Virtual Machines and Security

Paola Stone Martinez
East Carolina University
November, 2013.

Keywords: virtualization, virtual machine, security.

1. Virtualization

The rapid growth of technologies, nowadays, demands a high availability of equipment. One of these areas is the Information Technology (IT) field where the continuous development of new software is not backed up by hardware improvements. In the IT field it is very common to find that companies have equipment with great physical capabilities, but it is not being used at its maximum. "Individual severs machines often run at 5 – 10% CPU utilization. By using virtualization, various virtual servers can be consolidated within in physical server while still allowing independent configuration and failure isolation" [1]. These are some of the reasons of why virtualization has become very popular, and more companies and individuals are opting for its use.

Virtualization is a technology that separates hardware (Physical Host) from software (Operating System). It allows users to use different virtual machines running different operating systems on a single physical computer [2].

The NIST (The National Institute of Standards and Technology) defines virtualizations as "the simulation of the software and/or hardware upon which other software runs" according to them, there are two forms of virtualization: Application virtualization and Operating system virtualization. It depends on the computing architecture layer where it runs. For the purpose of this paper, the definition use for virtualization is the one which the NIST has named *full virtualization* where one or more Operating Systems and the applications they contain are run on top of virtual hardware. Each instance of an operating system and its applications runs in a separate Virtual Machine called a guest operating system [3].

1.1 What are Virtual Machines?

There are different definitions of what a virtual machine is. One of the most used is the one presented by VMware, one of the leading companies on virtualization. The definition given is: "A virtual Machine is a computer that is created by software that, like a physical computer, runs an operating system and applications. Each virtual machine contains its own virtual hardware including CPU, memory, hard disk, and network interface card, which look like physical hardware to the operating system and applications" [2]. Virtual machines or guest operating systems can be encapsulated and move from one physical host to another [3].

On a normally configured computer, the operating system detects and run processes as needed to use the different physical components of the equipment. On computers configured to run virtual machines, the host interacts with hardware through software called virtualization layer or hypervisor. The hypervisor provides the independence to virtual machines as well as the resources allocation [2], [4].

1.2 Advantages and disadvantages of using Virtual Machines

Advantages and disadvantages of using virtual machines instead of individually configured hosts are many, and it depends on the type of environment in which the virtual machines are created as well as the purpose of their use.

One of the most common motivations for companies to start using virtual machines is to improve their efficiency by using existing hardware as well as new one to create new virtual machines and use the physical capabilities of system as much as possible. Companies also benefit by using operating systems as needed by different applications: different virtual machines with different operating systems can run in the same computer and used as needed. Nowadays, people are also using virtual machines as a way to keep using legacy applications that are not compatible with newer hardware. This is becoming more common because of the use of web browser with different purposes [3].

More technical advantages can also be found on the use of virtual machines. Some of these are cited below [2], [5]:

- Easy provisioning and fast scalability: a base model of virtual machines can be created and from this all new virtual machines can be cloned. This offer homogeny and at the same time makes the process of creating new virtual machines easier and quick.
- Easy to relocate: virtual machines are a compilation of files that can be saved and move between different physical hosts. They are independent of the physical parts of the systems. As long as all needed files are saved, users will be able to start the virtual machine on a different host.
- Easy to manage: all virtual machines running on a single physical host do not know or detect the presence of the other virtual machines installed on the host. They are totally independent from each other. Also, if physical changes need to be done to the physical host, it does not affect the virtual machines. They are insulated from hardware changes. This said, if one virtual machine breaks, the other ones keep working without being affected by the failure.
- Provides the ability to support legacy applications: virtual machines can be created with different capabilities and hardware needs, this allows users to recreate the system based needed to run legacy applications.
- Allow servers to be consolidated: having the option to use a physical equipment to host more than one guest operating system benefits users in different ways like the use of hardware, space and resources. This capability makes it easier to recover from a disaster improving uptime and reducing recovery time.
-

The disadvantages of virtual machines are various, but it also depends on the environment on which they are being use and the purpose of their use. The NIST summarizes these disadvantages in the following paragraph:

"Full virtualization has some negative security implications. Virtualization adds layers of technology, which can increase the security management burden by necessitating additional security controls. Also, combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs. Further, some virtualization systems make it easy to share information between the systems; this convenience can turn out to be an attack vector if it is not carefully controlled. In some cases, virtualized environments are quite dynamic, which makes creating and maintaining the necessary security boundaries more complex" [3].

On high performance environments, virtualization is used for very specific cases. Some of these challenges are as follow [6]:

- Overhead: because of the privileged operations from all the virtual machines, the virtual machine monitor has to register all processes and request from each one. This disadvantage is mainly visible in environment where I/O operations are constant.
- Memory consumption: the physical memory available on the host is distributed between all virtual machines running on a physical host. If there are continuous operations, the memory needed for them might not be available.
- Efficiency: high performance environments need to have management software with which systems with low overhead can be shut down.

