Top virtualization security risks and how to prevent them

There are multiple attack avenues in virtual environments, but this tip highlights the most common threats that are likely to be experienced by all. In addition, you’ll find best practices for preventing hypervisor malware.
Top virtualization security risks and how to prevent them

Table of Contents

Top virtualization security risks and how to prevent them

Virtualization security concerns: The threat of hypervisor malware

Resources from CA Technologies
Top virtualization security risks and how to prevent them

By Philip Cox

One of the top cloud computing threats involves one of its core enabling technologies: virtualization. In virtual environments, there are multiple attack avenues, but this tip will look at ones that are most likely to be experienced by users of the technology:

- Prebuilt virtual machines/virtual appliances containing malicious code (Trojaned)
- Improperly configured virtual firewalls or networking
- Improperly configured hypervisor
- Data leakage through offline images

When building security defenses against these virtualization security risks, it’s important to keep in mind a concept that is typically understood and yet often overlooked: The hypervisor and its guests are really just one big pile of code on one physical box. There is no guarantee that the hypervisor is more secure or less buggy than any other software of comparable size (unless “evaluated,” according to e.g., United States Government Department of Defense (DoD) Trusted Computer System Evaluation Criteria). The physical isolation/separation that was relied upon (at some level) for security is gone, and we need to take that into account when thinking about threats.

Trojaned virtual machines/virtual appliances

The presence of untrusted virtual machines or Trojaned virtual appliances in the environment should be the first virtualization security risk you address. The untrusted virtual machine will manifest itself in public clouds (i.e., multitenant), and is a bad guy bringing up a malicious system that will attempt to identify “proximity” related vulnerabilities. The threats are created because the VM is either running on the same hypervisor or within the same cloud, and the cloud provider has created some level of “trust” between the virtual machines that the consumer is not aware of. If those vulnerabilities exist, the likelihood of exploit increases significantly.
Malicious virtual appliances (an appliance in this sense is anything that is “pre-packaged” for you to just download and run as a VM) would be a threat in public or private cloud environments. Since you install/use these appliances, there’s an element of trust you have given them. The malicious system would then attempt to find vulnerabilities through its “trust” and exploit them. Now an attacker would have a compromised machine in your environment, thus the intrusion succeeded. Recently, Amazon notified its Elastic Compute Cloud customers that it had identified compromised Amazon Machine Images (AMI) in its community set of AMIs, which are combinations (i.e., stacks) of software created to help users deploy servers quickly in EC2. The notification reminded users about the danger of compromised AMIs. Amazon realized that a compromised “appliance” or “build image” provides a trusted foothold in obtaining critical information, such as credentials for further exploit.

The keys to preventing these threats are to only use verified and tested appliances/images, and have assurance that your cloud provider has properly configured hypervisor and networking configurations that do not create unintended proximity trust. Further, keep in mind the nature of physical isolation/separation in the virtualized environment and configure systems accordingly.

**Improperly configured virtual firewalls or networking**

Traditionally, the networking team handled the configuration of firewalls and network equipment. They understand the intricacies and security implications of VLANs, tagging, routing, stateful connections, how inbound vs. outbound apply to interfaces, etc. This may or may not be true for many host administrators. In a virtual environment, many of the host administrators are now configuring and managing these network security devices. If these devices are not configured correctly, you can have traffic meant for one VM being seen or delivered to another VM or an outside entity.

While tools exist to do this right, it is primarily a people “issue,” in that administrators are being asked to manage security devices they do not understand. Overlook this, and you can have your underbelly exposed.
The key to minimizing this virtualization security risk is to have the network team handle the networking in the virtual environment, even though the virtual networking devices are not physical pieces of networking equipment. If you don’t have that luxury, then training the host administrator in the security aspects of network configurations is the next best mitigation.

**Improperly configured hypervisor**

The security of the environment is linked to the security of the hypervisor; any unauthorized access to the hypervisor compromises the environment. The main threat here is a lack of controls to limit who can gain access, and once in, what access they have. These are pretty straightforward threats, in that allowing unrestricted access to hypervisors, especially one that can be reached from an untrusted network (e.g., the Internet) increases the threat of attack. Secondly, if you do not restrict what legitimate users can access once they authenticate, you open yourself up to attack.

