Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

January 23, 2017

Outline

What is Virtualized Networking?

1. Full virtualization hypervisors can provide networking capabilities, allowing the individual guest OSs to communicate with one another while simultaneously limiting access to the external physical network.
2. The network interfaces that the guest OSs see may be virtual, physical, or both.
3. Typical hypervisors offer three primary forms of network access:
   - Network Bridging:The guest OS is given direct access to the hosts network interface cards (NIC) independent of the host OS.
   - Network Address Translation (NAT):The guest OS is given a virtual NIC that is connected to a simulated NAT inside the hypervisor. As in a traditional NAT, all outbound network traffic is sent through the virtual NIC to the host OS for forwarding, usually to a physical NIC on the host system.
   - Host Only Networking:The guest OS is given a virtual NIC that does not directly route to a physical NIC. In this scenario, guest OSs can be configured to communicate with one another and, potentially, with the host OS.
4. When a number of guest OSs exist on a single host, the hypervisor can provide a virtual network for these guest OSs.
5. The hypervisor may implement virtual switches, hubs, and other network devices.

What is Virtualized Networking?

6. Using a hypervisors networking for communications between guests on a single host has the advantage of greatly increased speed because the packets never hit physical networking devices.
7. Internal host-only networking can be done in many ways by the hypervisor. In some systems, the internal network looks like a virtual switch. Others use virtual LAN (VLAN) standards to allow better control of how the guest systems are connected.
8. Most hypervisors also provide internal network address and port translation (NAPT) that acts like a virtual router with NAT.
9. Networks that are internal to a hypervisors networking structure can pose an operational disadvantage.
10. There are some hypervisors that allow network monitoring, but this capability is generally not as robust as the tools that many organizations have come to expect for significant monitoring of physical networks.
11. Some hypervisors provide APIs that allow a privileged VM to have full visibility to the network traffic. Unfortunately, these APIs may also provide additional ways for attackers to attempt to monitor network communications.

What is Virtualized Networking?

12 Another concern with network monitoring through a hypervisor is the potential for performance degradation or denial of service conditions to occur for the hypervisor because of high volumes of traffic.

13 The security implications of networks internal to a hypervisor should not be minimized. For example, assume that an organization has two computers, one that acts as a public-facing web server and another that is an internal database server.

14 The organization also monitors the switch that connects the two computers, watching for traffic that would indicate an attack on the database.

15 If both of those servers were moved onto a single hypervisor, and the hypervisors virtual network was used for communications between the servers for increased efficiency, the ability to monitor all the traffic between the two systems would be lost unless the hypervisor itself can perform this monitoring that meets the organizations security policies.

16 To get around this loss of visibility, some organizations purposely expose network traffic between virtualized hosts to the physical network already in place in the organization.

What is Virtualized Networking?

17 This requires the system on which the hypervisor is running to have multiple network interfaces, and this may significantly slow network communications as compared to a virtual-only network, but the advantage is that the organization does not need to change its security policies to gain the cost advantages of virtualization.

18 Organizations should consider the tradeoffs between traffic being hidden within a hypervisor and the extra overhead and risk of exposing that traffic but being able to control it using the same tools already used for controlling other network traffic.

What is Virtualized Storage?

1. All hypervisors in common use present the guest OSs with virtual hard drives though the use of disk images.
2. A disk image is a file on the host that looks to the guest OS like an entire disk drive.
3. Whatever the guest OS writes onto the virtual hard drive goes into the disk image.
4. With hosted virtualization, the disk image appears in the host OS as a file or a folder, and it can be handled like other files and folders.
5. The security implications of using virtual storage are essentially the same as using real storage.
6. Access to the various types of storage that a guest OS has access to should be controlled as it would be if the storage were being used by a full computer.
7. Access to the virtual storage can be controlled at the host and VM level. Existing authentication and authorization mechanisms is leveraged to restrict user access to the file and object resources according to the organization policy.

What is Guest OS Images?

1. A full virtualization hypervisor encapsulates all of the components of a guest OS, including its applications and the virtual resources they use, into a single logical entity.
2. An image is a file or a directory that contains, at a minimum, this encapsulated information. Images are stored on hard drives, and can be transferred to other systems the same way that any file can (note, however, that images are often many gigabytes in size).
3. Some virtualization systems use a virtualization image metadata standard called the Open Virtualization Format (OVF) that supports interoperability for image metadata and components across virtualization solutions.
4. A snapshot is a record of the state of a running image, generally captured as the differences between an image and the current state.
5. For example, a snapshot would record changes within virtual storage, virtual memory, network connections, and other state-related data.
6. Snapshots allow the guest OS to be suspended and subsequently resumed without having to shut down or reboot the guest OS. Many, but not all, virtualization systems can take snapshots.

