# Building a Defensible Virtual Environment

**Shaun Walmsley**
Department of Computer Science
Sam Houston State University
Huntsville, Texas, USA 77341

**Lei Chen**
Department of Computer Science
Sam Houston State University
Huntsville, Texas, USA 77341

***Abstract* — As the scope and utilization of virtual technology continues to grow, so does the importance of securing that technology. Virtual technology is now relied upon to support production level environments, and with that increased reliance on virtual technology comes an ever increasing need to ensure that these virtual environments are built and maintained with security as a primary concern. Companies can no longer afford to treat virtual environment security as an afterthought. Virtual environments present several security concerns which are unique to their specific nature. It is imperative that companies and administrators understand these concerns and implement proper measures to deal with these unique issues accordingly. Additionally, virtual environments often have the same security concerns as regular hardware environments, but the unique nature of the virtual environment requires that these well known security concerns be addressed in new ways. The intent of this paper is to identify the various areas of security which are of concern in virtual environments and to provide recommendations on how best to address these concerns.**

**Keywords**: hypervisors, security, virtual environment, Virtual Management System, virtualization, VMWare

## I. INTRODUCTION

### *A. Background*

Computer virtualization is a hot topic in the technological industry. With companies striving to reduce costs and increase efficiency and agility, the adaptation of virtualization is no surprise. Virtualization has many applications, some of which include hardware consolidation, resource distribution, application or system sandboxing, and increased supportability and flexibility. Although virtualization is not a new concept, it is only within the past few years that it has really seen widespread acceptance and utilization.

A survey conducted by Zenoss in 2010 shows that nearly 95% of participant's organizations make use of virtualization in their environments, with over 40% stating that virtualization is their preferred server deployment method. It is important to note that virtualization is no longer a "lab only" or "development environment only" technology. 70% of participants state that their organization uses virtualization in production environments. [1]

With virtualization receiving such widespread use, we cannot afford to ignore the security of virtual environments. It is imperative that the virtual infrastructure be protected and secured with the same rigor that is used to protect traditional hardware systems. In addition to the more traditional security considerations such as policy enforcement, access control, auditing capabilities, traffic monitoring, intrusion detection systems, firewalls, and anti-virus/anti-malware systems, virtualization presents new and unique security challenges that are difficult to address without specialized tools designed for virtual environment security.

Among the chief concerns that administrators of virtual environments face are visibility into the virtualized devices, communication throughout the environment, data segregation, access restrictions, accountability, and integrity. Due to the dynamic nature of virtual environments, all of these considerations must be addressed in a manner which allows persistent and reliable enforcement of security policies. There is a growing market for tools which address these security concerns, and while it is still a relatively new field of development, there are many reliable tools which help to achieve the goals of information security.

While there will be mention of specific software vendors and products, the goal of this paper is not to evaluate the effectiveness of those products; but rather to evaluate their functionality as a means of identifying the different aspects of securing a virtual environment. This paper will provide information which will help identify areas of concern, as well as provide recommendations on how to build a defensible virtual environment.

### *B. Relevance of Information*

There exists a wealth of information regarding virtual environment security. Unfortunately, there also exists a vast amount of misleading information on this same subject. Often times the information is misleading simply because it is outdated, and thus easily misinterpreted when evaluated in a current day context. Other times, the information may be misleading as a result of the perspective of the author.

As with most emerging technologies, many vendors create products to address new and specific concerns with regards to that technology. These vendors conduct research and provide statistical information supporting the need for their product. While this information is typically correct and accurate when provided by a reputable vendor, it is nevertheless presented with some bias. As a result, the concern which is addressed by the advertised product may be over-stated or over-generalized to make the product more desirable to a larger consumer base.

With the abundance of outdated and/or biased information, it can be difficult to obtain a consolidated understanding of relevant and applicable security concerns

for today's virtual infrastructure. It is nearly impossible to properly implement security measures for a new technology without first gaining an understanding of the security risks. And while understanding the risks is important, it is equally as important to understand how to address those risks.

In spite of – or perhaps because of – the overabundance of information available on the topic of virtual security, it can be extremely difficult to find relevant and thorough information which addresses the security of a virtual environment as a whole. Often times the problem will be described in great detail, but no vendor-independent solution will be provided. Other times, a solution will be implied but little consideration will be given to understanding the root problem. Even when a problem and solution are presented in an appropriate manner, it often only addresses one specific aspect of virtual security. It can become a frustrating matter to research and understand the various aspects of virtual environment security.

