Journal of Business & Leadership: Research, Practice, and Teaching (2005-2012)

Volume 7
Number 1 *Journal of Business & Leadership*

Article 4

1-1-2011

Real Risks In A Virtualized World: How Virtualization Is Changing The Way We Manage, Assess, and Mitigate Risk

Brian Boyer
Fort Hays State University

Keyu Jiang
Fort Hays State University

Robert Meier
Fort Hays State University

Hongbiao Zeng
Fort Hays State University, h_zeng@fhsu.edu

REAL RISKS IN A VIRTUALIZED WORLD: HOW VIRTUALIZATION IS CHANGING THE WAY WE MANAGE, ASSESS, AND MITIGATE RISK

Brian Boyer, Fort Hays State University
Keyu Jiang, Fort Hays State University
Robert Meier, Fort Hays State University
Hongbiao Zeng, Fort Hays State University

A dramatic shift has started to take place in the last decade that is having a pronounced impact on how organizations view information security. Large datacenters and small server rooms alike are being impacted by the development and growth of virtualization and the many benefits it provides. This essay will examine how hardware virtualization has changed the landscape of datacenter risk management and how organizations must adapt their security posture to those changes. As mainstream hypervisors like VMware ESXi, Citrix XenServer, and Microsoft Hyper-V become more affordable and easier to implement, their use in providing low-cost, high-utilization solutions is steadily becoming an industry standard, even for smaller shops. Organizations must understand how to assess, manage, and mitigate new types of risk unique to virtualization. By examining the technology behind virtualization, the risks associated with it, and the methods organizations can use to mitigate and minimize those risks, we will see that virtualization, when implemented properly, can provide a secure, highly beneficial technology on which datacenters can be built.

INTRODUCTION

A dramatic shift has taken place in the last decade that is having a pronounced impact on how organizations view information security. Experts predict that by 2012 approximately 50% of x86 server workloads will be virtualized (Gartner, 2009). It's a phenomenon that is undoubtedly gaining momentum. Gartner's Phil Dawson went so far as to state that visualization will be "the highest-impact issue challenging infrastructure and operations through 2015" (Gartner, 2010). Though virtualization as a technology has been around since the 1960s when IBM developed it for use with its large mainframes (Reuben, 2007), a number of factors have led to its marked increase over the last decade. First, the cost of hardware to support virtualization has gotten significantly smaller in recent years as processor, memory, and storage components have advanced (Koomey, Belady, Patterson, & Santos, 2009). The power of today's hardware has outpaced operating system (OS) and application utilization so much that most resources go unused. Second, the development of processors designed specifically for virtualization, like the Intel VT and AMD SMV processors (Perez, van Doorn, & Sailer, 2008), along with the development of x86 virtual host operating systems (VM Tech, 2010), like VMware's ESXi and Microsoft's Hyper-V, has made virtualization available to organizations that previously couldn't afford it. Third, the benefit organizations get from rolling out a virtual environment, such as better utilization of hardware, lower maintenance and renewal costs, increased availability and portability, and a smaller carbon footprint, have spurred CIOs around the globe to hang their reputation (and their company's bottom line) on virtualization's very real benefits (Plas, 2007).

Though virtualization provides a number of benefits, it is not without issues, and security is at the top of the list (Price, 2008). One of the most common pitfalls during the introduction of any new technology is that security is considered only as an afterthought. Rather than building it into the planning and testing phases, too often security considerations are left for after the technology deployment is nearing completion or even already in production. This can cause considerable difficulty and cost if the technology is implemented using inappropriate security practices, and therefore must be refashioned in order to adhere to the organization's security policies. Virtualization is no exception to this pitfall. Gartner predicts that 60% of virtualized servers will be less secure than their physical counterparts through 2012. In this essay we will examine the benefits and risks associated with virtualization in order to determine if it truly presents a secure, long-term solution for enterprise and small business server deployments. Much has been written about the advantages of virtualization, but what sort of vulnerabilities are associated with it, and are those vulnerabilities worth the risk? What security controls should be implemented in order to mitigate vulnerabilities unique to virtualization? This essay will shed light on virtualization's unique security issues and identify the appropriate steps for minimizing its vulnerabilities and properly deploying a virtual infrastructure. In so doing, we will see that virtualization, if implemented properly, may not only be a paradigm shift changing the way we think about datacenters and computing (Hau, 2007), but also the way we manage, assess, and mitigate datacenter risk.

