5 LAWS OF VIRTUALIZATI SECURITY

VIRTUALIZATION TECHNOLOGY CAN DELIVER COST SAVINGS AND IMPROVE IT PERFORMANCE, BUT IT ALSO INTRODUCES NEW SECURITY CONCERNS. IN THIS SUMMARY OF A BURTON GROUP REPORT, SECURITY EXPERT PETE LINDSTROM EXAMINES THE SECURITY CONSIDERATIONS UNIQUE TO VIRTUALIZED IT ENVIRONMENTS.

THE VIRTUALIZATION OF CLIENTS AND SERVERS—AND THE impact it has on networks and storage—is a hot topic in IT. As a result, it's also a hot topic in security.

There are multiple perspectives on how virtualization impacts security. Some claim that virtualization's isolation properties make it beneficial to security, while others say the added complexity of the overarching management software—known as the hypervisor—and the opportunity to "escape the virtual machine (VM)" are detrimental to security.

As with any new technology as broad and comprehensive as virtualization, such security concerns are critical. In addition, the combination of technical details and marketing messages from vendors can create a potent cocktail of ambiguity about the real impact these new architectures have on risk management and security.

Beyond the superficial discussions of hypervisor-based rootkits and discovery techniques are the very real issues of allocation of information assets and the relative impact on threats and vulnerabilities. Indeed, virtualization comes with its own set of unique security considerations. The appropriate protection response to these inherent security characteristics is a measured approach that carefully considers the impact on the existing IT infrastructure; a factored analysis of threats, vulnerabilities and consequences; and an understanding of the impact on existing security solutions.

Rules of the Game

There are five immutable laws of virtualization security. It's essential to understand them and use them to drive security decisions. They are:

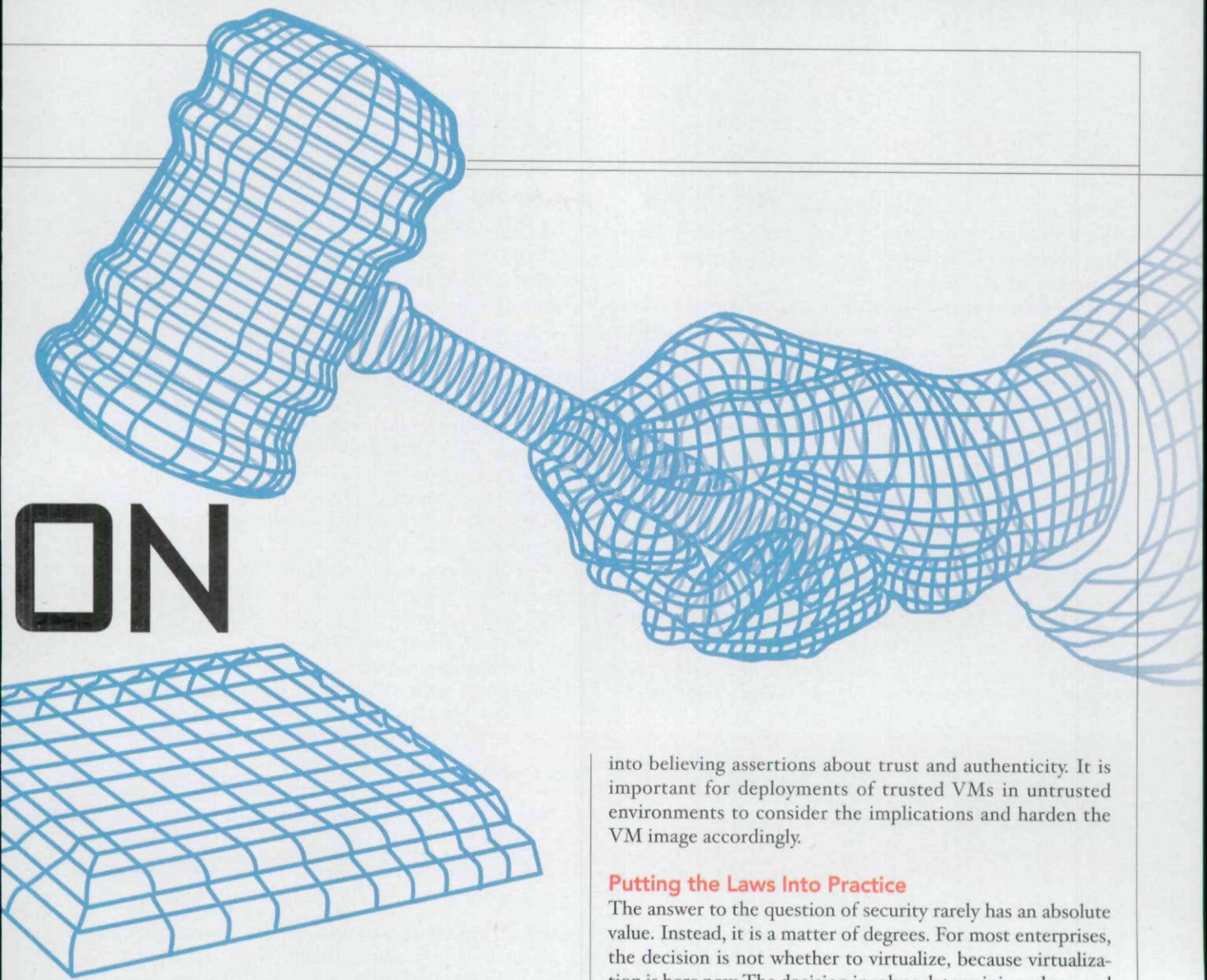
1. ATTACKING A VIRTUAL combination of operating systems and applications is exactly the same as attacking the physical system it replicates.

