

Realtime
publishers

The Essentials Series:
Virtual Security Concerns & Solutions

Understanding & Improving Hypervisor Security

sponsored by



eEye Digital Security®

by Greg Shields

Understanding & Improving Hypervisor Security.....	1
What Is the Hypervisor?	1
Why Is Hypervisor Security Important?	2
The Security Implications of Hypervisors	3
Hypervisor-Based Attacks: An Example	3
Preventing Hypervisor-Based Attacks	4
Virtual Machine Eggs in Your Hypervisor Basket.....	5

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Understanding & Improving Hypervisor Security

A successful virtualization deployment delivers a host of compelling benefits to the IT organization—reduced costs from power and cooling, a right-sizing of resource demands to supply, and improved operational agility. But there’s a hidden risk that lurks in, around, and through virtualization environments that only the most observant are aware of today. That quiet killer is virtualization’s hypervisor itself.

What Is the Hypervisor?

Although not all virtualization solutions leverage a hypervisor, those most commonly used for the processing of production workloads typically leverage the use of one. Virtualization platforms today that make use of a hypervisor are VMware ESX and Virtual Infrastructure, Microsoft Hyper-V, and Citrix XenSource, among others. Within these virtualization architectures, the hypervisor is a thin layer of code that resides between the physical hardware and any virtual machines that are hosted on the virtual server itself.

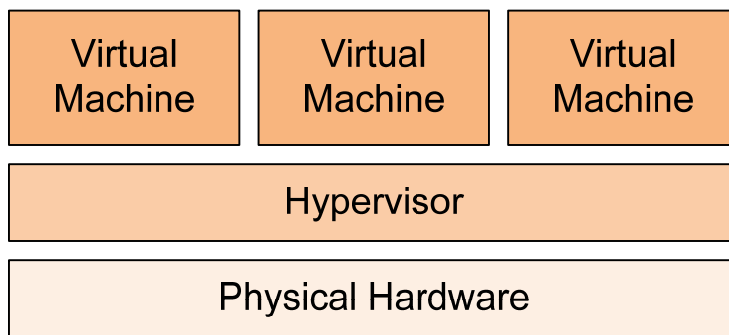


Figure 1: A hypervisor is used by many virtualization solutions; it is positioned between physical hardware and residing virtual machines.

Figure 1 shows a simplistic graphical representation of this layering. With virtualization solutions that make use of them, the job of the hypervisor is effectively to “proxy” requests by virtual machines to resources that are available on the physical hardware of the server.

Why Is Hypervisor Security Important?

Organizations that leverage virtualization do so because virtualization's hypervisors enable a level of commonality between virtual machines across all hypervisors of the same platform. When a virtual machine is created atop a virtualization solution's hypervisor, that virtual machine is functionally similar to other virtual machines in terms of its emulated hardware composition. This commonality allows virtual machines from one host to function when relocated to another. It also allows virtual machines collocated on a single host to share the physical resources of that host while maintaining hard boundaries between individual virtual machines.

Yet at the same time this introduction of a singular hypervisor across the IT environment adds a common codebase atop which resides all the virtualized computing resources of that IT environment. Should a security vulnerability in that common codebase be exploited through the use of malicious code, it would put each and every virtual machine at risk for failure. The pervasive nature of the hypervisor across all virtual hosts means that a single piece of malicious software that has the capability to compromise one hypervisor instance can easily compromise others.

Figure 2 illustrates how the introduction of this single instance of replicating malware can quickly exploit each hypervisor in the IT environment. The result of this replication is the potential for failure of all the virtual machines atop each hypervisor.

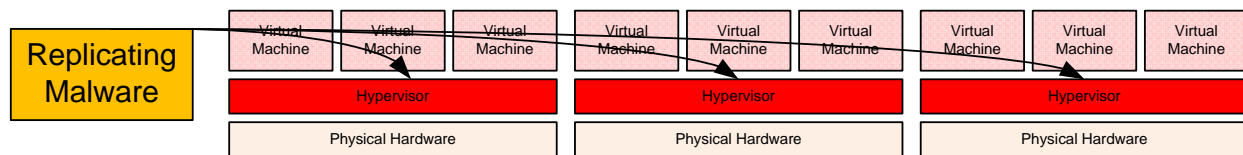


Figure 2: The hypervisor's pervasive nature within the virtualized environment makes it a single point of failure in the case of malicious compromise.


🔴 In short, the move to virtualization effectively puts an IT environment's virtual machine eggs in a single hypervisor basket.

The Security Implications of Hypervisors

Although hypervisor-based security exploits today remain mostly within the realm of academic research, their potential for massive environment failure makes them an important consideration for environments that have made the jump to virtualization. Hypervisors are by nature software-based code, which infers that they require occasional updating to patch security holes and protect against discovered vulnerabilities. Examples of this need have already been seen with hypervisors in production use today. For example, the security group Secunia has reported as of the time of this writing:

- 19 advisories and 128 vulnerabilities for VMware ESX Server 3.x
- 7 advisories and 14 vulnerabilities for XenSource Xen 3.x

As with traditional operating systems (OSs), most hypervisor-based vulnerabilities are constrained by a need for administrative rights in order to accomplish their mission. Without the proper administrative rights, the hypervisor remains off-limits to exploitive code. Yet the level of maturity associated with rights and privileges in virtualization environments may not be to the same level as those already in place for Windows. If IT environments do not properly lock down privileges and console access to virtual environments with the same level of care seen with directory services, this situation exacerbates the potential for successful code exploitation through malicious software.

