Implementing Security on virtualized network storage environment

Benard O. Osero, David G. Mwathi
Chuka University
bosero@chuka.ac.ke
dgmwathi@chuka.ac.ke

Abstract
This paper presents a literature study on various security issues in virtualization technologies. Our study focus mainly on some security vulnerabilities that virtualization brings to the virtualized and open environment. We delve into security issues that are unique for Network attached disks. 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 come together with virtualization. Finally we provide a detailed discussion of virtualization model running on a virtualized environment where a client machine interacts with a virtualized file server to directly access a file from storage area network (SAN).

KEYWORDS: Virtualization, Security, Threats, Virtual Secure Storage Management (VISSM).

1.0 Introduction

Virtualization was first developed in 1960's by IBM Corporation, originally to partition large mainframe computer into several logical instances and to run on single physical mainframe hardware as the host. This feature was invented because maintaining the larger mainframe computers became cumbersome. The scientists realized that this capability of partitioning allows multiple processes and applications to run at the same time, thus increasing the efficiency of the environment and decreasing the maintenance overhead. By day to day development, virtualization technologies have rapidly attains popularity in computing; in fact it is now proven to be a fundamental building block for today's computing [5].

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 come together with virtualization. Two primary benefits offered by any virtualization technology are resource sharing and Isolation. With 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 issues 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 machine. This is contrast to non-virtual environment where the running programs can see each other and if allowed can communicate 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 [7].

EXISTING VIRTUALISATION TECHNOLOGIES

Virtualization can be done in several ways. There are various virtualization technologies available in the market that helps to virtualize the environment. Depending on the needs and goals of the organization, no 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 system 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. Figure 1: Overview of a virtual machine environment that provides the ability to run multiple operating systems on a physical hardware. It sits between the host physical hardware and the guest machines.

Virtualization is a technology that has an enormous effect in today's IT world. It is a technique that divides a physical computer into several parts or completely isolated machines commonly known as virtual machines (VM) or guest machines. In today's modern computer architectures, virtualization exists in almost every layer, from the application to the operating system, server, networks, and storage devices. For example, application clustering technologies such as Microsoft Clusters and Oracle's Real Application Clusters (RAC) manage the process of selecting a server to deliver an application without the user knowing which server it's coming from. Server virtualization allows you to run multiple operating systems on the same physical hardware platform to improve utilization of the central processing unit (CPU) and memory. Most of these form of virtualization work together to optimize efficiency throughout the layers of technology.

2.0 Related Work

2.1 Storage virtualization

Modern storage virtualization technologies pool heterogeneous storage vendor products together in a specific way to provide advanced features such as non-disruptive migration of data and thin provisioning. This level of abstraction can be implemented in three layers of the infrastructure, in the server, in the storage network, and in the storage controller. Storage virtualization is a form of Resource virtualization, where a logical storage is created by abstracting all the physical storage resources that are scattered over the network. First the physical storage resources are aggregated to form a storage pool which then forms the logical storage. This logical storage which is the aggregation of scattered physical resources appear to be a single monolithic storage device to the user [6].The computer that is being virtualized is of no difference from the computer that is not virtualized. The virtualized environment is vulnerable to all the traditional attacks and exploits that are common to the normal environment. The case is even worse in the virtualized environment, where there are several virtual computers running. The security expectations are higher here because "there are more systems to protect", more possible points of entry, more holes to patch and there are more interconnection points in the virtualized environment [3]. Attackers and Hackers have already been actively developing new malware programs for virtual machine environment. "Root kit infections, malware that detects a virtual environment and modifies itself accordingly"[3], [8] are some of them. "Low-level hypervisor attacks, and deployment of malicious virtual systems" [3] are few possible attacks that are unique to this environment. On the other hand new security protection programs are also emerging in the market every now and then from different vendors, but most of these security solutions are mainly focused on hypervisor. Since hypervisor is a new layer between the host's OS and virtual environment, it creates new opportunities for the malicious programs. And more over, hypervisor is basically a software program, so it has all the traditional software bugs and the security vulnerabilities as any software have. One of such product that hits the market recently is SHype [3], a new secure hypervisor that binds security policies to the virtual environment. A good debate on recent security solutions can be found on [1].However, virtual machine security is more than just deploying a secure hypervisor to the environment. Virtualization technologies are still evolving. Newer versions with added features are introduced before the security consequence of the older version has been fully studied. This work analyzes the general security threats in a virtual environment and suggests possible solutions for some specific model for virtual/ cloud environment. Understanding of virtualization technologies greatly helps to understand the security consequences that occur in the environment.

In virtual machine architecture the guest machines and the underlying host share the physical resources such as CPU, memory disk, and network resource. So it is possible for a guest to impose a denial of service attack to other guests residing in the same system. Denial of service attack in virtual environment can be described as an attack when a

guest machine takes all the possible resources of the system. Hence, the system denies the service to other guests that are making request for resources; this is because there is no resource available for other guests.
The best approach to prevent a guest consuming all the resources is to limit the resources allocated to the guests. Current virtualization technologies offer a mechanism to limit the resources allocated to each guest machines in the environment. Therefore the underlying virtualization technology should be properly configured, which can then prevent one guest consuming all the available resources, thereby preventing the denial of service attack [6].

2.2 Hardware support virtualization

This approach has recently gains attention when Intel and AMD released their processors with inbuilt hardware which supports virtualization. The hardware support virtualization architecture creates a trusted "root mode" and an un trusted "non-root mode". The hypervisor resides in the root mode whereas all the guest operating systems reside in the non-root mode. Hypervisor is responsible for resource allocation and I/O device interaction. Since the hypervisor reside in the root mode the guest operating systems calls out for the hypervisor in order to process their requests for resources by means of a special virtualization instruction known as hypercalls [7].