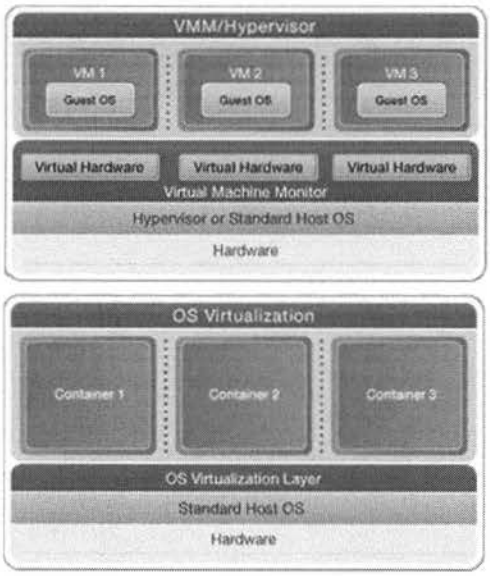
VIRTUALIZATION AND ITS MANY BENEFITS

In order to accurately evaluate its unique risks, we must first have some understanding of how virtualization works. As mentioned earlier, virtualization as a technology has been around since the 1960's when IBM developed it for use with its large mainframes (Reuben, 2007). However, the largest share of today's market is comprised of two types of virtualization technology (IDC, 2010). The first is called hardware virtualization, or full virtualization, and is the primary focus of this paper. The three core components of hardware virtualization are the host OS, which enables booting and provides a local management interface into the system; the hypervisor, or virtual machine monitor (VMM) as it is sometimes called; and the guest operating systems, or virtual machines (VMs). The hypervisor is "a thin software layer" (Price, 2009) which runs on top of the host OS. Its primary purpose is to manage resource allocation and task scheduling for the guest virtual machines. It is responsible for presenting abstracted hardware to the guests, and for controlling the flow of instructions between that hardware and the guest OSs. The hypervisor is also capable of partitioning the host's physical resources in such a way that the VMs are isolated from one another, so that they only have access to their own resources. The hypervisor gets its magic from its ability to present the guest operating system abstracted hardware. The guest in turn "sees" the abstracted hardware as if it were actual hardware. It is unaware that it is being presented "virtual" resources, including virtual CPU(s), memory, network interface card(s), and storage. Therefore, multiple guest operating systems can sit on one physical server, each unaware of the other it is sharing resources with other VMs on the same physical machine. Examples of hardware virtualization include VMware's ESX and ESXi, Microsoft's Hyper-V, and Citrix's XenServer.

With the second type of virtualization, called software virtualization, the hypervisor runs as an application on a standard OS, such as Windows or Linux. It doesn't have direct control over the physical hardware (Price, 2009), and therefore the hypervisor is dependent on the traditional OS for access to the hardware. Resources are therefore emulated rather than abstracted. This type of virtualization is primarily used in testing and development environments and typically not used in production. Examples include VMware's VMware Workstation, Microsoft's Virtual PC, and Parallels Desktop 5. The Figure provides a visual representation of the differences between hardware virtualization abstraction and the emulation of software virtualization.

FIGURE

Representation of the Difference between Hardware and Software Virtualization (Solarvps, 2010)



There is strong statistical evidence that virtualization now plays a prominent role in the implementation plans of many organizations' datacenters (Gartner, 2010). A recent CDW survey of 387 IT executives from organizations with 100 or more employees found that more than 90% of those surveyed said they had begun implementation of virtualization at some level (Caraher, 2010). There is a reason why virtualization is being implemented at such an astounding rate and why it has become a hotbed for research and literature—the many benefits it provides saves

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

organizations time and money (Caraher, 2010). Though the leadership of many organizations may not understand the technology behind virtualization, they certainly understand the importance of remaining technically relevant in their chosen line of business. The ability to effectively adapt to technological change has become a vital component of organizational leadership (Kearns, 2004), and the benefits virtualization promises—financial savings, energy savings, more effective disaster recovery, and lower administrative overhead—have organizational leaders appetites whetted.

Hardware virtualization possesses three key features which are the source for its unique benefits. Encapsulation occurs when the hypervisor keeps all components of a VM, including the OS, applications and all virtual hardware, combined in a single logical unit (Price, 2008). Encapsulation allows multiple VMs to reside on a single host without stepping on one another's toes. The VMs are therefore logically isolated from one another despite residing on the same physical hardware. Interposition occurs when the hypervisor manages all privileged operations to the hardware and intercepts I/Os via I/O abstraction, thus presenting a single set of resources to multiple virtual machines (Price, 2008). The hypervisor, in effect, manages resources in such a way that they appear to the guest OS as a real piece of hardware rather than abstracted hardware. Resources on one physical host are therefore shared among multiple VMs. Considering that only five to eight percent of traditional servers' resources are used (Plas, 2007), resource sharing, as interposition is sometimes called, enables the physical server's hardware to be fully utilized. The hypervisor can also allocate and retract resources based on what a particular VM needs at a given time, thus resulting in better utilization of resources. Introspection provides monitoring and auditing capabilities unique to virtualization. Because the monitoring and auditing takes place outside the confines of the encapsulated VM, audit logging and process monitoring, oftentimes the first target of an attacker, cannot be tampered with in the event the VM is compromised (Scafone, Souppaya, & Hoffman, (2010). Additionally, introspection can modify a guest's state (King, Chen, Verbowski, Wang & Lorch, 2006), including capturing an image of a VM at a specified time, called a snapshot, applying patches to a VM, or mounting file systems to a VM. Each one of these features provides unique benefits. Table 1 lists each benefit and the feature(s) that correspond to it:

TABLE 1

Benefits Unique to Hardware Virtualization

Name	Description	Technology	Benefit
Recovery Time	VM portability introduces new methods for recovering systems in the event of a failure or a disaster.	Encapsulation	✓ Reduced recovery time objective (RTO) ✓ Increased recovery point objectives (RPOs) ✓ Reduction in fiscal cost for disaster recovery site
System Provisioning	VMs can be quickly provisioned from a predefined template, allowing for image standardization including system hardening and baselining	Encapsulation Interposition	✓ Reduction in fiscal cost during the setup and maintenance of deployed physical systems
Administrative Overhead	Centralized management of multiple systems within a single virtual infrastructure via the virtual management system	Encapsulation Interposition Introspection	✓ Reduction in fiscal cost of administering multiple physical systems, including, patching, system monitoring, and system recovery ✓ Reduction of system downtime due to multiple services running on a single physical server
Power Consumption	By hosting multiple VMs on a single piece of hardware, fewer physical resources are required per datacenter	Encapsulation Interposition	✓ Reduction in fiscal cost for power consumption ✓ Potential savings for qualifying Green IT Initiatives (Symantec, 2010)
Hardware Overhead	By hosting multiple VMs on a single piece of hardware, fewer physical servers are required	Interposition	✓ Reduction of fiscal cost for the purchasing, maintenance, and support of physical servers
Security Auditing and Inspection	The hypervisor provides a lower layer from which VM security logging, auditing, and intrusion detection and prevention can be performed	Introspection	✓ A more secure environment can be constructed by logging and auditing outside the VM ✓ Intrusion prevention and detection can monitor systems more effectively by leveraging the hypervisor
Security Forensics	VMs can be frozen at a specific point in time (called a snapshot), retuned to a point in time, and prior system activity that was recorded can be replayed after the attack has occurred	Encapsulation Introspection	✓ Forensic analysis of a compromised system is greatly enhanced by the ability to replay attacks ✓ System recovery from a compromise is greatly enhanced by the use of snapshots

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

RISKS UNIQUE TO VIRTUALIZATION

Paradoxically, the same features that are the source for virtualization's unique benefits—encapsulation, interposition, and introspection—are also the source for its unique vulnerabilities. As is often the case, additional layers of technology that provide greater power and ease-of-use also create additional vulnerabilities (Scafone, Souppaya, & Hoffman, 2010). Encapsulation, for example, allows VMs to be highly portable, able to be quickly moved from one piece of hardware to another (Chen & Noble, 2001). Such portability drastically reduces the recovery time objective (RTO) while also reducing the fiscal cost of maintaining recovery sites with one-to-one hardware for each physical server. However, such portability also creates an attack vector by allowing the theft of entire systems via replication of the VMs' disk image files over a network (Price, 2008). Such attack vectors do not exist with traditional servers because they are directly tied to the server hardware on which the OS is installed. Though interposition greatly reduces administrative overhead by allowing VMs to be quickly provisioned from a predefined template, it also opens the door for administrative misuse resulting in what's called VM sprawl, or the proliferation of VMs due to the ease of provisioning inherent in virtualization (Scafone, Souppaya, & Hoffman, 2010). If an organization does not manage its system provisioning using the appropriate change controls, any number of compromised VMs could easily be deployed from a corrupt template. Likewise, VMs lacking the appropriate hardening and baselining measures could be put on the wire and into production. Though this is also true with traditional servers, the ease with which VMs can be provisioned in a virtual infrastructure increases the likelihood of a corrupt system being introduced into the environment. By leveraging the hypervisor to monitor and audit VMs, introspection provides a unique method for detecting and preventing intrusion (Chen & Noble, 2001). However, by opening a communication channel between the host and VM, it also creates another attack vector for attackers to exploit (King, Chen, Verbowski, Wang & Lorch, 2006). A virtual-machine based rootkit (VMBR), for example, could be used by an attacker to exploit the hypervisor in order to gain access to a guest, thus breaking down the security framework on which virtualization is built. Though there is currently no known VMBR that can bypass the isolation provided by the hardware virtualization architecture, King, et al. (2006) showed with the creation of SubVirt that it is possible to do so using software virtualization. It is likely only a matter of time until the attack vectors created by introspection are exploited in hardware virtualization (Price, 2008).

