Resolving Security Issues in the Virtual Machine File System

Achal Sancheti
Master of Science in Information Systems,
Northeastern University
achalsancheti@gmail.com

Abstract - Security is an evolving domain of computer security, network security, cloud security and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of the system. The physical machines are logically divided into virtual machines and virtual machines are rapidly replacing physical machine infrastructures for their abilities to emulate hardware environments, share hardware resources, and utilize a variety of operating systems. Its security becomes more important. This paper focuses on the security issues that are still to be overcome in Virtual Machine File System and Network File System.

Keywords – Virtualisation, Security, integrity, cloud computing, virtual machine, VMFS, hyper jacking.

1. Introduction

Organisations today are increasingly looking towards cloud computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. [1]

Virtualisation: Virtualisation means to hide the physical characteristics of the computing resources. The virtual machines can be created by VMware. VMware enables users to set up one or more virtual machines on a single physical machine, and use them simultaneously along with the actual machine.

The term virtualization has become somewhat of a buzzword, and as a result the term is now associated with a number of computing technologies including the following:

Storage virtualization: The amalgamation of multiple network storage devices into what appears to be a single storage unit.

Server virtualization: The partitioning a physical server into smaller virtual servers.

Operating system-level virtualization: A type of server virtualization technology which works at the operating system (kernel) layer.

Network virtualization: Using network resources through a logical segmentation of a single physical network.

Application virtualization: Application virtualization is layered on top of other virtualization technologies, such as storage virtualization or machine virtualization to allow computing resources to be distributed dynamically in real time. [2] There are different types of files like text file (.doc, .pdf), log file, bios file, image file, etc but here the security issue of virtual machine file system (vmfs) and network file system (nfs) is the primary concern.

VMFS: VMware Virtual Machine File System (VMware VMFS) is a virtual machine file system used in VMware ESX Server software to store files in a virtualized environment. VMWare VMFS was designed to store files, images and screen shots within a virtual machine. Multiple virtual machines can share a single virtual machine file system. Its storage capacity can be increased by spanning multiple VMFS. This file system is not mandatory and is therefore not installed with every virtual machine

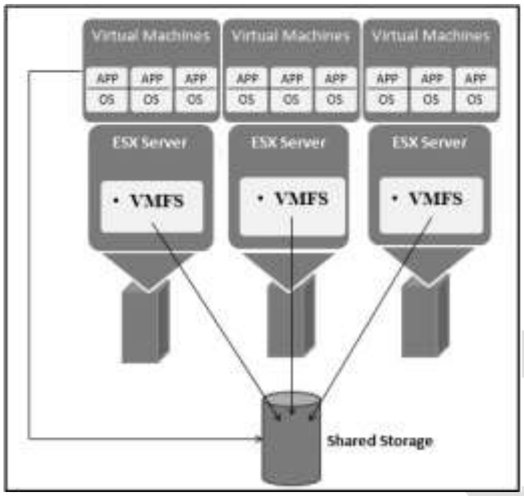

Figure1.1: Architecture of VMFS

VMware VMFS manages the creation, allocation and management of virtualized storage for all the different sets of virtual machines and servers created using VMware's set of tools and technologies. VMware VMFS is also known as VMFS vStorage.

The following are the **key features** of VMFS:

- It simplifies the storage issues of virtual machines as multiple virtual machines installed over different ESX servers can share a single shared storage area.
- Multiple instances of an ESX server run simultaneously and share VMFS.
- VMFS strongly supports the distributed infrastructure of virtualization by using various VMware services. [3]

2. Problem Domain

Cloud is totally depending on virtualisation of computing devices, network, applications and storage devices. Cloud services should ensure data integrity and provide trust to the user privacy. Data or file integrity means the accuracy and consistency of the data /file without being any alteration of those data/files. Security is the protection of systems and the data that they store or access. System security is the application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.

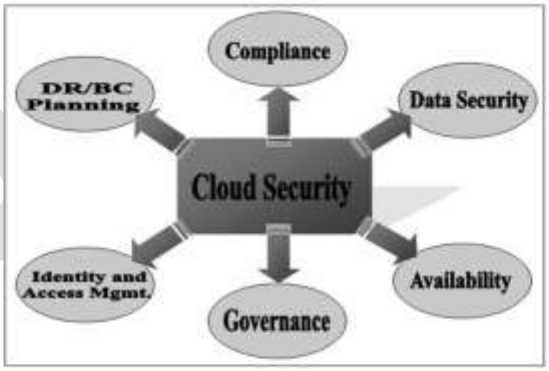

Figure 2.1 Factors of cloud security

Like physical machines, VMs are vulnerable to theft and denial of service attacks. The contents of the virtual disk for each virtual machine are usually stored as a file, which can be run by hypervisors on other machines, allowing attackers to copy the virtual disk and gain unrestricted access to the digital contents of the virtual machine. Virtual machines are inherently not physical, which means their theft can take place without physical theft of the host machine.