In environments where virtual machines are the main component and conform a red of available hosts, this is called a cluster. These environments have a specific number of physical hosts to support all the needed virtual machines. Here, the main disadvantage of using virtual machines is that one physical host holds two or more virtual host that are being used for different purposes, but that depend on the hardware of one physical host. In order to alleviate this problem, it is necessary to have redundancy. The redundancy should be physical and logical as well. If the virtual management software monitors that a host is having problems on running the virtual machines installed, it should be able to migrate those virtual machines to a different hosts without impacting the performance and up time of the environment. If downtime is needed, it has to be as lower as possible [7].

From the information presented above, we can say that the advantages and disadvantages of using virtual machines depend on the environment in which they are being used as well as the purposed of their use. One advantage that I believe has been left aside, and that to me is very important, is the use of virtual machines for educational purposes. Students do not need to have a totally hardware dedicated computer to learn and do basic procedures. When I was learning about different operating systems, it was very nice to know that I could just login to different virtual machines and I would be able to work on a totally different operating system. If I break one of them, creating a new virtual machine was easy and did not take more than few minutes. I believe that virtual machines are very helpful in the education field.

2. Security Vulnerabilities on Virtual Machines

Despite all the benefits offered by using virtual machines and their technology, these new capabilities have also raised issues related to security because of the implementation of virtualization. Specific characteristics of virtual machines and associated security issues are described as follows [8]:

- Scaling: it is easy to deploy virtual machines by cloning existing ones or even by using a base model. This characteristic needs security policies of the network to be flexible in order to handle the quick growth of host in the network.
- Transience: because virtual machines can be added and removed from the network, it can be hard to have a stable network infrastructure. If an infection is detected on a network, it is hard to ensure that all infected computers have been removed. Also, if the infection was identified and vulnerable computers were patch for protections, it is possible that new virtual machines do not have the patch and are still vulnerable and restart the infection process.

- Software lifecycle: because virtual machines can be restored to different checkpoints, this can cause that an updated virtual machine with protection against actual vulnerabilities loses it by being restored to a previous checkpoint.
- Diversity: in companies where usually the same image is used for all systems. If one virtual machine is successfully attacked, all of them can be affecting by using the same process.
- Mobility: virtual machines are composed by different files that can be saved and installed on different hosts. When this is done, it is assumed that all other hosts where that virtual machine has been installed are protected and that have are no danger to the network.
- Identity: this is usually associated to the MAC address on physical hosts, since virtual machines can be moved from host to host, it is difficult to keep track or associate them to a specific physical host.

The NIST lists three main ways to improve security on virtual environments. These are basic actions that can protect systems. They are [3], [10]:

- Secure all elements of a full virtualization solution and maintain their security.
  It is important for organization which environments are virtualized to secure all the physical components as well as the logical ones. Keeping software up-to-date with security patches, using secure configuration baselines, and using host-based firewalls, antivirus software, or other appropriate mechanisms to detect and stop attacks is vital on having a secure infrastructure. Companies should have the same level of protection for all environments, physical or virtual.
- Restrict and protect administrator access to the virtualization solution.
  Access to the virtualization management system should be restricted to authorized administrators only. Some virtualization products offer multiple ways to manage hypervisors, so organizations should secure each management interface, whether locally of these actions, or remotely accessible.
- Ensure that the hypervisor is properly secured.
  The hypervisor software should be protected as any other software like updates, but it also needs to have physical security. On virtualizations, it is important to disable any piece of hardware that is not being used for any of the virtual machines running on the physical host.
- Carefully plan the security for a full virtualization solution before installing, configuring, and deploying it.
  As in any new environment implementation, planning plays a very important role when transforming physical environments to virtual. It will help to make sure all resources are being used and that the virtual machines work as expected.

3. **Security Tools on Virtual machines**

Because of the specification on the virtual machines, there are some tools developed in order to offer better security option for users of virtual machines. These options are [9]:

- VM-Based Intrusion Detection Systems
  This is developed on based to three virtual machine capabilities: isolation, inspection, and interposition. Example of this are:
  1. Livewire which enforces security policies on guest virtual machines. It has two main components: the OS Interface Library, and the Policy Engine.
     The OS Interface Library provides an OS-level view of the target virtual machine by interpreting the hardware state on the VMM. This component is important because VMMs manage state strictly at the hardware level.

The policy engine is the heart of Livewire. This component obtains events from the VMM interface and the OS Interface Library, and decides whether or not the system has been compromised

2. Siren helps to detect malicious software operating within a guest virtual machine that is trying to send packets over to other hosts on the network.