Though some risks are unique to virtualization, a number of other risks are common to both virtualization and traditional hardware servers, but manifested themselves in different ways. For example, unhardened and misconfigured systems are a vulnerability of both virtual and physical servers. However, a virtual infrastructure presents additional hardening and configuration concerns due to the additional components involved, e.g., the host machine, virtual switches, and how those components interrelate with the guest OSs (Scafone, Souppaya, & Hoffman, 2010). Such layers of complexity only prove to further complicate an analysis of the risks of virtualization. One must not only account for vulnerabilities unique to virtualization, but also account for those traditional vulnerabilities that are exacerbated by virtualization. Though this realization complicates the risk analysis, acknowledgment is a critical piece to fully understanding the unique characteristics of virtualization as opposed to traditional server implementations. Table 2 provides an overview of the vulnerabilities unique to virtualization in addition to those traditional vulnerabilities that are exacerbated by virtualization:

TABLE 2

Risks Unique to Hardware Virtualization

Vulnerability	Description	Example of Threat
VM Portability	Encapsulation of VMs into a single set of files enables them to be highly portable. Where traditional systems were tied to a specific piece of hardware, VMs are not and can be quickly transported, even in a running state.	Theft of VM from compromised host
Virtual Machine Based Rootkit (VMBR) & VM Escape	The host system adds an additional layer of technology which must be accounted for when securing the infrastructure. A VMBR installs an additional, ultrathin virtual machine monitor between the VM and host, thus allowing it to go undetected by the VM.	SubVirt, Blue Pill
Unhardened or Misconfigured System	This is no different than a traditional system being compromised, however with virtualization there are additional layers of technology (namely the virtual host, virtual networking, virtual storage, and the interrelatedness to the VMs) that must be accounted for.	Compromise of an unpatched system
VM Sprawl	Because VMs are so easy to provision when compared to physical servers, the likelihood of unpatched and misconfigured systems being deployed is increased. Likewise, the likelihood of VMs being deployed without going through the proper change control measures is increased.	Multiple VMs being created from an infected template
Virtual Communication Channels	Much of the communication that occurs between the host and VMs, and between VMs residing on the same host, cannot be monitored by traditional methods. For example, two VMs located on the same host communicate via a virtual switch, yet that network traffic never leaves the host's internal bus.	Network intrusion detection system does not flag suspicious traffic between two VMs located on the same host.
Natural or Manmade Disaster	Because multiple VMs reside on a single host, or host cluster, the failure of a piece of hardware will effect multiple systems.	20 VMs fail due to a power surge that brings down a single server rack of hosts machines

RISK MANAGEMENT METHODOLOGY

In order to effectively perform a risk vs. benefit analysis for hardware virtualization, a framework must be chosen on which to build the investigation. NIST's SP 800-30 Risk Management Guide for Information Technology Systems provides just such a framework that can be used by the general public for a wide range of assessments (Harris, 2008). Comparing the vulnerabilities of hardware virtualization and the methods and controls available to mitigate them with its benefits will allow us to determine if virtualization is truly a secure datacenter solution. A qualitative risk assessment method was chosen primarily due to the desire for a broad perspective of the risks associated with virtualization—a perspective built from the literature and research that had been done and not tied to any specific implementation or historical data. A view of the risks unique to virtualization was sought as a phenomenon in toto, from the general to the specific. In accordance to SP 800-30, risk-level matrix (Table 3) and risk scale tables (Table 4) were created and provide an initial starting point for the risk analysis.

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

TABLE 3

Risk Level Matrix

Threat Likelihood	Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	Low: 10 X 1.0 = 10	Medium: 50 X 1.0 = 50	High: 100 X 1.0 = 100
Medium (0.5)	Low: 10 X 0.5 = 5	Low: 50 X 0.5 = 25	Medium: 100 X 0.5 = 50
Low (0.1)	Low: 10 X 0.1 = 1	Low: 50 X 0.1 = 5	Low: 100 X 0.1 = 10

TABLE 4

Risk Scale

Risk Level	Risk Description
High	If a hardware virtualization risk is evaluated as a high risk, the risk may prohibit the implementation of virtualization if the likelihood is high, or if corrective measures are not available to eliminate or properly mitigate the risk.
Medium	If a hardware virtualization risk is evaluated as a medium risk, the risk may deter the implementation of virtualization if the likelihood is high, or if corrective measures are not available to eliminate or properly mitigate the risk.
Low	If a hardware virtualization risk is evaluated as a low risk, corrective measures are recommended in order to mitigate the risk

RISK VERSUS BENEFIT ANALYSIS

Now that the benefits and risks unique to hardware virtualization have been defined, and a framework established on which to build the risk analysis, we must now perform the qualitative risk analysis, and from those results determine if hardware virtualization provides a secure, cost-effective datacenter solution. With more than 80% of organizations with some sort of virtualization project underway, yet only 25% of server workloads expected to be virtualized by the end of 2010 (Caraher, 2010), many organizations are asking the same question, "Is virtualization a viable, safe solution?" (Plas, 2007).

