

Securing a Virtual Environment

By Brian Fowler

Abstract: In today's world many corporations are moving into the realm of virtualization. Although this new technology allows companies to reproduce many different virtual servers and desktops, it also creates new problems in the ways of security. In this paper we will take a look at exactly what virtualization is, as it applies to servers and desktops. Through this we will learn of the various problems and vulnerabilities that virtualization will cause. Knowing the problems with virtual systems, we will answer the real question how can a virtual environment be secured. Follow with me as we take an in depth at virtualization and the means of securing it.

Virtualization is an older technology that has been around for years. "Virtualization dates back to the mid-1960s and IBM's virtual machine-enabled operating systems for mainframes." [1] Many administrators have been using this technology on large super computers. It is only in the last few years have implemented it on servers and started using it on a larger scale.

What is Virtualization and why do we use it?

In the world of computer technology virtualization is the ability to create a virtual copy of a device or some type of resource. These devices and resources include equipment like servers, storage devices, networks, and even the operating systems that could divide multiple resources into different execution environments.

Virtualization can be divided into three different categories Full virtualization, Para-virtualization, and Operating system-level virtualization.

The first is full virtualization uses what is called hypervisor. It interacts between the server's physical processor and the actual disk space. This serves as a platform for an operating system to be based virtually. The Full virtualization keep the different operating system totally separated from each other so that one doesn't know about the other. Setting up a system like this is more intensive on the hardware CPU because it has to keep track of each operating systems needs and manage them. This setup is good for running multiple different operating systems at once, such as Windows and Linux.

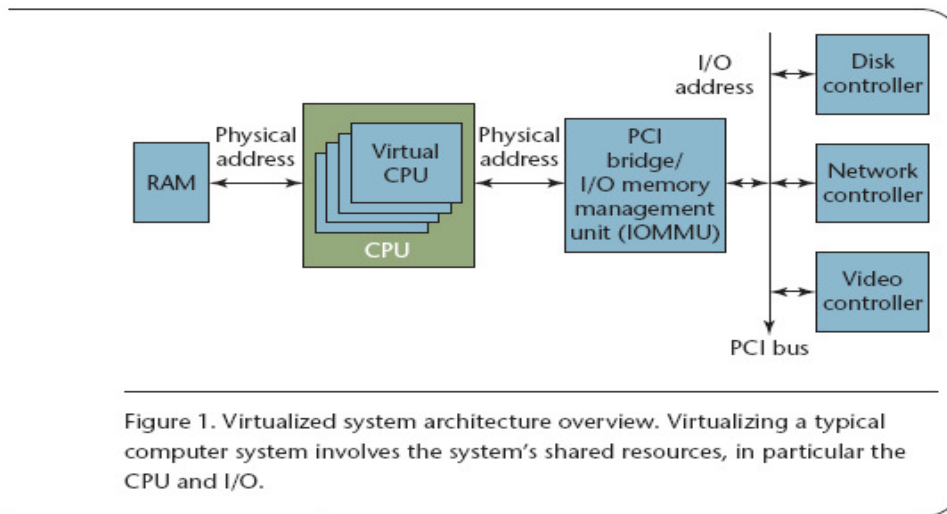
The second type is para-virtualization. Different from full virtualization, para-virtualization allows the systems to know about one another. Also this type of virtualization is not as intense on the hardware's CPU because of each OS knowing of the other. This allow each operating system manage there own resource needs accordingly.

The third and final one is OS-level virtualization. Instead of setting a hypervisor system to run, it uses a base operating system to run it virtualization. With this approach all the system have to run the same type of OS such as a Windows base with only Windows virtual systems.

Knowing the different types of virtualization now, why do we use virtualization? Industries use this system to lower their cost of hardware. Another reason that virtualization is used is also to consolidate the space needed to store multiple servers. Network engineers can consolidate multiple operating systems to a single hardware platform. From a single server, a number of virtual servers could be created to run multiple different services. In turn this will reduce other areas of cost such as reduced energy consumption, and the need for cooling that would have been needed to cover multiple physical servers. [2]

How does virtualization work?

Originally an operating system was linked to the hardware that it was installed on. With the use of virtualization tools like VMWare or Microsoft Virtual Machine the operating system could be split from the hardware and have its resources delegated to it from the host software and hardware. This allows many instances of operating systems.



