Abstract

Security in Virtualization

by

Larry Gene Hastings Jr

Hastingsl14@students.email.ecu

Fulfillment of ICTN 6823 Course Requirements

Formatting in APA

Master of Science

Network Technology

East Carolina University

July 24, 2014

To be Submitted to http://www.infosecwriters.com

Abstract

Virtualization has many benefits that corporations are now beginning to understand more thoroughly and, thereby, take advantage of. Not long ago, a computer was represented by by a physical case coming in many forms, but inherently separate and functioning completely independent of other computers. Basically, this means motherboards, hard drives, power supplies, and various adapters had to be assigned and used in each individual unit. Each of these units could have one operating system installed as well. This meant that if an operator wanted to use multiple systems, then they would also need multiple physical machines. This is no longer true because of the advent of virtualization, which allows for physical storage systems such as raids to be virtually divvied up with varying size and memory requirements to function optimally without wasting resources. It is especially useful because load requirements change, and additional resources can be decreased or increased as needed. But, having all these operating systems together logically, if not physically, presents new avenues for possible breaches of security. This paper will describe how virtualization works, what security problems it presents, and what measures can be taken for security that may differ from traditional measures used for physically separate machines.

Security in Virtualization

by

Larry Gene Hastings Jr

Hastingsl14@students.email.ecu

Fulfillment of ICTN 6823 Course Requirements

Formatting in APA

Master of Science

Network Technology

East Carolina University

July 24, 2014

To be Submitted to http://www.infosecwriters.com

Table of Contents

Security in Virtualization

Summary

In computer terms, virtualization means creating or installing a system on, possibly, a small part of one hard disk or across many using an array of disks. As opposed to traditional methods of hosting operating systems, virtualization provides a different approach. One that can both save an organization overhead cost, but also enable a higher ability to be flexible and adapt to changing situations. More organizations are delving into this technology every year, but with any new method of conducting operations, there will be different or possibly unforeseen security vulnerabilities that present themselves. How then, can the information security officers overseeing this newer addition for hosting and providing operating systems provide the same level of security expected from the organization methodology? Understanding what virtualization is, what different security issues it may present, and how both management and technical personnel should go about securing it is a good start. Through these understandings, an organization implementing virtualization may meet its information security goals.

Analysis

What is Virtualization

There are actually many different types of virtualizations. Network virtualization is the separating of physical computing networks used for connecting and sharing data. A widely used method by the IT network administrator, it is an invaluable tool in organizations. The next type is desktop virtualization, which involves hosting a desktop at a central location that is accessible remotely by logging in with valid credentials. Another is storage virtualization, that can be summed up as using a centrally accessed storage location that makes data duplication and redundancy throughout an organization more easily controlled. Application virtualization is

much like storage virtualization in that certain applications, such as those found in Microsoft Office, can be offered when connected to specific servers. A good example of this is using the limited version of Microsoft Office when accessing data on Microsoft OneDrive or Google Drive through their respective email services. Many of these virtualizations are used each and every day by the common user without understanding the underlying aspects making them work. Although these are all important tools in their own respects, this paper will focus on operating system virtualization or virtual machines.

Operating systems come in many forms. Microsoft is a popular one used throughout the world as well as Unix and Linux systems. Each may come in flavors that pertain to average users and their personal desktops or may work on larger scale servers. Virtualization is especially useful in server environments because it can reduce a company's footprint. Douglis & Krieger (2013) state "It's critical to green computing" and "it's even being used today across data centers" (p. 7). The general makeup of a virtual machine setup involves hardware, a host operating system, a virtual application, and any virtual operating systems installed. It is important to understand the characteristics of the different parts that make up a system.

Hardware is the underlying equipment used to host any system. The general makeup of a computing system as listed by Kyrnin (2014) includes a case, power supply, motherboard, processor, heat sink, memory, hard drive or drives, Optical disk, video card, sound card, and a network card. A system with multiple virtual machines allows all operating systems installed to utilize each piece of hardware concurrently while running atop the host operating system.

Although not always true, normally host systems are a bare-bones version of an operating system, often coming with command line interface only. Some of the more popular host systems include Linux versions, but being seen more in the IT community is the utilization of operating

systems designed for virtualization only. This takes away the need to install an additional application on top of the host. One of the more popular virtualization specific hosts in large organizations is VMware vSphere or ESXi. It is installed much like a normal system, but is designed to use very little hardware resources. VMware (2014) describes it as "a bare-metal hypervisor that installs directly on top of your physical server and partitions it into multiple virtual machines" and "each virtual machine shares the same physical resources as the other virtual machines and they can all run at the same time" (para. 1). The hypervisor that is described is the platform or underlying software that enables the virtual machines to interact with the hardware system. If this type of host system is not used, a virtual application must installed.