The risk level table below illustrates our findings from the literature using the risk level matrix and risk scale tables. The values assigned for the likelihood and magnitude of impact of the vulnerabilities were determined from the research we performed and are found in Table 5.

TABLE 5

Virtual Environment Qualitative Risk Level Values

Vulnerability	Likelihood	Magnitude of Impact	Likelihood/Impact Score	Risk Level
VM Portability	Medium	High	50x1.0 = 50	50
Virtual Machine Based Rootkit (VMBR)	Low	High	100x0.1 = 10	10
Unhardened or Misconfigured System	Medium	Medium	50x0.5 = 25	25
VM Sprawl	High	Low	10x1.0 = 10	10
Virtual Communication Channels	High	Low	10x1.0 = 10	10
Natural or Manmade Disaster	Low	High	100x0.1 = 10	10

Though Table 5 gives us a very basic idea of the likelihood and magnitude of impact for the vulnerabilities, it does not account for their mitigation. Without such information a true comparison of the benefits and risks is not possible. A mitigated risk scale is needed in order to evaluate the numeric values of each risk after mitigation controls are applied. Once we have the qualitative risk value for each of the vulnerabilities, we will assign values to each mitigation control and apply them to the numeric values for each risk. This is important for evaluating if the risk associated with virtualization warrants the benefits it has to offer. Table 6 associates the mitigated risk values with a meaningful explanation that will ultimately be used to determine if the risk outweighs the benefit.

TABLE 6

Mitigated Risk Scale

Mitigated Risk Value	Mitigated Risk Description
Very High 15.01 and above	If a virtualization mitigated risk is evaluated as 15.01 or higher, almost no correlating organizational benefit will outweigh the amount of risk associated with the implementation of this element. Extreme care must be taken in implementing this element to minimize exposure to the risk.
High 10.01 – 15.00	If a virtualization mitigated risk is evaluated as 10.01 – 15.00, the correlating organizational benefit must be very strong. Extreme care must be taken in implementing this element to ensure the proper mitigation steps have been performed.
Medium 5.01 – 10.00	If a virtualization mitigated risk is evaluated as 5.01 – 10.00, the correlating organizational benefit must be relatively strong. Moderate care must be taken in implementing this element to ensure the proper mitigation steps have been performed.
Low 0 – 5.00	If a virtualization mitigated risk is evaluated as 0 – 5.00, the correlating organizational benefit can be of moderate value.

Now we must determine the mitigated risk value for each of the vulnerabilities we've identified. We will be able to use these values to determine the significance of the vulnerability as it relates to the benefits the organization will receive from implementing virtualization. The table below takes the vulnerability and its associated risk level, and then describes the mitigation controls for each to determine the mitigated risk level. Each mitigation step is assigned a numeric value ranging from 0 to 1. Numeric assignments closer to 0 provide a greater amount of mitigation, while those closer to 1 do an inferior job of mitigating the vulnerability. Vulnerabilities with more than one mitigation control have the mitigation value of each control applied to the risk level value to determine the final mitigated risk value as shown in Table 7.

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

TABLE 7

Virtual Environment Mitigated Risk Level Values

Vulnerability	Risk Level Value	Mitigation Controls	Mitigation Score	Mitigated Risk Value
VM Portability	25	✓ Physical security of storage area where VMs are kept (.8) ✓ Strict access controls applied to encapsulated VMs so that only authorized users have access (.4) ✓ Network perimeter controls applied to limit minimize external access to VMs (.9) ✓ Policies and procedures in place to minimize the likelihood of VMs being copied to unauthorized target (.7)	.8x.4x.9x.7x50 = 10.08	10.08
Virtual Machine Based Rootkit (VMBR)	10	✓ Ensure systems are kept up-to-date with the latest patches, anti-virus definitions, etc. (.4) ✓ Install virtual-specific host based intrusion detection or prevention systems (.7) ✓ Development of ultra-thin hypervisors reduces the risk of VMBR (.9)	.4x.7x.9x10 = 1.40	2.52
Unhardened or Misconfigured System	25	✓ Ensure proper change control process is in place for system, changes, hardening, and monitoring (.4) ✓ Create systems from "golden" template that is configured according to organizational security standards (.7)	.4x.7x25 = 5.00	7.00
VM Sprawl	10	✓ Ensure proper change control process is in place for new system deployment (.4) ✓ Monitor environment to track new systems being created (.6)	.4x.6x10	2.40
Virtual Communication Channels	10	✓ Ensure proper change control process is in place for creation and management of virtual environment (.4) ✓ Utilize virtualized-specific security tools to monitor and manage virtual communication channels (.7)	.4x.7x10 = 2.80	2.80
Natural or Manmade Disaster	10	✓ Setup offsite disaster recovery site for fault tolerance (.3) ✓ Configure local resources in such a way to minimize power disruptions (.9)	.3x.9x10 = 2.70	2.70