[3]

The weaknesses encored from using virtual machines and how to secure them

The security risk that come along with using virtual machines varies depending on what the virtual system is being used for. Virtual Machine environments are like any other system; they still need the basic updates and security holes patched. One of the first incidences is problems with roll backs and restore points. Administrators enjoy the ability to be able to rollback or restore a virtual machine to a original configuration if the system crashes or becomes corrupted by a infection or hacker. As this is done patches could be rolled back and not placed back on the virtual machine. Also just rolling back to a previous state does not force an intruder from attacking a previous exploit. Another aspect of this is a roll back will reopen old accounts that may have been shut off for security purposes. "Rollbacks can also make VMs susceptible to new attacks because many security mechanisms rely on linear time, and revisiting a particular point in time in the virtual system violates these protocols. For example, rolled-back and replayed key streams in a stream cipher can be used to encrypt different plaintexts where analysis could help decipher the encrypted data. However, using the

same nonce twice in the Fiat-Shamir and Schnorr authentication protocols can cause the encryption system to leak the private key.”[4] The best way to act on this problem and secure it is through policies and procedures. A policy needs to be written that covers the rolling back, reapplication of updates and patches, and to search for any reopened accounts.

With the use of virtual machine you will bring new risk to the table. Virtualization has given the ability to make whole operating systems more mobile. A stolen or lost flash drive with an entire computing environment as a VM could reveal the victim’s entire desktop environment, complete with a company’s proprietary applications, configured with “remember password” settings and network mappings onto company servers. This is akin to having a laptop stolen, but with the theft concealable in a device the size of a pinky. Similarly, the next wave of malicious hackers could focus on breaking into suspect file servers to steal complete VMs.”[4]

. To secure these problems, two things must be done. First, with employees transporting virtual environments around the flash drive that are being used need to be encrypted or have some type of biometric like thumb print reader. To solve the problem with an intruder the main hardware that supports virtual needs to be stored in secure area with locking doors and limited access.

The next weakness is found in migration. “Data moves in clear-text format during a VM migration, permitting an attacker to perform a man-in-the-middle attack on a virtual machine’s hypervisor that would allow stealing data in transit, Oberheide said.”[5] The relevance of this is that it shows that implementing virtual machines can introduce its own inherent security issues. The way to protect against this vulnerability is through introducing manual authentication between the two migrating machines.

Then Network connection over the virtual network cards is also a point of interest that needs to be addressed. “network-based security systems typically don’t track communications between virtual machines on the same server. These systems generally examine traffic only between machines over physical network connections. The lack of visibility into virtual-machine traffic could enable attacks on VMs—or undetected attacks on physical systems that subsequently affect VMs—to spread.” [4] Since virtualization is a new and budding technology there is not many network monitoring systems that can track the exchanges that occur in between the virtual machines on a single hardware system. This allows malicious software to move undetected between multiple virtual machines. The way to secure the virtual machine environments is by placing a software firewall on each of them. This will allow for detection of malicious software as it travels between the virtual environments.

Virtual environments are used for many different reasons. Some companies use them to setup secondary networks such as building honeypots. Webopedia says honeypots are: “An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet

, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out. “[6] These honeypots require a lot of equipment in the past but thanks to virtualization this is no longer an issue. The security issue that comes into play here is that hackers have now developed tools like “VmDetect” [6] to determine that they are in a Virtual machine environment. This is accomplished through detecting the backdoor code that allows the VMs to interface with the hardware. Depending on the software being used this code looks different. An example of this code for VMware is bellow.

```
bool IsInsideVMWare()
{
    bool rc = true;

    __try
    {
        __asm
        {
            push    edx
            push    ecx
            push    ebx

            mov     eax, 'VMXh'
            mov     ebx, 0 // any value but not the MAGIC VALUE
            mov     ecx, 10 // get VMWare version
            mov     edx, 'VX' // port number

            in     eax, dx // read port
                    // on return EAX returns the VERSION
            cmp     ebx, 'VMXh' // is it a reply from VMWare?
            setz   [rc] // set return value

            pop     ebx
            pop     ecx
            pop     edx
        }
    }
    __except(EXCEPTION_EXECUTE_HANDLER)
    {
        rc = false;
    }

    return rc;
}
```

[7]

This in turn allows a hacker to learn that they are in a honeypot. The way to secure a honeypot to prevent the hacker from seeing it is to hide the Virtual machine. The way this can be accomplished is through disabling certain services in the configuration options of VMware. There options are:

- isolation.tools.getPtrLocation.disable = "TRUE"
- isolation.tools.setPtrLocation.disable = "TRUE"
- isolation.tools.setVersion.disable = "TRUE"
- isolation.tools.getVersion.disable = "TRUE"
- monitor_control.disable_directexec = "TRUE"
- monitor_control.disable_chksimd = "TRUE"
- monitor_control.disable_ntreloc = "TRUE"
- monitor_control.disable_selfmod = "TRUE"
- monitor_control.disable_reloc = "TRUE"
- monitor_control.disable_btinout = "TRUE"
- monitor_control.disable_btmemspace = "TRUE"
- monitor_control.disable_btpriv = "TRUE"
- monitor_control.disable_btseg = "TRUE"

[8]

These will effectively eliminate the detection of an instance of VMware.

