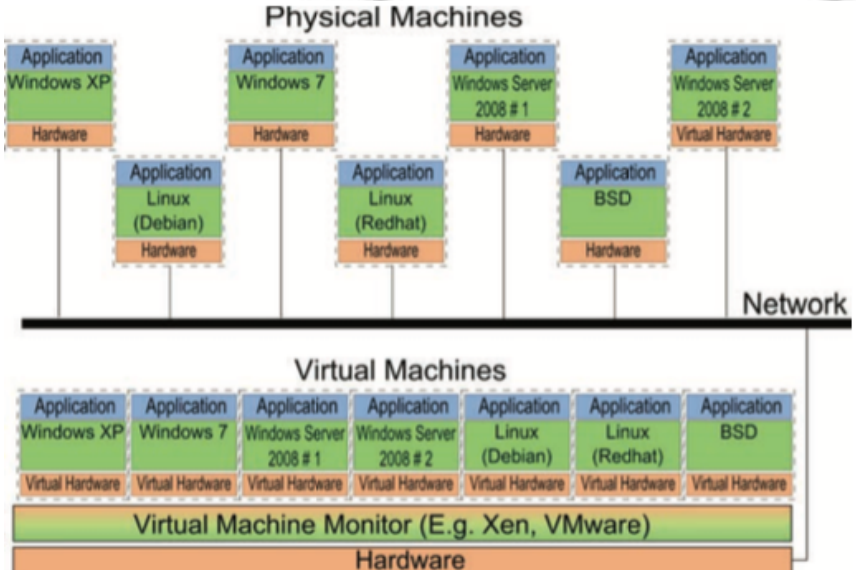
Security and Privacy Risks Associated With Using Virtual Machines

By Julien Kuzniarek

What are Virtual Machines?



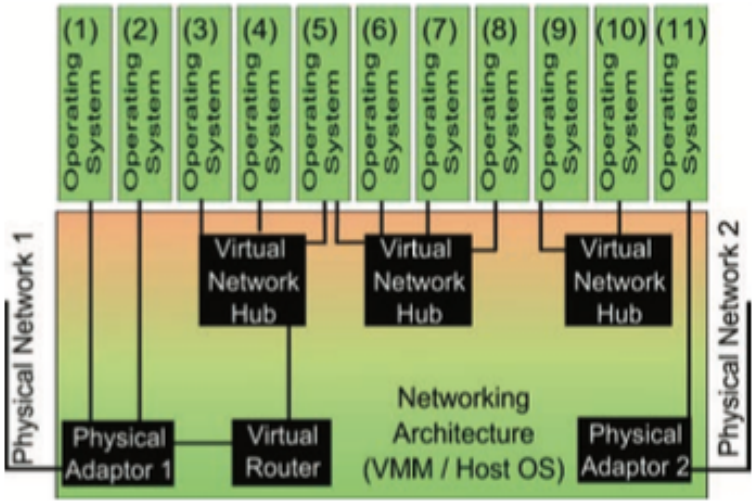
- "System virtualization is the use of an encapsulating software layer that surrounds or underlies an operating system and provides the same inputs, outputs, and behavior that would be expected from physical hardware." (M.pearce et al.)
- This encapsulating software is a Virtual Machine Monitor (also known as a Hypervisor) and each instance where an operating system is installed is called a Virtual Machine.

Why use Virtual Machines?

- Virtual Machine Monitors work by simulating the physical hardware that an operating system normally runs on.
- This enables an individual hardware system to run more than one instance of an operating system.
- The ability to use virtual machines enables consolidation of physical servers to conserve power and increase efficiency.
- Most importantly, the Cloud could not exist without modern virtual machines.
- Together, this means that virtual machines are becoming and in many cases have already become more widespread resulting in an increased probability of being the target of a security breach.

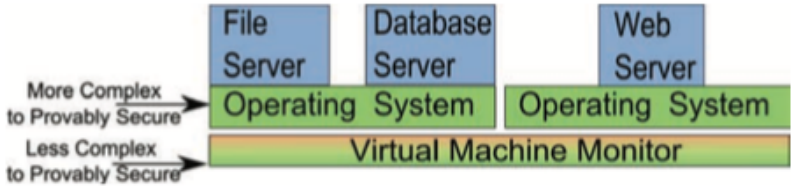
Security Benefits

Because VMMs simulate the hardware that operating systems rely on they are not only able to function as a DMZ between the Virtual Machines and the internet, but can also allow the formation of a completely virtualized network between Virtual Machines hosted on interlinked servers located at a single location.



Security Benefits

- Through the Isolation of the significantly more complex operating system, the Hypervisor (VMM) is able to improve system Confidentiality.
- Through the increased oversight resulting from the ability to control and filter all the resources moving to and from the operating system, the Hypervisor is able to improve system Integrity.
- Through the ability to run, manage, and save multiple Virtual Machines on a given hardware system the Hypervisor enables easy duplication and subsequently increased system Availability.