We now have all the pieces in place so we can evaluate whether the benefits of implementing a hardware virtualization infrastructure are warranted given the unique risks associated with it. As mentioned earlier, the goal is to perform a holistic analysis that includes both virtualization risk management and virtualization's benefits as they relate to organizational needs. To do this, we must look at the mitigated risks of virtualization while also keeping in mind its benefits. Hence, we are not only evaluating the security aspects of hardware virtualization, but also the impact the benefits of virtualization will have on an organization's business objectives and the fulfillment of its mission. The table below summarizes the findings by pulling together the results of the information we have gathered thus far. Most of the vulnerabilities can be directly associated to a benefit by connecting the two via the virtualization technology they have in common. For example, the vulnerability of VM Portability can be correlated to the benefit Recovery Time because both use the underlying technology of Encapsulation. It should be noted, however, that not all vulnerabilities correlate directly to a benefit. These are noted in Table 8 and evaluated on their own individual merit.

TABLE 8

Hardware Virtualization Risk versus Benefit Analysis

Vulnerability	Benefit	Mitigated Risk Value	Determination
VM Portability	Recovery Time	High 10.08	VM Portability has a high mitigated risk value; however the benefit of recovery time, especially during disaster recovery planning and in calculating the RTOs and RPOs for critical systems, is an enormous benefit. Extraordinary care must be taken during the testing, development, and implementation of the virtual infrastructure to ensure the risks associated with VM portability are addressed using physical security and access control; however the benefit will outweigh the risk for most organizations.
Virtual Machine Based Rootkit (VMBR) & VM Escape	Null	Low 2.52	There is no clear benefit associated with VMBRs, so an organization would have to be willing to accept this risk as part of their hardware virtualization implementation, and ensure the appropriate security controls are built into it. Properly patching, configuring and using standard best practices, like disabling unnecessary hardware and services, goes a long way in reducing the risk of VMBR and VM Escape. Because the mitigated risk level is low, and other benefits very high, this is a risk most organizations would be willing to accept.

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

Vulnerability	Benefit	Mitigated Risk Value	Determination
Unhardened or Misconfigured System	Administrative Overhead	Medium 7.00	Bill Hau notes that the virtualization risks are not solely comprised of technical problems. Like any information technology, it requires people to be trained and processes put in place to ensure system security is developed properly and maintained (Hau, 2007). Though technology of virtualization might require unique procedures for hardening and configuring the virtual environment, the methods for doing so are no different than any other technology. The fiscal savings from being able to centrally manage, monitor, and audit multiple VMs adds further value.
VM Sprawl	System Provisioning	Low 2.40	Again, this is more of a "people and processes" (Hau, 2007) issue than a technical risk. Ironically, one of the major strengths of virtualization, i.e., the ability to provision a system in a matter of minutes, has the potential for becoming a major vulnerability if not managed properly. Security must be built into the virtual infrastructure from the beginning, and a major part of that is having the proper procedures and change controls in place to maintain a secure environment. Add to that the benefit of using a golden template that is hardened and configured to an organization's standards as the base image for all VM deployments and the benefits far outweigh the risks.
Virtual Communication Channels	Security Auditing and Inspection	Low 2.80	Introspection and interposition are two of the more powerful features of the hypervisor; however this technology opens a whole new attack vector that can be exploited by the bad guys. Nonetheless, the likelihood of such an exploit on a properly hardened and patched system is relatively low. And the benefit of being able to use the hypervisor to audit and inspect VMs from outside the guest OS using virtual communication channels provides security professionals new ways for monitoring VMs and dealing with compromised systems.