This paper will identify the primary security concerns of a virtual environment without bias and with respect to relevancy, taking into consideration the fact that the technology and implementation of virtual environments has evolved since its initial resurgence and that it will continue to do so as the technology changes and grows. The security concerns addressed will be presented in a cause and effect manner so that the reason behind and need for the various security recommendations can be understood.

## II. WHAT IS VIRTUALIZATION?

Virtualization is not a new concept. Virtualization was initially developed in the late 1950s and early 1960s, but was deemed obsolete through most of the following two decades due to a lack of flexibility and an inability to adapt to the computing demands of the time. Virtualization as we know it today didn't reemerge as a driving technological force until the mid-1990s [10]. Since then, the application and varied use of virtual technology has continued to grow at a rapid pace.

Fundamentally, virtualization is the separation of a request from the underlying physical delivery of that request [9]. Typically, this refers to the separation of a request or instruction sent by an operating system from the underlying physical hardware of the computer. Virtualization has many implications, and although the virtualization of an entire operating system may be the most common, virtualization can also be applied to the processing of a single program or application. Another common use is the virtualization of resources such as storage, CPU, or network resources.

Virtualization functions by placing an abstraction layer between two points of communication [5]. This virtualization layer may reside between the hardware and the OS, as with Operating System and Resource virtualization, or it can be between an application and the OS, as seen with application virtualization. This abstraction layer is responsible for controlling communication between those two points. Since the abstraction layer, rather than the requesting process, has control over the resource, the abstraction layer can partition use of that resource as desired; effectively hiding the raw resource from the requesting process.

### *A. System Virtualization*

System virtualization is one of the more well known types of virtualization in use today. It provides a complete system platform which is capable of executing a full Operating System independent of the underlying hardware. The two primary methods of implementing this type of virtualization can be referred to as Hosted and Native [9]. One of the more well known hosted environment products is VMWare Player. ESX Server is an example of a Native, or Hypervisor, environment.

Hosted System virtualization implements the virtualization layer as an application. This application is installed and runs on top of a Host Operating System. The virtualization application then serves as the abstraction layer between the physical hardware and the Guest Operating Systems which it hosts. Hosted System virtualization allows for a wide range of hardware virtualization, effectively showing the guest systems whatever hardware configuration is desired rather than the true underlying hardware.

Hypervisor system virtualization implements the abstraction layer closer to the actual hardware. The hypervisor runs directly on the physical hardware, and in effect serves as the operating system. The hypervisor then controls communication between its guest operating systems and the underlying hardware.

### *B. Virtualization Techniques*

Regardless of the architecture used, several methods of virtualization have been developed to address the issue of properly trapping and translating communication between the operating system and the underlying hardware.

Full Virtualization is a method in which the guest operating systems are completely decoupled from the hardware [9]. No modification of the guest OS is required. VMWare offers a Full Virtualization implementation.

Paravirtualization is a method in which the guest operating system is modified slightly to allow it to be virtualized. Xen offers virtualization solutions which utilize paravirtualization.

Hardware assisted virtualization is relatively new technology in which the physical hardware is designed to support virtualization, bypassing the need for the trap and translation methods utilized in Full and Para virtualization. Intel and AMD released the first generation of hardware assist features in 2006 [9].

### *C. Other Types of Virtualization*

In addition to System Virtualization, other widely used implementations of virtualization include Application Virtualization and Resource Virtualization.

Application Virtualization functions by implementing an abstraction layer between the application and the underlying operating system. This allows greater control over what the application can access, providing benefits to both efficiency and security.

Resource Virtualization is used to manage resources such as CPU, Storage, and Network bandwidth. It can be used to aggregate resources, making several small hard drives appear as one large drive, or allowing several CPUs to function as one supercomputer. It can also be used to isolate, partitioning a large drive into smaller segments for individual use.

## III. Virtual Environment Security

### A. Current State of Virtual Environment Security

While virtualization may have been around for quite some time, the security of virtualization is a relatively new field of technology.