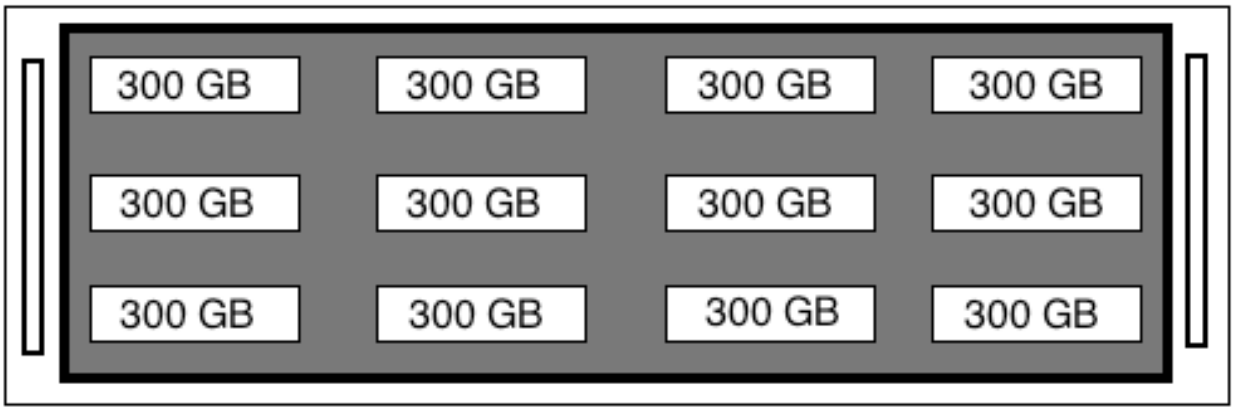
There are numerous virtual applications that can be installed that support many different types of virtualization. As stated above, this type of program needs to be installed on an up-and-running system to work. When the program is started, one has the option to install and allocate resources for each virtual machine. There are numerous free versions and costly ones that may offer an abundant array of options and services. Once the operating system is installed through the virtual application, it is considered a virtual operating system because it can be brought up through this application simultaneously with either the host system, or in some cases, another virtual operating system.

Virtualization Storage

Data storage can be a complicated matter, especially with large amounts. Virtualization of many different machines seems like it would be very difficult using a single server or tower setup, but it inherently makes it easier. Actual operating systems do not normally require a lot of disk space, but it is the user files that do. Some companies require picture and video storage which will eat up space quickly. An industrial type server virtualization system, especially those

found in data centers, will use sophisticated storage systems such as a redundant array of independent disks (RAID) setup. There are various ways to connect these systems, but here it is important to understand how virtualization takes advantage of the storage. Figure 1 shows an example of the faceplate of a general RAID hard disk system. A host system may connect to this rack mounted unit that holds an array of 12 independent 300 Gigabyte (GB) disks. Thus, when combined, this system becomes a 3600 GB virtual hard drive that can be divvied up as virtual machine needs rise or lower. For instance, a company may run 5 virtual servers on one system; one requiring 600 GB, one requiring 900 GB, one requiring 300 GB, one requiring 12150 GB, and the last one needing only 100 GB. This setup would consume all but 350 GB, which could be used in the future when additional space is required. The unique part of virtualization enables administrators to increase and decrease storage as needed or let the virtual application itself expand the size as required, which is the most efficient method (Microsoft, 2014). This is an optimal way to manage storage and virtualization makes this possible.

Figure 1.



Benefits of Virtualization

Benefits of virtualization are numerous, but one author puts it best by stating "Virtualization can reduce capital spending on unnecessary IT resources, as well as reduce the

amount of energy consumed by increasingly power-hungry IT departments, thereby reducing total cost of ownership" (Kenney, 2008, p. 63). Although, initially setting up a virtualized system can be costly, in the long run, it does pay off. This is possible because virtualization enables the efficient use of all the hardware that makes up a computing system. This cuts down on such things as server sprawl, which is the poor use of hardware resources. Now, IT departments can allocate resources to optimally take advantage on all hardware such as processors, memory cards, and as illustrated above, storage. More to the point though, input/output (I/O) devices can be utilized better because it will only require one network device, peripheral device, optical device, and, possibly, tape device. Think of the cost of having 10 machines with 10 physical hardware components, which entails all the hardware items listed above for each. This becomes extremely inefficient, requires lots of power, and makes for a very large footprint. Through virtualization, organizations can combine all these machines on one small system that uses much less power and costs much less for hardware.