Vulnerability	Benefit	Mitigated Risk Value	Determination
Natural or Manmade Disaster	Recovery Time	Low 2.70	As mentioned in *VM Portability* in this table, the benefit of recovery time, especially during disaster recovery planning and in calculating the RTOs and RPOs for critical systems, is an enormous benefit. The dreaded financial costs of hot sites and cold sites are greatly reduced because so much less hardware needs to be purchased. Multiple VMs can share a single piece of hardware, thus drastically reducing the fiscal cost of buying and maintaining one-to-one physical servers and the offsite rental space to house those servers. This is one of the primary benefits that organizations seek when first evaluating hardware virtualization.
Null	Hardware Overhead	Null	There is no vulnerability for needing less hardware in a datacenter. In fact, just the opposite. From a security perspective, less hardware means less firmware that can be compromised, less downtime due to hardware failure, and perhaps even fewer physical security requirements, such as physically secured server and network racks. From a fiscal perspective, less hardware means big monetary savings. This is another benefit which CIO's and CFO's happily embrace.
Null	Security Forensics	Null	Giving a forensics investigator the ability to replay system attacks is a huge advantage when trying to determine how a system was compromised. Likewise, being able to roll back a compromised system to a previous, uninfected state via a snapshot greatly reduces the recovery time for a compromised system. Rather than having to rebuild the system using a backup or some other method, an uncompromised system can be restored in a matter of minutes rather than hours or even days. There is no vulnerability associated with this benefit.
Null	Power Consumption	Null	Another benefit CIOs and CFOs gladly embrace is the fiscal savings brought about by having to provide power to fewer systems. The difference between having to power 20 physical servers versus one virtual host with 20 VMs adds up quicker than one might expect. Joe Vanden Plas estimates the savings could be as much as $3,000 per processor (Plas, 2007). Big savings indeed.

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551

CONCLUSION

The risk versus benefit analysis demonstrations that virtualization can provide a secure, highly beneficial technology on which datacenters can be built. Though it does possess unique risks in addition to exacerbating traditional risks, the likelihood of those vulnerabilities being exploited is greatly reduced through appropriate mitigation. Special care and a thorough understanding of the technology and security best practices are required for the proper implementation of a virtual infrastructure. Like any project, organizations must bake security into the testing, development, and implementation of their virtualization plans rather than attempting to secure the environment after the fact. Including security in the initial project development, through its implementation, and making it a key element of ongoing maintenance, is an integral component of successfully securing any system (Conklin & White, 2010), and virtualization is no exception.

Perhaps the most daunting aspect of securing a virtual infrastructure is the complexity of the system. Virtualization adds layers of technology to a datacenter (Scafone, Souppaya, & Hoffman, 2010). Not only must you secure the server OS, but also the host OS, hypervisor, virtual network, virtual hardware, virtual management system, on down the line, while also securing the virtual communication channels on which all these components communicate. Of course, the perplexing terminology of virtualization, with different companies and researchers referring to the same technology with different names, doesn't help. Nonetheless, a thorough understanding of the technology behind virtualization, knowing the ingredients that make the special sauce perform its magic, is crucial to being able to properly secure a virtual infrastructure.

Most surprising is the paradoxical nature of virtualization (Price, 2008). Many of the technologies that make it unique are both the source of security risks and the foundation for its unique benefits. As Jenni Susan Reuben (2007) puts it, "virtualization is both an opportunity and a threat." The technology of virtualization is truly a double-edged sword that cuts both ways, for better and for worse. This is yet another reason why it's so important to have a firm understanding of the technology, and to incorporate security and security processes into the planning stages. What may at first appear to be a great fiscal and administrative godsend might quickly spiral into a security nightmare without proper hardening, mitigation, policies, and procedures.

Virtualization will likely be seen as a paradigm shift for the way datacenter architectures are configured and managed. Better utilization of hardware, lower maintenance and renewal costs, increased availability and portability, and a smaller carbon footprint are just a few of the benefits of virtualization. It is the cornerstone of cloud computing's Infrastructure as a Service (IaaS) (Scafone, Souppaya, & Hoffman, 2010), and provides the foundation from which Platform as a Service (Paas) and Software as a Service (SaaS) is built. Green IT, once considered desirable, is now considered essential by most organizations (Symantec, 2009), and virtualization provides the bedrock on which a greener IT is built. It has given disaster recovery, once the bane of CFOs around the world due to its costly nature and its seemingly improbable purpose, a much needed face lift. Overworked in a down economy, system administrators, with technologies like snapshots, hot migrations, storage migrations, and VM templates, respond to requests for new servers and system patching with a smile and a wink instead of a grunt and moan. The social relevance of hardware virtualization, though perhaps not fully understood at this point in its development, is undoubtedly a technical force to be reckoned with. As Bill Hau states, virtualization "may very well be one of those revolutionary paradigms that could fundamentally change the way we think about and approach computing." (Hau, 2007). Paradigm or not, virtualization is having a profound impact and is likely here to stay. It is our duty as security professionals to ensure that it is secure.

REFERENCES

Caraher, K. (2010). CDW's Server Virtualization Life Cycle Report, January 2010. *CDW News Room.* Retrieved from http://webobjects.cdw.com/webobjects/media/pdf/Newsroom/CDW-Server-Virtualization-Life-Cycle-Report.pdf

Chen, P., & Noble, B. (2001). When Virtual is Better Than Real. *University of Michigan. IEEE CS Press.*

Conklin, W. A. & White, G. (2010). *Principles of Computer Security*. New York, NY: McGraw Hill.