Due to the fact that virtual security is relatively young, it has become a prime target for attacks. Attackers know that the security aspects of virtual environments may be underdeveloped and that organizations and administrators deploying those virtual environments may be inexperienced. As a result, virtual environments become a very attractive target. The fact that a virtual environment provides a single point of entry and/or a single point of failure only adds to that attractiveness.

Virtual management systems have experienced several security issues including flaws in the fundamental architecture as well as flaws in software design [10]. While patches have been released to address these problems, it stresses the importance of maintaining the devices and software responsible for hosting and controlling the virtual environment.

Aside from architecture and design flaws, there are security concerns that present themselves as a result of the way that a virtual environment functions. Virtual environments communicate in a manner which may not be detectable through traditional traffic monitoring means. Virtual devices may also interact in ways that are vastly different from traditional hardware devices [2]. These are not security concerns resulting from flaws or bugs, but rather they are security concerns resulting from the very nature of the designed intent of how virtual environments work. An understanding of virtual technology is required to ensure that these security concerns are properly addressed. In some cases, the built-in functionality of the virtual environment is insufficient to achieve the security goals of an organization, and so new technology is required.

Virtual environments also introduce an entirely new group of security concerns related to deployment and design. Without proper restrictions and procedures in place, improper use of a virtual environment can present numerous issues such as improperly patched or improperly maintained systems, unintended denial of service, breach of confidentiality, lack of integrity, and lack of verifiable authenticity. It is important that proper policies and procedures be established and maintained to ensure that these types of security concerns are addressed.

Since virtual environments present a desirable target for attackers, and because virtual environments introduce a wide variety of new and unique security concerns, it has become increasingly important that administrators develop a solid understanding of these concerns. It follows that it is also important that virtual environments be designed and deployed with these unique characteristics in mind.

### B. Visibility and Transparency

The dynamic nature of virtualization can make it difficult to keep track of devices in the environment. Virtual guests can quickly be moved, copied, created, or removed. As with most aspects of security, it is important to identify the assets that need to be managed and secured. For this reason, it is important to implement a process for establishing and maintaining a map of the virtual environment.

At a minimum this map should include details about the host machines such as physical location and hardware capabilities, as well as which guests are hosted on each machine. Depending on the environment other details may be necessary such as network zones, applications running on each machine, and resources allocated to each guest. In small environments, a map with these details can be maintained manually using a Visio diagram or something similar. Larger environments may find the use of more automated discovery and mapping tools beneficial. Products such as VMWare vMotion are designed specifically for this purpose. Other “virtual suite” products such as Reflex Virtual Management Center often include discovery and mapping tools which also provide status information for the virtual environment.

Status information is another key element in maintaining the overall stability (and thus, the security) of an environment. If availability is a concern, it can be very helpful to have a tool which monitors the status (online, offline, suspended, etc.) as well as the resource utilization (CPU, Memory, Network) of devices. Small environments can make use of the built-in monitoring and trending features of most virtual management products, while larger environments can make use of automated tools such as VMSafe. This data can be used to redistribute load and resources to maximize efficiency and ensure consistent availability.

Another important aspect of device mapping is software inventory. When looking at the “big picture” overview, it may be easy to forget that some of these devices represent fully functional operating systems; complete with security holes and bugs. Maintaining a list of installed and running software complete with version and patch level information will go a long way in helping to secure a virtual environment. In some environments it may be appropriate to leverage normal software and patch management capabilities to keep the virtual devices up to date. Others may benefit from software inventory tools which integrate with the virtual environment and keep track of the pertinent information.

### C. Policy Configuration and Management

The security policy of the virtual environment is a key aspect of security. It is responsible for enforcing aspects of security including user privilege, network access, and change management. User privilege management can be as basic as defining who is allowed to access the virtual management environment, or it can be more granular to the level of defining who is allowed to take specific actions on a specific host or guest. Since most virtual host tools allow full access to its guest systems by default, it becomes increasingly important to restrict access in sensitive environments. Actions such as setting up new virtual guests, starting/stopping/suspending guests, and cloning/copying guests should be restricted to only those specific users which require those privileges.

Network policy configuration ensures that each virtual guest is appropriately segmented and isolated. There are various methods that can be used to achieve this goal – some of which will be discussed in the next section – but whatever the method, it is important that a policy management system is in place to enforce the policy and uphold the segmentation.