The beauty of a virtual machine is that it acts just like a physical system. However, in most environments, that means it can be attacked in the same way. Any data on the VM can be stolen, and if the VM has network access, it can be used as a stepping-stone to attack other systems.

2. A VIRTUAL MACHINE poses a higher security risk than an identically configured physical system running the same operating system and applications.

This corollary to the first law accounts for the additional vulnerability of a virtual system's controlling software, the hypervisor. Because the hypervisor monitors and responds to a VM, it is susceptible to attack. So it's important to recognize the risks inherent in the virtual environment and to offset them in other ways.

ILLUSTRATION BY MARCOS SINCONEGUI



3. VIRTUAL MACHINES CAN be made more secure than similar physical systems when they separate functionality and content.

When two processes share the same memory space, an attack against one process can impact the other. One way to benefit from virtualization is to separate functions and data into isolated operating environments. Such segregation helps reduce the risk added by the virtualization software that's part of the second law.

4. A SET OF virtual machines aggregated on the same physical system can only be made more secure than separate physical systems by modifying the VM's configurations to offset hypervisor risk.

While separating resources reduces risk, combining resources will initially increase risk (see #2). At this level of aggregation, VMs must be reconfigured to attain the same level of risk achieved through the third law. Turning off services, adding controls and separating content can help reduce overall risk.

5. A SYSTEM CONTAINING a trusted virtual machine on an untrusted host poses a greater risk than a system containing a trusted host with an untrusted VM.

Attacks at lower levels pose greater risks than those at higher levels, because higher-level programs can be tricked into believing assertions about trust and authenticity. It is important for deployments of trusted VMs in untrusted environments to consider the implications and harden the VM image accordingly.

Putting the Laws Into Practice

The answer to the question of security rarely has an absolute value. Instead, it is a matter of degrees. For most enterprises, the decision is not whether to virtualize, because virtualization is here now. The decision involves determining where and when to apply controls that are sufficient in the environment based on risk tolerance. Ultimately, whether virtualization is bane or boon for security depends on how the systems are configured, deployed and managed.

To manage these new security concerns, it's important to understand the underpinnings of today's virtual systems.

The primary components of a virtual environment are:

- **VIRTUAL MACHINES AND THEIR ACCOMPANYING GUEST OPERATING SYSTEMS:** These are the core components of the virtual architecture.
- **VIRTUAL MACHINE MONITOR (VMM):** The software component responsible for managing interactions between the VM and the physical system.
- **HYPERVISOR AND/OR HOST OPERATING SYSTEM:** The software that handles kernel operations.

A virtualized environment consists of a VMM and one or more VMs. The VMs and VMM interact with either a hypervisor or a host operating system to access hardware, local I/O and networking resources. In addition to these components, virtualization architectures leverage virtual networking, virtual storage and terminal service capabilities to complete their architectures.