Security Issues

Network security is a way to protect an entire organization. It is an important part of information security. It can be thought of as a first line of defense, but it is not guaranteed to thwart all attacks. Virtualized machines have different parts that need to be protected, and because many parts reside on the application layer more than anything, which network security may or may not address, it is important to identify these parts. To be protected and monitored are the virtual machine or guest machine, the host operating system, the hypervisor, management interfaces, and virtual infrastructure including networks linked to storage systems (Pék, Buttyán, & Bencsáth, 2013). Because there are so many parts, each area must be specifically broken down to show vulnerabilities.

Virtual machine. The operating system that has been virtually installed is, realistically, the focal point of attackers. Through the virtual machine, attackers are able to gain valuable information. Virtual machines were intended to be transparent to attackers; that is, they were meant to be invisible or undetectable, but in today's world, this is not so (Pék et. al, 2013). As virtualization has evolved, so have the threat agents. Because the underlying system of a virtual machine is normally running all the time, it presents an ability to access dormant or powered-down systems. The information is still stored to hard disk. It may be inoperative at the moment, but the data is present in the storage system. Pek et. al (2013) writes "dormant VMs are inadvertently neglected in most of the cases, which is a serious problem, as they can still contain encryption keys, authentication data, or other sensitive information" and "moreover, inactive images are typically left out of security measures, such as security patches, access policies, or sensitive configurations" (p. 40:13). These are threat vulnerabilities only for dormant virtual machines.

In addition, active virtual machines have some different issues to deal with. With so many avenues of attack, active systems are especially risky. The biggest threat is a cross-virtual machine attack where one machine is compromised, and then the attacker is able to access other machines (Pek et. al, 2013). There are many other avenues of attack as well, but it is important to understand that hackers have developed ways to identify virtual machines when accessed, and therefore can use certain proven methods to infiltrate either virtual or physically connected systems.

Host operating system. The host is much like any system. Normally, it is in a constant state of power, constantly running to provide a platform for any virtual machines that are needed to be functional. In saying this, it is susceptible to the normal array of attacks, but the problem is

that it can be used to attain connectivity to virtual machine systems. It is then the responsibility of the administrators and management to use proper security measures that protect it from common and uncommon attacks as pertain to any other system.

Hypervisor. This layer is the mechanism that allows virtual machine creation and operation by assigning physical resources. The hypervisor "surrounds or underlies an operating system and provides the same inputs, outputs, and behavior that would be expected from an actual physical device" (Pearce, Zeadally, & Hunt, 2013, p. 17). Being that it interacts with the host system, the hardware, and the virtual machines, there are many vulnerabilities that must be protected against. This may be the most essential part of virtualization to protect. In a report made by IBM, more than a third of security threats come from the hypervisor most notably in the form of hypervisor escape and hyperjacking (Cmeier & Mnovellino, 2013). These attacks entail gaining administrator privileges to an in-use hypervisor or installing a malicious and unseen hypervisor that can control the virtual machines.

Management interfaces. This tool, which may come in different forms as pertains to the virtualization setup, is a method for administrators to oversee all the virtual machines and their setups through one tool. Whether it be a program installed on a host operating system or, as in ESXi from VMware, whether it be a specifically designed operating system for virtualization. These management tools can be accessed locally or remotely for convenience, but opens the system up to security threats such as arbitrary code execution, information leakage, or remote network access (Pek et. al, 2013). These types of attacks generally involve inserting malicious code or the intercepting of administrator credentials to gain access to the system.

Virtual infrastructure. The complete package of what makes up a virtualized system can be deemed the virtual infrastructure. Using a server that connects to a large storage space

demonstrates two parts, but more importantly, it is what enables them to talk to each other. An organization may use an internet small computer system interface (iSCSI) or it may use network access storage (NAS). It may be contained on a private local area network (LAN), which entails the use of switches and routers. Using remote access to manage a system, as talked about above, entails access to and through these appliances. The system as a whole must be looked after. It is important to have administrators, possibly expert network personnel, that can maintain and secure these different parts adequately.

Identification of Solution

Security at the Technical Level

Personnel at the technical level hold the true knowledge base of the systems in place. These persons know the intricacies of their respective fields and how their equipment is mobilized. The levels seen in this field vary from junior technical support to expert technical support. It is the responsibility of these employees to not only implement security, but to also maintain and investigate security weaknesses. Management can institute policies and procedures, but they will also look to the technical level for knowledge on specific implementations.

One of the best ways to stay ahead of security threats is to harden all systems. "Hardening refers to providing various means of protection in a computer system," which "means to protect at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between" (Janssen, 2014, para. 1). To break this down, it basically means to take away any unneeded services on any virtual system that may be used as an avenue of attack. This is a process that takes much time and contemplation. Technical knowledge must either be gained through experience or training.