Securing virtual machines

From the previous sections we have come to understand what virtualization is, how it works and a few of the vulnerabilities that it has. Now, with this information I will put all of this into a comprehensive plan for securing a network.

Protocols and procedures

The first step in any type of network is to lay out the protocols and procedures that must be followed. Inside of a virtual environment this must also be done. Below are a few guidelines that need to be added to procedure manuals.

- Updates must be checked and applied on a weekly basis for the operating system hosting the virtual machines.
- Updates must be checked and applied on a weekly basis for the virtualization software
- Updates must be checked and updated on a weekly basis for the virtual machines.
- When an account has been disabled it must be kept track of from at least two previous image resort points
- If a roll back occurs must re-disable any previously disabled accounts.
- If a roll back occurs on virtual machine to fix a corrupt image, all updates must be re-patched to the most current updates.

These are just a few procedures that need to be added to procedural manuals. As virtualization changes over time these are subject to change and be added to.

Software firewalls

The next security measurement that should be taken is to add a software firewall. As discussed earlier, when there multiple virtual machines environments on a single hardware system, there isn't a good way to monitor the transactions between the different virtual machines. This allows malware to run unchecked. To solve this it is good to install a good software firewall one each of the virtual machine environment. Some of the more popular firewalls that are out there include Comodo, zone alarm, and etc. These firewalls will be placed on every virtual machine. This will allow for detection and prevention of unwanted intrusion from malicious software.

Anti-virus software

Does a virtual machine need anti-virus software? In short yes, virtual machines are setup to be self-contained environments, in doing this there is a need to protect each virtual machine environment with some kind of anti-virus software. Although you might have Anti-virus setup on the host machine this will not cover the virtual machine environments. Anti-virus check file and folder on the local host machine but has no way of scanning the files on the inside of the virtual environment. That is why anti-virus must be placed on all the virtual machine environments. This will keep all virtual environments clear of virus, Trojan, and worms that it might inherent from it connection to the network. Among the more popular anti-virus software are Norton, Mac Affe, and Panda. It is strongly encouraged that this is applied.

Physically Securing

As mentioned earlier the introduction of virtual machine environments has made operating systems very mobile. Virtual environment are no longer tied to a particular hardware system. This allows it to be removed or copied very easily. Now that we have thumb drives upwards of 64 GB, it would be easy to steal a virtual environment. This is why it is important now more that ever to lock down the physical installation of virtual servers. To secure the virtual machines, they must be stored in a limited accessed area. The storage area must have a locking door with a keyed access.

Along with the physically securing the virtual environment's hardware, there must be some type of security for any instances of the employees storing copies of virtual servers on separate media. Secondary media in this case is devices like flash drives. When storing copies of virtual machine environment on flash drives the need to be protected in case of theft. If a flash drive was lost it would equate to the lose of a laptop with all the companies information on it. So how do we secure something like a flash drive? This is done through one of two ways, through using a flash drive that has a fingerprint reader or encrypting the flash drive. The flash drive with the fingerprint can be purchased for use, as for the encryption. To encrypt a flash drive is fairly easy there are many third party encryption software out there to use. One of these encryption software is "truecrypt." [9]

Virtual environments do have security risk associated with there implementation. Through the paper I have explained some of the weaknesses of virtual environment and how they can be secured. If these simple rules are followed and implemented then your virtual network will exhibit a fairly strong security.

Work Cited

1. *Steven J. Vaughan-Nichols, “Virtualization Sparks Security Concerns”, Technology News, Aug 2008, pp. 13-15
2. Jonathan Strickland “How Server Virtualization Works” How stuff works, <http://communication.howstuffworks.com/server-virtualization2.htm>
3. *Ronald Perez , Reiner Sailer, Leendert Van Doorn “Virtualization and Hardware-Based Security” , IEEE Computer Society, Sept/Oct 2008 pp. 24-31
4. *Michael Price “The Paradox of Security in Virtual Environments” IEEE Computer Society, November 2008 pp.22-28
5. Jim Carr “Two vulnerabilities found in VMware virtualization products” SC magazine, <http://www.scmagazineus.com/Two-vulnerabilities-found-in-VMware-virtualization-products/article/107207>
6. “Honeypot” Webopedia. <http://www.webopedia.com/TERM/h/honeypot.html>
7. lallous “Detect if your program is running inside a Virtual Machine” <http://www.codeproject.com/KB/system/VmDetect.aspx>
8. Tom Liston, Ed Skoudis “On the Cutting Edge: Thwarting Virtual Machine Detection” Intelguardians, 2006 http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf
9. Truecrypt <http://www.truecrypt.org>