This minimum set of components makes up virtual

environments in several distinct ways:

- **TYPE 1 VIRTUAL ENVIRONMENTS** are considered full virtualization environments and have VMs running on a hypervisor that interacts with the hardware.
- **TYPE 2 VIRTUAL ENVIRONMENTS** also are considered full virtualization environments, but work with a host operating system instead of a hypervisor (though sometimes the VMM is called a hypervisor).
- **PARAVIRTUALIZED ENVIRONMENTS** make performance gains by eliminating some of the emulation that occurs in full virtualization environments.
- **OTHER DESIGNATIONS** include hybrid virtual machines (HVMs) and hardware-assisted techniques.

From a security perspective, the most important thing to remember is that there is a more significant impact in a Type 2 environment where a host operating system with user applications and interfaces is running outside of a VM at a level lower than the other VMs. Because of the architecture, the Type 2 environment increases risk through its incorporation of potential attacks against the host operating system. For example, a laptop running VMware with a Linux VM on a Windows XP system inherits the attack surface of both operating systems, plus the virtualization code of the VMM.

OF COURSE, A VIRTUAL SYSTEM IS NOT WITHOUT ITS ATTACK VECTORS. ROGUE HYPERVISORS AND THE VM ESCAPE ARE TWO ASPECTS OF THREATS THAT SHOULD BE EVALUATED FULLY.

Security Benefits

Shared content and resources are the bane of security professionals, who spend most of their time collecting, categorizing, grouping and then separating resources in ways that make sense. Sometimes this grouping is done by business units, and sometimes it's done by other means, such as the classification of the content.

A virtual environment can provide a way to separate program resources and content to enhance security. Shared resources also share risk at the aggregate level. Separating resources and content allows for stronger protection of higher-risk resources and reduces the overall impact of a compromise. A number of valuable uses could come out of this. For example:

- **A SINGLE APPLICATION** or a set of applications could be run in a VM guest (or compartment) separate from all other applications.
- **A CONSULTANT WORKING** for two different companies could do work for each client in a separate VM.
- **AN INDIVIDUAL WORKING** on a personal computer could use one VM for business and another for personal finances and other home-related work.

User behavior can vary widely—from strong risk tolerance to strong risk aversion. Sometimes, this behavior can change quickly. Obviously, this creates a problem whereby the risk-tolerant behavior impacts the risk-averse requirements. An isolated temporary environment can provide a way to allow risk-tolerant behavior without significantly impacting the risk-sensitive resources.

One technique for virtual environments involves creating a "sandbox" VM and using it for risky activities. Assuming the content being created and the changes being made are insignificant in the long term, a user can "turn back time" to a point where the VM configuration was "known good"—typically reverting to the standard image. An obvious use for such a configuration is for shared systems, such as training systems and kiosks, to allow for maximum flexibility on the user side without creating any long-term damage.

The sandbox scenario also provides an obvious case in which streamlined recoverability is useful. In fact, the more frequent the reversion to a known-good state, the lower the potential for harmful consequences.

VMs also can be multiplied and distributed in many different ways. This flexibility is a boon to disaster recovery specialists looking for ways to increase availability. Maintaining replicated environments that are physically separate and creating images that can be recovered quickly contribute to the overall availability of the resources.

Attacking Virtualization

Of course, a virtual system is not without its attack vectors. Rogue hypervisors and the VM escape are two aspects of threats that should be evaluated fully.

In the past few years, much attention has been given to the use of virtualization in support of rootkits. Rootkits gain their effectiveness when they are hidden, and hypervisor rootkits—sometimes paradoxically called VM-based rootkits—hide by launching a rogue hypervisor and porting the existing operating system into a VM.

The guest operating system within the VM believes it is running as a traditional operating system with the corresponding control over local hardware and networking resources afforded to these systems—but it isn't. The hypervisor has control and can manipulate the activities on the system in any number of ways.

In 2006, a security researcher named Joanna Rutkowska introduced what she called the "blue pill," a hypervisor rootkit that inserts itself into memory, subordinates the real operating system to VM status and gains a level of invisibility by extension. To date, the rogue hypervisor is of greater concern to security researchers than to the enterprise. In fact, using

virtual systems becomes a sort of protection in itself, since malware installed in a VM would not execute its payload.

Another security concern involves what is known as "escaping" the virtual machine. This ability to move malware outside the VM and execute arbitrary code on the physical host is considered the holy grail of virtualization security research. Given that the intent of virtualization is to be transparent to existing functionality, the hypervisor is the only new component that need be assessed.

The ability of the hypervisor to withstand attack and provide some level of isolation among VMs is at the root of how risk will fare in these environments. Since the hypervisor is, after all, a software program, it stands to reason that additional software initially increases the risk in any environment, simply because there is more code implemented with more complexity than with traditional IT environments.