 Essentially, IT environments must use the same level of due diligence with virtual environment security as with OS and directory services security. If security controls for the virtual environment are lax, there is a greater chance for infection.

Hypervisor-Based Attacks: An Example

The situation described up to this point is perhaps best illustrated through a real-world example. In this example, let us examine a typical healthcare environment that has recently completed a substantial migration of server resources to virtualization. This company has standardized on a single virtualization platform due to the associated cost savings as well as the benefits to systems management.

All hosts run the same version of the virtualization solution's software. However, due to the timing of the virtualization project, hosts were brought online over a period of months. Not planned for in this environment was the need to monitor the versions of the hypervisor code itself. Although all hosts run the same *version* of the virtualization software, hosts that were installed later in the project quietly run a later *build* of the version. The changes associated with the newer build versions were incorporated to protect against a known network-based vulnerability.

As with many healthcare organizations, the example network here operates with a centralized data center but a federated operating model. Multiple offices and hospitals share the use of the network and services on that network. Due to this federated model, security controls are not cohesively applied in all areas. At some point during its operation, an instance of replicating malicious software was introduced into the environment which infected earlier builds of the virtualization software. The end result was a loss of virtual machines atop those hosts that were not properly secured.

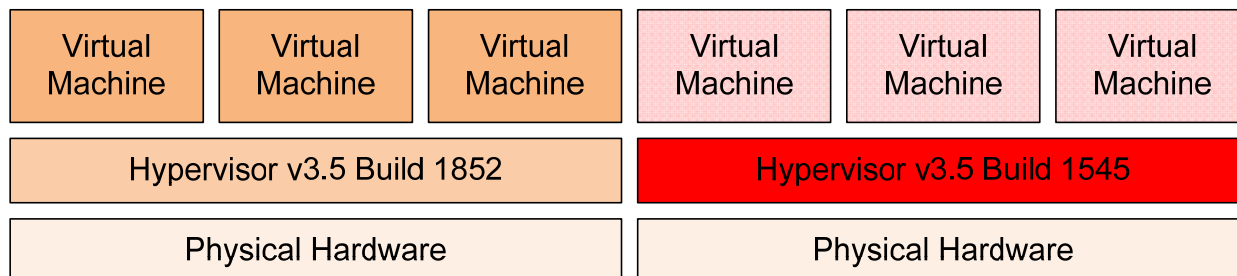


Figure 3: Patch levels are critical even with hypervisors. On the left is an up-to-date hypervisor that survives the attack, while on the right is one that does not because it is not up to date.

Preventing Hypervisor-Based Attacks

The previous example is a simplistic one that is quickly resolved by applying the right patches. But hypervisor-based attacks can come from many possible vectors. Adding to this complexity, vulnerabilities are likely to impact every virtualization solution available on the market today. With many environments leveraging the use of multiple virtualization solutions—each requiring its own vendor-specific tool for scanning—administrators are likely to see a significant added workload associated with verifying their virtual security.

In order to best recognize and prevent hypervisor-based attacks, IT organizations should consider the following suggestions for improving their security posture for virtualized environments:

- *Identifying hypervisor vulnerabilities with vulnerability assessments.* Hypervisor-based attacks exist on-disk and on the network in much the same way that traditional malware does with physical OSs. Thus, locating potentially unwanted software means identifying their known heuristics. Using an effective vulnerability assessment solution, organizations can assess hypervisors for missing updates and properly plan change control windows to mitigate risks. Although the proper defense against a hypervisor-based attack is the installation of necessary patches, assessing their risk to the environment is equally critical.
- *Prevent network exposure.* Virtualization environments enjoy a much greater level of agility in terms of network configuration. With essentially all virtualization solutions including virtual networking components inside the virtual server, it is possible to restrict traffic to those connections that have access to the hypervisor. Preventing all but the most critical of network connectivity to the hypervisor itself goes far in preventing network-based attacks from impacting the hypervisor.

-
- *Segregate management networks.* One way in which the previous points can be accomplished is through a logical separation of management networks from those used by virtual machines themselves. Virtual machines and their network traffic typically have no need for direct network access to those networks used for hypervisor management. Segregating traffic to networks exclusively used for hypervisor management limits hypervisor exposure.
 - *Consider agent-based approaches.* Although agentless approaches may involve fewer requirements for management, there are certain needs that can only be fulfilled through agent-based approaches. Scanning, patching, reporting, and suggesting improvement actions work best when agents leverage administrative access for digging deep into system processes. This is particularly the case when other securing mechanisms—such as those discussed in the earlier bullet points—are being used in the environment.

Virtual Machine Eggs in Your Hypervisor Basket

Virtualization indeed promises huge improvements to cost and management flexibility but with the silent risk associated with its common hypervisor code across the environment. Thus, hosting all your virtual workloads atop that singular entity brings the need for added diligence in terms of security for the hypervisor itself. Environments that don't move now to protect this pervasive interface will see the risk of large-scale virtual machine failure in the case of an infection event.