Change management ensures that only authorized users can perform changes, and it also ensures that only authorized changes can be performed. If any machine can be cloned at any time, this compromises authenticity since that machine is no longer unique, and it becomes difficult for a user to validate that they are interacting with the system that they think they are interacting with. On a similar note, if any machine can be rolled back or restored to a previous state, integrity may be compromised. It becomes difficult to rely on the integrity of that system when the state can be so easily altered. The dynamic nature of virtual environments makes change management a critical security measure to maintain integrity and authenticity.

Another aspect of change management is patch management. A patch management policy can be useful for standardizing and automating patch management within a virtual environment. A solid patch management policy can increase the efficiency of delivering security patches and help to ensure full and expedient coverage.

It is important to note that policy enforcement must take place at the hypervisor level to be effective. This ensures that virtual devices are covered under policy regardless of the state of the device.

Scalability is a must when it comes to security policy management. Because virtual environments are so dynamic, it is of key importance that the security policy be both persistent and scalable. Scalability ensures that the policy can grow along with the environment, creating new policy groups as necessary and allocating resources appropriately. A persistent policy is one that actively applies itself to any new systems that come online. This ensures that there is no chance of an admin forgetting or neglecting to set up the security policy when standing up a new virtual system. It also ensures that the policy remains enforced on the system regardless of the state of the system.

### D. Traffic Analysis

Arguably one of the largest security gaps in a standard configuration virtual environment is the inability to analyze "intra-VM" communication; that is, communication between the host and the guests as well as communications between guests. When thinking in terms of a single host, this may seem somewhat irrelevant; however, this security issue expands exponentially when it comes to a clustered environment using virtual switching which supports hundreds of hosts and thousands of virtual devices.

Traditional network monitoring tools are designed to provide visibility and alerting capabilities on network traffic traveling through an environment. On a virtual host (or virtual switch) that traffic never actually makes it to the physical network. Instead, that traffic is all handled internally, effectively making it invisible to traditional tools monitoring traffic across physical wires.

Fortunately, several solutions are available. One solution which may be useful is to utilize port groups and the built-in functionality to allow those port groups to run in promiscuous mode. An IDS device would be connected to the promiscuous port group while other virtual guests are connected to other port groups. This allows the IDS device to monitor intra-VM traffic while preventing guest system from monitoring other guest's traffic. While this may be a feasible solution for a small environment, larger environments may require a more robust solution.

Several vendors now offer infrastructure-level monitoring products. These products integrate at the hypervisor level which allows accurate and efficient monitoring of all traffic in the virtual environment. Most products are agentless – that is, there is no requirement to install an agent on each virtual device – which allows them to run with little impact to the virtual environment. Regardless of which approach administrators choose to implement, it is important that some form of intra-VM traffic monitoring is established to ensure that network security policies are properly enforced.

### E. Reporting and Auditing

As with traditional security systems, auditing and reporting capabilities must be integrated with the security policy. Important events such as altering the state of a virtual guest, access requests to sensitive data, and specific network activity should be recorded to provide an audit trail. Such an audit trail may be useful in the event of a security incident, or even an outage due to misconfiguration. It is often helpful to be able to retrace the activities leading up to an event to better understand the what/how/who/when of an occurrence. Potentially high impact events should be reported on as well as recorded. Reporting typically involves some form of automated messaging, most likely via e-mail, page, or text messaging.

Most tools which provide a security feature also come with built in auditing and reporting capabilities. However, it is up to the administrators of the system to correctly configure those capabilities. It is important to restrict your auditing and reporting to only those events which are of value, as over-recording can make it difficult to extrapolate

any useful data. It can also leave your system susceptible to log flooding which is a security risk in itself.

Some additional common events which may be helpful to audit/report on are: high volume authentication attempts, unexpected shutdown, unauthorized deletion, unauthorized rollback, abnormally high resource use, access requests to sensitive data, unexpected inbound or outbound traffic, detection of potentially unwanted software, deviations from expected configurations and changes to policy settings.

## IV. Conclusion – Summary of Recommendations

The security needs of each environment are distinct and unique. However, there are many basic principles which are useful to follow in almost all scenarios.

Visibility into the virtual environment is a basic security need. It is easy to neglect or forget about little used devices, particularly in a virtual environment. As such, having a well maintained map of the virtual environment with as much detail as is feasible lays a solid foundation for securing an environment. A Microsoft Visio map can be used for smaller environments, while administrators of larger environments may wish to use an automated discovery and mapping tool such as VMWare vMotion.