Several researchers have demonstrated rudimentary VM escape exploits, and as the popularity of virtual systems increases—and the platform becomes a more lucrative attack target—the threat will continue to increase.

The Impact on Risk

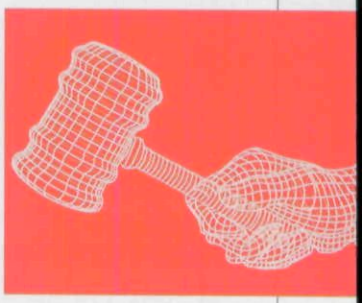
Although the benefits of a virtual environment are clear, they are not always realized in every architected environment. The fact is that the various characteristics will be mixed and matched with other IT resources. Given that probable outcome, it is useful to review risk principles and apply them to a virtual environment. The Burton Group defines risk as a function of threats, vulnerabilities and consequences, and an increase in any of these three elements increases overall risk.

THREATS: At this stage of virtualization technology development, the likelihood that malicious attackers will target virtual environments is relatively low. That said, as more people get trained on and learn about virtualization, attackers are bound to follow. Given the adoption rate of virtualization technology, it's reasonable to assume this threat is accelerating quickly.

VULNERABILITIES: The vulnerability of a system is a measure of its attack surface: the nature and extent of resources that are exposed and therefore attackable. Of course, if isolation mechanisms like firewalls or operating system access controls fail, the attack surface balloons to encompass the entire machine. The question, then, is whether the attack surface of a system or of an enterprise IT environment as a whole increases or decreases with the deployment of virtual environments.

The attack surface increases with the increased availability of services on any IT resource. This means that the addition of a system to an enterprise environment increases the attack surface. At a more granular level, starting services, opening Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and registering remote procedure call (RPC) endpoints also increase the attack surface. If more resources are consumed, more risk is incurred.

Most virtual environments aim to make themselves transparent throughout the environment. However, something new is behind the scenes of the systems: the hypervisor and VMM. The addition of the hypervisor resource increases risk, just as any other additional service does.



So, if everything else remains constant, the vulnerability component of risk is increased in virtual environments. Everything else does not have to remain constant, however. To whatever extent other resources can be reduced, eliminated or isolated so they are no longer part of the attack surface, that will offset the increased attack surface and reduce overall vulnerability.

CONSEQUENCES: The final component of risk is the impact or consequences of a successful attack. In most IT environments, the value of information assets is increasing as organizations work to squeeze out more benefits from systems. As these functions take on more mission-critical capabilities, associated losses increase as well.

Security Safeguards

Security teams should take a number of steps to ensure the improved protection of virtual environments, including:

USE ALL EXISTING SECURITY MECHANISMS. Since one of the primary goals of virtualization is transparency, all current host-based solutions should operate in exactly the same way, with limited need for modifications. Existing solutions may not be optimal, but they'll provide reasonable security.

GET YOUR ADMINISTRATIVE ACT TOGETHER. The dynamic nature of the VM lifecycle and the potential for VM sprawl hint at an even more difficult asset-management environment in the virtual world. It is prudent to ensure that administrative procedures are ready for identifying and tracking VMs throughout the environment.

LOOK FOR WAYS TO MOVE SECURITY OUT OF THE VM. Enterprises can reduce or eradicate agents from VMs and create separate process spaces for user activities and security functions.

MANAGE VIRTUAL MACHINES LIKE FILES AND SYSTEMS. The portability of VMs makes them vulnerable to file-style attacks, so they must be protected in a similar fashion. The goal of file-oriented management is recognizing the file objects and providing cryptographic and access-control protection for them.

ENCRYPT NETWORK TRAFFIC WHERE POSSIBLE. Encrypted communications provide some protection against local sniffing threats that may come from other VMs or the hypervisor.

PRACTICE SEGREGATION OF FUNCTIONS. Because multiple VMs can be run on the same machine, it may be possible to create separate compartments for security components. Strong candidates for segregation include logging events externally, maintaining separate keys for encryption, and separating policy and configuration from the image.

PETE LINDSTROM, A SENIOR ANALYST AT THE BURTON GROUP, SPECIALIZES IN SECURITY METRICS, RISK MANAGEMENT, WEB 2.0/SOA/WEB SERVICES SECURITY AND SECURING NEW TECHNOLOGIES.