Security Vulnerabilities

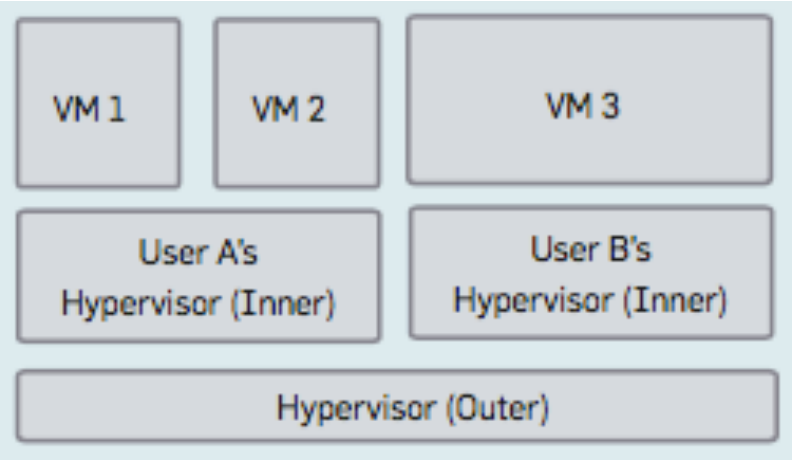
- Unfortunately, the strengths of using Virtual Machines are also their weaknesses.
- The concentration of virtual machines within a single, all powerful, virtualization platform means that if the platform is compromised than so are the Virtual Machines and all their data and processes.
- Further complicating the matter is that despite the Virtual machine's isolation, it is still susceptible to the vulnerabilities in the applications it is running.
- The potentially numerous number of Virtual Machines operated by different clients within a given server or server network means that if any client's Virtual Machine results in the compromise of the VMM, then all of the other clients have been compromised as well.

Security Vulnerabilities

- Concentrating Virtual Machines and their associated data in one location under the control of a single entity (frequently a separate entity from the one utilizing the Virtual Machines) also means surrendering complete control to someone outside your organization who you most likely have no oversight over.

- Because clients access Virtual Machines over a network of some sort (usually the internet), they are still susceptible to a large amount of malware as well as other network threats such as Man in the Middle attacks, rootKits uploaded to Virtual Machines, viruses, worms, exploits and more.

Nested Virtualization (Nanavati)



- Nested Virtualization allows an outer Hypervisor to host other inner Hypervisors, which in turn host the Virtual Machines.
- This provides an additional layer of isolation for client's Virtual Machines.
- It also enables the client to manage their Virtual Machines through the inner Hypervisor, while the system administrator is limited to managing the outer Hypervisor.
- Through Nested Virtualization, clients are able to maintain greater control of their systems and even encrypt and organize their own data as they see fit.

Virtual Private Networks

- VPNs allow encrypted transmission of data through networks.
- “Restrict remote access to virtual server hosts to requests coming in via a VPN tunnel” (Mattsson)
- While you can’t necessarily guarantee that the information exchange between the client computer and the virtualization system wont be intercepted, you can at least transmit it in a way that will maintain the Confidentiality of the data.

Firewall and AV Software

"Rather than seeing an emergence of active exploits targeting virtual machines, we're likely to continue to experience attacks aimed against operating systems, applications and web services for several years to come as they almost certainly harbor the most effective exploit avenues due to legacy code." (Mattsson)

- Since Virtual Machines still utilize traditional operating systems and applications, they are still potentially vulnerable to threats that this software is vulnerable to.
- Utilizing a firewall, and frequently updated antivirus software on each the Virtual Machines, servers, and the client's computers remains an important component of system security.

Threat Vectors

- Broadly speaking, the threat vectors for the entire virtualization system can be divided as follows.
- Network oriented: data is intercepted on the network between the client computer and the physical machine running the VMM.
- Virtualization platform oriented: servers and VMM are compromised.
- Application oriented: the operating system and/or applications running within a Virtual Machine are compromised.

Risk

Vector	Likelihood	Impact
Network	High	Medium
Virtualization Platform	Medium now, High in the Future	Very High
Applications	High	High

Optimal Solution

- If possible, integrate a VPN into the VMM and/or servers. As a client always access Virtual Machines through a VPN.
- Utilize nested virtualization architecture. Provide some means of teaching the clients how to manage their Hypervisor so it is utilized properly.
- Maintain a firewall for all systems interacting over a network and updated AV software on all machines, both Physical and Virtual.

Benefits of My Solution

- Utilizing VPNs will prevent patient data, as well as passwords, and account information from being intercepted and stolen.
- Nested Virtualization will prevent other virtualization clients that have been compromised from compromising the data and systems of your healthcare organization.
- Maintaining a Firewall and updated AV software will help to ward against threats that are not specific to Virtual Machines and that may be accidentally transmitted to a Virtual Machine from an infected employee workstation.

Other Reasons For Implementation

- While some healthcare organizations may be choose to support local, non-virtual Machines, the economics of the technology will push most into opting for virtualization systems.
- Given the importance of maintaining HIPAA and HITECH compliance, and the consequences associated with not doing so, healthcare organizations will want as many protections as they can get.
- Until Virtualization companies develop Hypervisors that are specifically security oriented, healthcare organizations will need to press for implementation of Nested Virtualization, VPNs, and frequently updated AV software from vendors in order to improve security beyond the little that is available in current systems.

References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*357-383. doi:10.1016/j.ins.2015.01.025

Li, J., Li, B., Wo, T., Hu, C., Huai, J., Liu, L., & Lam, K. (2012). CyberGuarder: A virtualization security assurance architecture for green cloud computing. *Future Generation Computer Systems*, *28*379-390. doi:10.1016/j.future.2011.04.012

Mattsson, U. (2009). Virtualisation: Real security for virtual machines. *Network Security*, *2009*15-17. doi:10.1016/S1353-4858(09)70041-8

NANAVATI, M., COLP, P., AIELLO, B., & WARFIELD, A. (2014). Cloud Security: A Gathering Storm. *Communications Of The ACM*, *57*(5), 70-79. doi:10.1145/2593686

PEARCE, M., ZEADALLY, S., & HUNT, R. (2013). Virtualization: Issues, Security Threats, and Solutions. *ACM Computing Surveys*, *45*(2), 17-17:39. doi:10.1145/2431211.2431216