Gartner, Inc. (2009). Gartner Says 16 Percent of Workloads are Running in Virtual Machines Today. *Gartner News Room*. Retrieved from http://www.gartner.com/it/page.jsp?id=1211813

Gartner, Inc. (2010). Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012. *Gartner News Room.* Retrieved from http://www.gartner.com/it/page.jsp?id=1322414

Gartner, Inc. (2010). Gartner Says Virtualization to Be Highest-Impact Issue Challenging Infrastructure and Operations Through 2015. *Gartner News Room.* Retrieved from http://www.gartner.com/it/page.jsp?id=1440213

Harris, S. (2008). *All-In-One CISSP Exam Guide*. New York, NY: McGraw-Hill.

Hau, B. (2007). Virtualization and Risk: Key Security Considerations for Your Enterprise Architecture. *McAfee, Inc.* Retrieved from http://www.vmware.com/files/pdf/partners/security/mcafee-key-security-ent-arch-wp.pdf

IDC (2010). Virtualization Market Accelerates Out of the Recession as Users Adopt "Virtualize First" Mentality,

According to IDC. *IDC - Press Release.* Retrieved from http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22316610&sectionId=null&elementId=null&pageType=SYNOPSIS

Kearns, B. (2004). Technology and Change Management. *School of Computing, Dublin Institute of Technology.* Retrieved from http://www.comp.dit.ie/rfitzpatrick/MSc_Publications/2004_Brenda_Kearns.pdf

King, S., Chen, P., Verbowski, C., Wang, H., & Lorch, J. (2006). Subvirt: Implementing Malware with Virtual Machines. University of Michigan. Retreived from http://vxheavens.com/lib/vsk00.html

Koomey, J., Belady, C., Patterson, M., Santos, A., & Lange, K. (2009). Assessing Trends Over Time in Performance, Costs, and Energy Use for Servers. *Final report to Microsoft Corporation and Intel Corporation v25.* Retrieved from http://www3.intel.com/assets/pdf/general/servertrendsreleasecomplete-v25.pdf

Perez, R., van Doorn L., & Sailer R. (2008). Virtualization and Hardware-Based Security. *IEEE Security and Privacy*, Volume 6 Issue 5

Plas, J. (2007). Pitching Virtualization: Benefits Go Far Beyond Cost Cutting. *WTN Media, LLC.* Retrieved from http://wistechnology.com/articles/4226/

Price, M. (2008). The Paradox of Security in Virtual Environments. *Computer*, Vol. 41, No. 11, pp. 22-28

Reuben, J. (2007). *A Survey of Virtual Machine Security.* TKK T-110.5290 Seminar on Network Security. Retrieved from http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf

Scafone, K., Souppaya, M., & Hoffman, P (2010). *NIST Special Publication 800-125 (Draft): Guide to Security for Full Virtualization Technologies (Draft).* National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/drafts/800-125/Draft-SP800-125.pdf

SolarVPS, (2010). How Virtuozzo Cotainiers Work? *OS Virtualization content © 1999-2010 Parallels.* Retrieved from http://www.solarvps.com/linux-vps.php#about-tab

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Special Publication 800-30: Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Symantec Corp. (2009). Green IT Report Regional Data – United States and Canada. *Symantec Enterprise.* Retrieved from http://www.symantec.com/content/en/us/about/media/GreenIT09_Report.pdf

VM Tech (2010). History of Virtualization. Retrieved from http://www.vmtech.com.au/virtualization/history.html

---

Brian Boyer received an MLS degree from Fort Hays State University with an emphasis in Information Assurance. He can be reached at briankboyer@gmail.com.

Keyu Jiang, Ph.D. in Computer Science, Arizona State University, 2001, is currently an Associate Professor at Fort Hays State University where he leads the Information Assurance program. He is also a lead Research Fellow in the Informatics Department. Jiang has published widely the Journal of Software, Journal of Computing Sciences in Colleges, Journal of Business and Leadership, Academic Perspective, and the Proceedings of the Colloquium on Information Systems Security Education. His research interests include information assurance, distributed system computing, Leadership and organizational management. He has received research funding from the National Science Foundation, Department of Defense and National Security Agency.

Robert Meier is a Professor of Informatics at Fort Hays State University. He received his Ph.D. in Statistics from Kansas State University. His current research interests include pedagogy and instruction in business subjects, including information technology. He has published in International Journal of Education Research, Journal of Computer Information Systems, Journal of Business and Leadership: Research, Practice, and Teaching, and the Southwestern Business Administration Journal.

Hongbiao Zeng graduated from Wichita State University in December 2001 with Ph.D in Applied Mathematics. He is an associate professor in the Department of Mathematics & Computer Science at Fort Hays State University.

https://scholars.fhsu.edu/jbl/vol7/iss1/4
DOI: 10.58809/VWWY8551