The second danger of virtual disks is that the attacker could corrupt or externally modify the file while the VM is offline. This means the integrity of an offline VM may be compromised if the host is not securely protected. [4]

The problems with the existing system are:

- Integrity of the system
- Hyper jacking

2.1 Hyper jacking

Hyper jacking is an attack which takes control over the Hypervisor that creates the virtual environment within a VM Host. It is a critical threat to the security of every virtualized environment. Hyper jacking involves installing a rogue hypervisor that can take complete control of a server. Gaining control of the hypervisor the attacker can control everything running on the machine and may spoil the integrity of the system. [5]

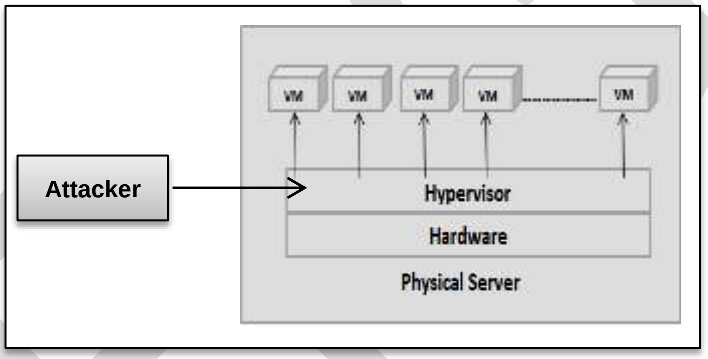

Figure 2.1.1 Process of hyperjaking

3. Proposed Solution: Flow Chart

Today security risks to cloud computing are active, including privacy, trust, data location, security policy and security threats and attacks. The virtual files on these virtual storages are prone to these risks. In order to deal with them, many security features are present which provide Data Integrity, Non-Repudiation, Encryption but somewhere lacks to provide higher levels of Authentication and Confidentiality. Finally, a multi-layered architecture is being proposed to assist the users for their satisfaction when choosing cloud delivery services.

Majority of cloud service providers store customers' data on large data centres. Although cloud service providers say that data stored is secure and safe in the cloud, customers' data may be damaged during transition operations from or to the cloud storage provider. In fact, when multiple clients use cloud storage or when multiple devices are synchronized by one user, data corruption may happen.

All data on the network need to be secured. [6]

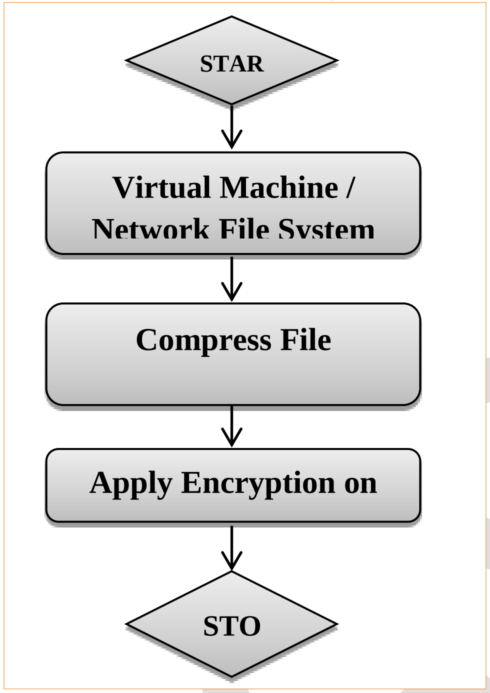

Figure 3.1: Flow of System

Let the file in the VMFS and NFS format has been saved by the registered organization on the cloud box. The authorized user may have only access to these files of the particular organisation. It is dependent on the user whether to encrypt these file and then save or save only in compressed format. The encrypted file may be decrypted by only the user who is authorized to access these files. In this way, this flow continues to provide a secured environment in cloud and to maintain the file integrity.

4. Application Domain

VMware, VCloud, Networking and Security Edge deliver an operationally efficient, simple and cost-effective security services gateway to secure the perimeter of virtual data centre.
The solution's virtual security appliance delivers gateway services such as firewall/NAT, load balancer, VPN and DHCP and is fully integrated with VMware.

- Easily support multi-tenant IT environments.
- Safely share network resources by creating logical security zones that provide complete network isolation for virtual systems.
- Enable role-based access control and separation of duties as part of a unified framework for managing virtualization security. [7]

5. Conclusion

Security includes the integrity and confidentiality. Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes. The proposed algorithm will prove to be beneficial in the context of resolving the security related issues in the system. This system is expected to be secured. Integrity of data and files will be maintained of the system.

REFERENCES:

1. 'About file integrity in cloud computing' at "http://www.academia.edu/1475574/Ensuring_Data_Integrity_in_Cloud_Computing_-_EICA272" accessed on 06/04/2015.
2. 'Virtualization' at "www.webopedia.com/TERM/V/virtualization.html" accessed on 24/03/2015.
3. 'Virtual machine file system' at "www.techopedia.com/definition/16827/vmware-virtual-machine-file-system-vmwarevmfs" accessed at 24/03/2015.

4. ‘Attacks on Virtual machine’ available at “http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html” accessed on 17/08/14.
5. ‘Hyperjacking’ at “itsecurity.telelink.com/hyperjacking/” accessed on 24/03/2015
6. ‘Security in cloud computing’ available at “http://cloudtweaks.com/2014/07/computing-security-network-application-levels/” accessed on 18/08/14.
7. ‘Application of cloud security’ available at “http://www.vmware.com/cloud-security-compliance/cloud-security#sthash.ZlPNsEsd.dpuf” accessed on 20/08/14