Experience is gained through years of working on virtual systems. Knowing the intricacies of a system is important, but technology changes and new systems can be introduced. This is why training and certification are important aspects in the security field, especially those pertaining to virtualization because it is a relatively new concept for many users. There are many low-level training and certification opportunities up to mid-level and expert areas. As virtualization becomes more common in all organizations, the technical expertise must increase as well.

Training is not enough though. Personnel implementing security for virtualization must stay vigilant as the computing world changes. Each and every day, hackers are coming up with new ways to infiltrate systems. It is the responsibility of the technical level administrators to stay abreast of new types of attacks and concerns. A security implementation is only as good as long as it is maintained or upgraded to meet new threats. For specific virtualization countermeasures, Pek et. al (2013) provides these recommendations for virtualization security:

- Secure Programming
- Hardening the Hypervisor and VMs
- Restriction of Physical Access
- Policy and Isolation
- Separation of Roles
- Separation of VMs
- Consider the State of VMs
- Mitigate Design Discrepancies
- Secure the Network
- Adequate Logging and Monitoring

Security at the Management Level

This level has the toughest time with virtualization security because many of these individuals came up through the ranks of employment at a time when virtualization was not used widely. Therefore, their technical experience in the field are, in most cases, less than adequate. How then can management bridge the gap between technical expertise and management? It is said that the boss is only as good as his or her employees. Management must refer to the technical experts that work for them to gain knowledge that will give direction on how the company will secure these systems. Training is also another method. This is important because management is often tasked with providing policies and procedures for the company, and especially for any virtualization within the computing department. This will not fall to upper-management such as a chief security information officer (CISO), which provides a more general overview of security, but will, more than likely, be the responsibility of a data center manager in larger organizations. When discussing virtualization security controls, Hoesing (2009) reports three critical themes that must be managed to include asset management, change management, and configuration management. Through managing each of these themes, the company can more easily ensure that virtualization is secure.

Asset management. Assets are often thought of as physical items such as computer hardware, but software is an asset as well. Virtual machines, host operating systems, and applications are all software items. Policies should be created to track where these different instances of virtualization reside. Knowing what storage system a virtual machine is located on can be important, especially those using and containing sensitive company content. Often, when virtualization takes place, dormant machines can be forgotten. Proper asset tracking will ensure that each one is known and seen to for security purposes. For instance, when applying security

patches, tracking and documentation of virtual machines will ensure that none are missed, which could possibly provide an avenue of attack.

Change management. During an instance where something changes concerning virtualized systems, a management of change procedure should be followed. Management should take advise from technical experts while creating this procedure to make it as efficient as possible. A change can be as small as updating an antivirus to installing a virtual machine. It can also represent making changes to any configurations that may be tied with security implementations. This procedure should take into account what the effects of this change may do. All changes should have an adequate level of authority to implement, thereby making them more secure.

Configuration management. The configuration of any hardware appliance or software application should be documented and approved. This is a policy that is created by management as well. Having consistent configurations across platforms will ensure security policies are being met.

Conclusion

Virtualized systems can make an organization more efficient and more productive. It can save money, time, and effort, but it must be implemented correctly. To understand and make virtualization efficient, organizations must take a proactive approach to understanding the intricacies of the systems in use. By doing this, organization computing personnel will be more able to apply best security practices to ensure that attacks are mitigated and sensitive data is secure.

References

Cmeier & Mnovellino. (2013, October 26). Virtualization vulnerabilities related to hypervisors. [Web log comment]. Retrieved from http://cybersecurity.mit.edu/2013/10/virtualization-vulnerabilities-related-to-hypervisors/

*Douglis, F. & Krieger, O. (2013). Virtualization. *IEEE Internet Computing, 17*(2), 6-9.

*Hoesing, M. T. (2009). Virtualization Security Assessment. *Information Security Journal: A Global Perspective, 18*(3), 124-130.

Janssen, C. (2014). *Hardening.* Retrieved from http://www.techopedia.com/definition/24833/hardening

Kenney, B. (2008). Virtual Machine Utilization. *Industry Week/IW*, *257*(3), 63.

Kyrnin, M. (2014). *Desktop PC parts checklist.* Retrieved from http://compreviews.about.com/od/general/a/DesktopPCParts.htm

Microsoft. (2014). *Planning for disks and storage.* Retrieved from http://technet.microsoft.com/en-us/library/dd183729(v=ws.10).aspx

Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualization: Issues, Security Threats, and Solutions. ACM Computing Surveys, 45(2), 17-17:39.

*Pék, G., Buttyán, L., & Bencsáth, B. (2013). A survey of security issues in hardware virtualization. *ACM Computing Surveys, 45(3), 40-10:30.*

VMware. (2014). *vSphere ESXi Hypervisor.* Retrieved from http://www.vmware.com/products/vsphere/features/esxi-hypervisor.html