What is Virtualization Security?

1. Migrating computing resources to a virtualized environment has little or no effect on most of the resources vulnerabilities and threats.
2. For example, if a service has inherent vulnerabilities and that service is moved from a non-virtualized server to a virtualized server, the service is still just as vulnerable to exploitation.
3. However, the use of virtualization may help reduce the impact of such exploitationbut virtualization may also provide additional attack vectors, thus increasing the likelihood of successful attacks.
4. Guest OS Isolation:
    1. The hypervisor is responsible for managing guest OS access to hardware (e.g., CPU, memory, storage).
    2. The hypervisor partitions these resources so that each guest OS can access its own resources but cannot encroach on the other guest OSs resources or any resources not allocated for virtualization use.
    3. This prevents unauthorized access to resources and also helps prevent one guest OS from injecting malware into another, such as infecting a guest OSs files or placing malware code into another guest OSs memory.
    4. Separately, partitioning can also reduce the threat of denial of service conditions caused by excess resource consumption in other guest OSs on the same hypervisor.

What is Guest OS Isolation?

5. Resources may be partitioned physically or logically.
6. In physical partitioning, the hypervisor assigns separate physical resources to each guest OS, such as disk partitions, disk drives, and network interface cards.
7. Logical partitioning may divide resources on a single host or across multiple hosts as in a pool of resources with the same security impact level categorization, allowing multiple guest OSs to share the same physical resources, such as processors and RAM, with the hypervisor mediating access to the resources.
8. Physical partitioning sets hard limits on resources for each guest OS because unused capacity from one resource may not be accessed by any other guest OS.
9. However, having physical separation for resources may provide stronger security and improved performance than logical partitioning.
10. Many virtualization systems can do both physical and logical partitioning.
11. Some organizations have policies about which application data can physically reside on drives with the data of other applications, and such policies should take into account physical and logical partitioning in hypervisors.

What is Guest OS Isolation?

12 Having separate partitions for resource is an important part of isolating guest OSs.

13 Isolation also involves limiting guest OS communications and the access that each guest OS has to the other guest OSs, to the hypervisor, and to the host OS (if present).

14 Hypervisors can theoretically support a level of logical isolation nearly equivalent to physical isolation, mediating all communications from each guest OS to have full control over each guest OSs actions.

15 Hypervisors can permit interactions between guest OSs as needed, such as allowing two desktop OSs to share a file system. Hypervisors can also dynamically alter isolation for each guest OS as neededfor example, enabling and disabling networking at specific times.

16 Isolation has obvious security benefits, but it can also increase the reliability of a host by preventing actions in one guest OS from directly affecting another. For example, if one guest OS crashes because of an application fault or an attack, the other guest OSs on that host are unlikely to be affected. Isolating each guest OS from the others and restricting what resources they can access and what privileges they have is also known as sandboxing.

What is Guest OS Isolation?

17 Another motivation for isolating guest OSs from each other and the underlying hypervisor and host OS is the mitigation of side-channel attacks.

18 These attacks exploit the physical properties of hardware to reveal information about usage patterns for memory access, CPU use, and other resources.

19 A common goal of these attacks is to reveal cryptographic keys. These attacks are considered difficult, usually requiring direct physical access to the host.

20 Attackers may attempt to break out of a guest OS so that they can access the hypervisor, other guest OSs, or the underlying host OS. Breaking out of a guest OS is also known as escape.

21 If an attacker can successfully escape a guest OS and gain access to the hypervisor, the attacker might be able to compromise the hypervisor and gain control over all of its guest OSs.

22 So the hypervisor provides a single point of security failure for all the guest OSs; a single breach of the hypervisor places all the guest OSs at high risk.

23 Guest OSs are often not completely isolated from each other and from the host OS because that would prevent necessary functionality.

What is Guest OS Isolation?

24 For example, many hosted virtualization solutions provide mechanisms called guest tools through which a guest OS can access files, directories, the copy/paste buffer, and other resources on the host OS or another guest OS.

25 These communication mechanisms can inadvertently serve as an attack vector, such as transmitting malware or permitting an attacker to gain access to particular resources. Bare metal virtualization software does not offer such sharing capabilities.