated trial machines. If beta software corrupts a given OS, a parallel operating system running on the same computer can still be used for development.

In addition, virtualization can help extend support for legacy applications and operating systems to latest hardware. By running legacy and new operating systems on the embedded controller or same PC (e.g. Windows 95 and Vista), engineers can reuse legacy applications and reduce the need to port programs to different operating systems.

E. Increase System Security

Since individual operating systems running on a virtualized machine can be isolated from all, virtualization is one way to create secure machines (e.g. for military applications). This reduces the need for multiple physical computers that operate at different security levels but are not fully utilized.

VIII. CONCLUSION

Virtualization brings very little added security to an environment. One of the key issues is that everyone should be aware of the fact that virtual machines represent the logical instance of an underlying system. So many traditional computer threats apply the same to the VM's also. Another issue that makes the security consequences difficult to comprehend, there are so many different types of virtualization technologies available in the market. Each of it has its own merits and demerits; each virtualization deployment is different depending on the need for the virtualization. Majority of the security issues presented here concerns the security of the host and hypervisor. If the host or the hypervisor is compromised then the whole security model is broken. Attacks against the hypervisor become more popular among the invaders realm. Therefore after setting up environment, care should be taken to ensure that the hypervisor is secure enough to the newly appearing threats, if not patches have to be done. Patches should be done frequently so that the risk of hypervisor being compromised is avoided. Virtualization is a powerful solution to reduce the operational costs in today's computing but if done wrong it become as a threat to an environment. While implementing, exaggerate the security model to with stand the attacks. And keep monitoring for new developments that emerges in this field and continue to stay up to date.

REFERENCES

[1]. (2009) Improving HPC Cluster Cost-Performance Through I/O Virtualization, Issue 1, Virtensys Ltd.
[2]. (2009) Virtualization Basics. http://zone.ni.com/ devzone /cda/ tut/p/id/8708.
[3]. M. Brandel, (2004) Wired over server virtualization. http://www.networkworld.com/supp/2004/ndc4/0621virtarch.html.
[4]. C. M. Burry and C. Nelson (2004) Plan on server virtualization. http://www.computerworld.com.
[5]. F. Morgan (2006) Virtualization. http://www. Window security.com /whitepapers /Network_ Security/.
[6]. J. S. Reuben, A Survey on Virtual Machine Security, Seminar on Network Security, (2007), TKK T-110.5290.
[7]. F. Sabahi, "Virtualization-Level Security in Cloud Computing", IEEE, Pp.250-54, (2011).
[8]. (2012) World of Virtualization. https://shounaksaheb. wordpress. com/2012/12/25 /world-of-_virtualization/.