- VM-Based Intrusion Prevention Systems
  This type of systems purpose is to protect virtual machines from attackers. Example of this are:
  1. SVFS is a secure virtual file system that protects important files even when the operating system is infected. When suspected software runs, SVFS makes a copy of shared files on the host in order to protect it from disruptive activities.
  2. NetTop bases its operation on the isolation property of virtual machines. NetTop runs two dedicated virtual machines, one to perform encryption using IPSec, and one filtering router machine. These two VMs enforce strict security policies that prevent network traffic from flowing between networks of different classifications.
  3. IntroVirt uses virtual-machine introspection to monitor application and operating system execution in a guest virtual machine.
  4. sHype mediates access to hardware resources at a low level eliminating the need to have multiple implementations for different operating systems. The downside of the SHype solution is that it cannot do anything to prevent resource starvation within a virtual machine.

- VM-Based Honeypots
  Virtual machines provide resource multiplexing, which allows more high interaction honeypots to run on the same hardware. Virtual machine technology makes it feasible to deploy more high-interaction honeypots on the same hardware. Furthermore, virtual machine technology allows more in-depth monitoring of malicious activities on honeypot machines without attackers being able to detect or disable monitoring software. Examples of honeypots are the Potemkin Virtual Honey farm and the Collapsar Honeypot Center.

- Terra: A Virtual Machine Based Trusted Computing Platform
  It uses a trusted virtual machine monitor (TVMM) to partition resources between isolated virtual machines (VM), thus providing the appearance of a dedicated physical machine for each Virtual Machine.

- ReVirt: A VM-Based Logging and Replaying System
  It is a virtual machine based logging and replaying system that attempts to address the lack of integrity and completeness provided by traditional loggers.

- SubVirt: VM-Based Malicious Software
  It poses significant challenges for designers of anti-malware protection programs. It exploits the isolation properties of virtual machines to achieve a new level of separation from the target operating system, making it very difficult to detect and remove.

4. **Conclusion**

Virtual machines offer a lot of benefits to us, but at the same time there are security considerations that need to be addressed in order to keep environments safe and the stable. As expressed in the paper, one of the great benefits of virtual machines that I considered is the help they can offer to formal education establishments. In this situation, and since the use for of them is very basic, security is not an important fact. When I used them, all virtual machines were in a totally different network in order to avoid any danger that affects the main

network or other physical hosts. In this case I believe the security level was enough.

In any other instance, it is important that users protect virtual machines as they will protect any physical computer. Even though it is easy to replace one virtual machine with another, there can be consequences associated to the fact that security was not done right. The paper presented different options in which virtual machines can be protected, so it is up to the IT specialists to decide which ways is the best to protect the environment.

References

[1] Gupta, D, et. al. Difference Engine: Harnessing Memory Redundancy in Virtual Machines. *In Proceedings of the 8th USENIX Symposium on Operating Systems Design and Implementation, 2009.* . Retrieved on November, 2013 from *https://www.usenix.org/legacy/event/osdi08/tech/full_papers/gupta/gupta.pdf*

[2] VMware Education Services. VMware vSphere: Install, Configure, Manage. Lecture Manual – Volume 1. VMware, Inc., 2012.

[3] Scarfone K., et al. Guide to Security for Full Virtualization. NIST Special Publication 800-125 Technologies. Recommendations of the National Institute of Standards and Technology. Retrieved on November, 2013 from http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

[4] WMware, Inc. VMware Server Virtual Machine Guide. Retrieved on November, 2013 from http://www.vmware.com/pdf/server_vm_manual.pdf

[5] Clark, C., et al. Keir Fraser, Steven Hand, Jacob Gorm Hanseny. Live Migration of Virtual Machines. University of Copenhagen, Denmark. Retrieved on November, 2013 from http://www.cl.cam.ac.uk/research/srg/netos/papers/2005-migration-nsdi-pre.pdf

[6] Huang, W., et al. A Case for High Performance Computing with Virtual Machines. Retrieved on November, 2013 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.7050&rep=rep1&type=pdf

[7] Le, M., et al. Resilient Virtual Clusters. *Proceedings of 17th IEEE Pacific Rim International Symposium on Dependable Computing. Pasadena, California, December 2011.* Retrieved on November, 2013 from http://www.cs.ucla.edu/~tamir/papers/prdc11.pdf

[8] Garfinkel, T., & Rosenblum, M. When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Retrieved on November, 2013 from https://www.usenix.org/legacy/event/hotos05/final_papers/full_papers/garfinkel/garfinkel.pdf

[9] Zhao, X., et al. Virtual Machine Security Systems. Department of EECS. University of Michigan. Retrieved on November, 2013 from http://courses.cs.vt.edu/~cs5204/fall07-kafura/Papers/Virtualization/VMM-Security.pdf

[10] Studnia, I., et al. Survey of Security Problems in Cloud Computing Virtual Machines. Retrieved on November, 2013 from http://hal.inria.fr/docs/00/76/12/06/PDF/cesar_paper71-version_publieI_e.pdf