Along with visibility goes transparency. Transparency provides insight into key details of the devices in a virtual environment such as status, resource usage and installed software. VMSafe is a great example of a tool which provides granular detail. Greater transparency allows for easier patch management. Patch management should be automated as much as possible to ensure that devices have the latest supported security patches. In addition to the traditional enterprise patch solutions such as WSUS or SCCM, the virtual world brings a new flavor of patch management which allows the host to maintain patching of virtual guests. VMWare vCenter Update Manager is one example of a virtual patch management application.

Access controls should be designed to restrict access to potentially harmful actions such as turning off, deleting, cloning, creating or reverting a virtual guest. Access to guests from a host should also be restricted on a per-user or per-zone basis, depending on the design of the environment. Change management should be enforced through access controls to ensure that only authorized users can make changes, and that only authorized changes can be made. This helps to ensure both the authenticity and identify of virtual devices. Most virtual management products have built in access control features which work well when configured properly.

Because intra-VM communication is handled by the host internally via virtual switching, the need to monitor communication between virtual guests is a concern unique to virtual environments. Perhaps the most straightforward solution is to implement a product which is specifically designed to monitor this type of communication. Products such as Catbird vSecurity and Trend Micro Deep Security provide network monitoring capabilities.

All aspects of the security policy must be scalable and persistent. As virtual devices are created, moved, reverted to old snapshots, and cloned, the security policy must continue to apply to those devices. Key events related to the security policy should also be recorded and, in some cases, reported. This includes access control events, change control events, status change events, network events, and events relating to software inventory or system configuration. Virtual security suite products such as Reflex Virtual Management Center provide scalable and persistent policy enforcement along with auditing and reporting capabilities. Reflex's product integrates policy enforcement at the hypervisor level, ensuring that devices are protected and monitored, even when in an inactive state.

With all of the advantages that virtual environments provide, it is no surprise that they are being implemented in an ever expanding capacity. As users and companies move to virtualize more critical aspects of their infrastructure, it is imperative that securing these virtual environments is more than an afterthought. The recommendations outlined here will go a long way in setting the foundation for security in a virtual environment. However, each environment is unique and thus has unique needs. There are numerous tools and resources available to help achieve security goals. It is important that administrators and security professionals leverage those resources to better understand the risks associated with virtualization and utilize that knowledge to plan and deploy defensible virtual environments.

## References


[1] Zenoss Inc. (2010). 2010 Virtualization and Cloud Computing Survey [Online]. http://mediasrc.zenoss.com/documents/wp_2010_virtualization_and_cloud_survey.pdf

[2] E. Ray, E. Schultz, "Virtualization Security," in 5th Annual Workshop on Cyber Security and Information Intelligence Research, Knoxville, TN, 2009, Article 42.

[3] S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, "TVDc: Managing Security in the Trusted Virtual Datacenter," ACM SIGOPS Operating System Review, vol. 42, no. 1, pp. 40-47, Jan, 2008.

[4] R. Perez, R. Sailer, L. Van Doorn, "Virtualization and Hardware-Based Security," IEEE Security and Privacy, pp. 24-32, Sept, 2008.

[5] J. Sahoo, S. Mohapatra, R. Lath, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues," in Second International Conference on Computer and Network Technology, Bangkok, Thailand, 2010, pp. 222-226.

[6] S. Campbell and M. Jeronimo, An Introduction to Virtualization, Hillsboro: Intel Press, 2006.

[7] C. Li, A. Raghunathan, N. Jha, "Secure Virtual Machine Execution under an Untrusted Management OS," in IEE 3rd International Conference on Cloud Computing, Miami, FL, 2010, pp. 172-179.

[8] A. van Cleeff, W. Pieters, R. Wieringa, "Security Implications of Virtualization: A Literature Study," in International Conference on Computational Science and Engineering, Vancouver, Canada, 2009, pp. 353-358.

[9] VMWare Inc, Understanding Full Virtualization, Paravirtualization, and Hardware Assist, Palo Alto: VMWare Inc., 2007.

[10] U. Gurav, R. shaikh, "Virtualization – A key feature of cloud computing," in ICWET 2010, Mumbai, India, 2010.