Virtual Machine

Simmy Agarwal, Rekha
Dronacharya College of Engineering

Abstract: **Virtualization plays a major role in helping the organ. This paper presents a literature study on various security issues in virtualization technologies. Our study focus mainly on some open security vulnerabilities that virtualization brings to the environment. We concentrate on security issues that are unique for virtual machines. The security threats presented here are common to all the virtualization technologies available in the market; they are not specific to a single virtualization technology. We provide an overview of various virtualization technologies available in the market at the first place together with some security benefits that comes together with virtualization. Finally we provide a detailed discussion of several security holes in the virtualized environment.**

I. INTRODUCTION

The concept of virtual machines is not new to the computer world, it is however a concept that not many people know about or understand. If you are a typical computer user and you use the Internet to browse the World Wide Web, then you have probably interacted with a virtual machine.

Virtual machines are a concept that is used quite often in the computing world to solve very important problems, but often these are transparent to you as the user because virtual machines are typically used within programs and operating systems that users use every day. Some of these problems include: sharing the same hardware among many programs by partitioning the hardware, allowing software to be "portable" between various operating systems, as well as running older software on a newer computer. All of these uses of virtual machines are very important to the way that we compute today.
As you read on, we will attempt to show you how virtual machines help to solve these important problems, and therefore why they are an important piece of computers today. In defining the term virtual, we have used the term 'simulation'. A simulation is something that imitates something else. A good example of a modern day application of a simulation is used in the training of Air Force and Marine pilots. Pilots are trained on flight simulators; computer based machines that look like the cockpit of a jet plane. This machine gives the pilot the look and feel of actually flying a real jet plane, without ever having to leave the ground. This simulator imitates everything from the actual maneuverability of the plane, to the effect of wind and weather conditions on flying the plane. In essence, the simulator allows the pilot to have all of the facilities and feelings of flying a real jet plane from the safety of the ground.

This concept of simulation or imitating another object has been carried over into the design of computer systems. Although there are many incarnations of virtual machines, at it's most basic, a virtual machine is the appearance of a machine that is not actually there.

II. BACKGROUND

Virtualization was first developed in 1960's by IBM Cor-poration, originally to partition large mainframe computer into several logical instances and to run on single physi-cal mainframe hardware as the host. This feature was in-vented because maintaining the larger mainframe computers became cumbersome. The scientist realized that this capa-bility of partitioning allows multiple processes and applications to run at the same time, thus increasing the efficiency of the environment and decreasing the maintainance over-head. By day to day development, virtualization technologies has rapidly attains popularity in computing, in fact it is now proven to be a fundamental building block for today's computing.

Although the main focus of this paper is to provide

an overview of security vulnerabilities in a virtual environment. It is worth mentioning some of the security benefits that comes together with virtualization.

Two primary benefits offered by any virtualization technology are 1.Resource sharing and 2.Isolation. Resource sharing Unlike in non-virtualized environment where all the resources are dedicated to the running programs, in virtualized environment the VMs shares the physical resources such as memory, disk and network devices of the underlying host. The resources are allocated to the virtual machine on request. Hypervisors plays a significant role in resource allocation.

Isolation - One of the key issue in virtualization, provides isolation between virtual machines that are running on the same physical hardware. Programs running in one virtual machine cannot see programs running in another virtual ma-chine. This is contrast to non-virtual environment where the running programs can see each other and if allowed can com-municate with each other.

Virtualization provides a facility of restoring a clean non infected environment even the underlying system is infected by malicious programs. Since, Virtualization provides an isolated environment this can be used for debugging malicious programs. and also to test new applications.

Virtualization can be done in several ways. There are var-ious virtualization technologies available in the market that helps to virtualize the environment. Depending on the needs and goals of the organization, one virtualization technology is better than the other. This section gives an overview of some of the existing virtualization technologies.

Before going into the details of different virtualization technologies, Fig. 1 gives a basic idea of a virtual machine environment.

there are two virtual machines running on top of a physical computer possessing their own operating sys-tem and applications. Every guest machines appears to be an independent computer for their running processes. As already mentioned, Hypervisor layer is the host software layer that provides the ability to run multiple operating system on a physical hardware. It sits between the host physical hardware and the guest machines.

III. FULL VIRTUALIZATION

In this approach the hypervisor simulates several logical instances of completely independent virtual computers possessing its own virtual resources. These virtual resources included IO ports and DMA channels. Therefore, each virtual machine can run any operating system supported by the underlying hardware. Besides the fact, that this is the most commonly used virtualization technology, true full virtualization where the virtual processors have to reproduce the CPU operations of the host machine is hard to achieve. Moreover, the overhead of handling these CPU operations makes true full virtualization difficult to manage. However the virtual machine environment that provides "enough representation of the underlying hardware to allow guest operating systems to run without modification can be considered to provide "Full Virtualization.

In this kind of setup the I/O devices are allotted to the guest machines by imitating the physical devices in the virtual machine monitor; interacting with these devices in the virtual environment are then directed to the real physical de-vices either by the host operating system driver or by the "hypervisor driver

Security vulnerabilities in virtualization

Most of security flaws identified in a virtual machine environment are very similar to the security flaws associated with any physical system. The following are some general flaws that are unique to the virtual environment.

Communication Between VMs and host

One of the primary benefits that virtualization bring is isolation. This benefit, if not carefully deployed become a threat to the environment. Isolation should be carefully configured and maintained in a virtual environment to ensure that the applications running in one VM don’t have access to the applications

running in another VM. Isolation should be strongly maintained that break-in into one virtual machine should not provide access either to virtual machines in the same environment or to the underlying host machine.

Shared clipboard in virtual machine is a useful feature that allows data to be transferred between VMs and the host. But this useful feature can also be treated as a gateway for transferring data between cooperating malicious program in VMs

In some VM technologies, the VM layer is able to log keystrokes and screen updates across the virtual terminals, provided that the host operating system kernel has given necessary permission. These captured logs are stored out in the host, which creates an opportunity to the host to monitor even the logs of encrypted terminal connections inside the VMs.

Some virtualization avoids isolation, in order to support applications designed for one operating system to be operated on another operating system, this solution completely exploits the security bearers in both the operating systems. This kind of system, where there is no isolation between the host and the VMs gives the virtual machines an unlimited ac-cess to the host's resources, such as file system and networking devices. In which case the host's file system becomes vulnerable.

Guest-to-Guest attack

It is important to prevent the host machine than the individual VMs. If an attacker gains the administrator privileges of the hardware then its likely that the attacker can break-in into the virtual machines. It is termed as guest-to-guest attack because the attacker can able to hop from one virtual machine to another virtual machine provided that the underlying security framework is already broken.

IV. SUMMARY

The paper has presented some of the security flaws in the virtual machine environment. Some of the threats presented here may be considered as benefits in some situations, but they are presented here so that proper care should be taken while designing and implementing the virtual environment.

Virtualization brings very little added security to the en-vironment. One of the key issue is that everyone should be aware of the fact that virtual machines represent the logical instance of an underlying system. So many of the traditional computer threats apply the same to the virtual machines also. Another issue that makes the security consequences difficult to understand is that, there are so many different types of virtualization technologies available in the market. Each of it has it own merits and demerits, each virtualization deploy-ment is different depending on the need for the virtualiza-tion. It is common that any single virtualization technology will not provide shield to all the security issues arise. How-ever, the key to create a good virtualization environment is to study carefully the environment that is to be virtualized, the needs and goals of the organization, and taking into con-sideration all the possible security issues that puts the virtual machines at risk. Finally carefully design the virtual envi-ronment with the help of correct virtualization technology that matches the goals.