The first vulnerability is easy to deal with by restricting what systems can get access to the management functions (GUI, API, login, etc.). The second is not quite as easy, because you need a robust access control mechanism to allow the access/management of the users VMs (workloads), but not to the host. Further, you likely want to allow certain operations on the host to some users, but not all operations. The underlying access control mechanism must be able to support this. Since many cloud providers (e.g., Amazon) are building hypervisors almost from the ground up, getting the necessary access control mechanisms is difficult.

The key to minimizing this threat is the use of granular role-based access control mechanisms to the hypervisor and management applications.

**Data leakage through offline images**

When guest images are suspended, unlike physical systems that would need physical access to pull data out of memory, the memory “footprint” now is in a file, and for all intents, searchable. Take an application securing Social Security or credit card numbers: The VM may be solid and secure, however, when the system is suspended, any information put in memory is likely not protected and assumed to be volatile. The problem arises when the
image suspends and writes that memory to disk. Also, with migration, information states that would never have existed before now exist. We need to protect against that.

The nice thing about virtual security is that if you have a good security program in general, you will likely have a secure virtual environment as well. The fact is that if you apply old system administration practices (as they relate to security) to virtual environments, you will be well on the way to minimizing virtualization security risks and a secure environment.
cloud security.
Can you see beyond the problem?
You can

The #1 issue for companies migrating to the cloud is identity and access management. But for the agile business, knowing users is always better than no-ing them.

In fact, agile businesses, using our Content-Aware Identity and Access Management solutions, have been able to reduce security risk while improving productivity, access and efficiency. More effective compliance, reduced IT risk, broader, more secure customer and partner relationships.

That’s what happens when no becomes know. And security turns into agility.

To see how we can help make your business more agile and secure, visit ca.com
Virtualization security concerns: The threat of hypervisor malware

By Nick Lewis

Malware for hypervisors is rare, but could have a significant effect on the trustworthiness of the system as reported. For hypervisor malware to increase in occurrence, it’s likely that criminals would need to find ways to more easily monetize attacks on the hypervisor. However, given the high level of access that could be gained by compromising a hypervisor, these types of attacks are one of several virtualization security concerns that are likely to increase in occurrence and could cause significant disruptions, such as denial-of-service (DoS) attacks or compromises of sensitive data.

Also, some hypervisors are vulnerable to malware attacks because of the platform they run on. Microsoft Hyper-V, VirtualPC and certain versions of VMware, run on top of Windows, and other hypervisors run on top of Linux-based systems. The Linux or Windows server components could be attacked to compromise the security of the virtual infrastructure.

A new method that can be used to prevent malware from infecting a hypervisor was discussed in a recent technical report by researchers at North Carolina State University and IBM, but some other best practices can be taken. These could include isolating the management interfaces of, and connections to the hypervisor to only the systems that need access, not running un-trusted code on the hypervisor, such as software not provided by the hypervisor vendor and keeping the hypervisor software up to date. This excludes any security measures that should be taken on the guest OSes on the virtual infrastructure to ensure the guests cannot be used to attack the hypervisor.
Resources from CA Technologies

Securing Virtualized Environments and Accelerating Cloud Computing

Webinar: Powerful Control of Privileged Users

Controlling Privileged Users with CA Access Control

About CA Technologies

CA is one of the world’s largest IT management software providers. Our software and expertise unify and simplify complex IT environments—in a secure way—across the enterprise for greater business results. We call this Enterprise IT Management (EITM)—our clear vision for the future of IT. It's how you can manage systems, networks, security, storage, applications and databases securely and dynamically. You can build on your IT investments, rather than replacing them, and do it at your own pace. Our more than 5,300 developers worldwide create and deliver IT management software that keeps our vision real. And we've taken our decades of experience solving complicated IT problems and developed practical paths for you to get from where you are today to where you want to be.