2.3 Resource virtualization

Virtualizing system specific resources such as "storage volumes, name spaces and the network resources "[2] is known as resource virtualization. There are various approaches to perform resource virtualization. Some of them are [6]

- Aggregating many individual components into larger resource pool
- Grid computing or computer clusters where multiple discrete computers are combined to form a large supercomputers with enormous resources
- partitioning a single resource such as disk space into number of smaller and easily accessible resources of same type

2.4 Storage virtualization vulnerabilities

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 worst case, it is used to "exfiltrate data to/from the host operating system"[4].

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 access to the host's resources, such as file system and networking devices. In which case the host's file system becomes vulnerable [4].

Isolation plays a vital role in virtualization. It is considered as a threat when one VM without any difficult may be allowed to monitor resources of another VM. Thanks to today's modern CPUs, which comes with a built in memory protection feature. The hypervisor who is responsible for memory isolation can make use of this feature; this memory protection feature prevents one VM seeing the other VM's memory resources. More over the VMs do not have the possibility to directly access the file system of the host machine, so it is impossible for a VM to access the virtual disk

allocated to another VM on the host. When it comes to the network traffic, isolation completely depends on the connection (network) setup of the virtualized environment. If the host machine is connected to the guest machine by means of physical dedicated channel, then it's unlikely that the guest machine can sniff packets to the host and vice versa. However in reality the VMs are linked to the host machine by means "virtual hub" or by a virtual switch. In which case, it enables the guest machines to sniff packets in the network or even worse that the guest machines can use ARP poisoning to redirect the packets going to and coming from another guest [5].Authenticating the network traffic could be a solution the problem described above.

2.5 Security Challenges.

1) Unauthorized access to data in the disk storage by the user is highly likely if the system is not protected by use of usernames and passwords.
2) If the client session to the file server is not limited then when a valid client has finished requesting data from disk and probably forget to log off a malicious client may easily gain access to the storage disks and download data.
3) There is a very high likelihood that a client might have copied the URL enabling him to access the data path to the storage disks without necessarily authenticating himself.
4) Physical security may be compromised. For example, unhappy employees may take advantage of their "inside" status to destroy critical data before being fired, or may modify personnel records for personal gain.

3.0 Research Methodology

This paper is a literature survey that analyzes various issues concerning security in virtualized environment. The security architecture discussed in this paper employs cryptographic capabilities issued by the file manager and checked by drives with minimal hardware support. The separation between issuing and verifying capabilities enables the separation of file storage from file management —they may be done by machines separated by distance and with only indirect communication. Access rights control is managed through the cryptographic information stored in the capabilities.

3. 1 VIRTUAL ENVIRONMENT ARCHTECTURE

Virtualized environment design and development

A virtualized environment was developed using SUN xVM Virtual box and Opensolaris. The design was preceded by an intensive literature review on work already done in virtualization. The conceptual design as seen in figure 3.1 was implemented and tested [9].

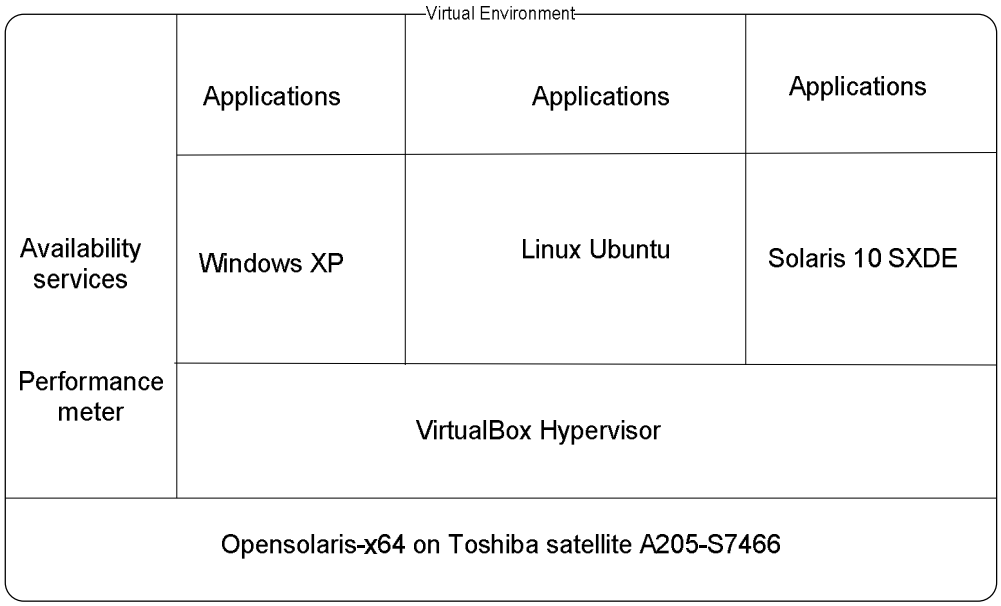

Fig 1.0: designed virtual environment [9]

Instead of using Solaris and Linux Ubuntu our Vmodel environment was implemented on the windows XP platform.

The steps involved in the design and implementation of the virtualized environment were:

- literature review and related work study;
- Windows XP installation on the test laptop;
- Configuration of the operating system networking and missing device drivers;
- Installation of the Virtualbox hypervisor;
- Setup of virtual computers on the hypervisor and resource allocation;
- Installation of operating systems in the virtual computers;
- Setup of networking on the virtual computers.

The above approach for virtualization was taken because Virtual box is an open source hypervisor that has strong support in the open source community through discussion lists, code contributions and elaborate documentation.

3.2 Virtualized Secure Scalable Storage Design

The model proposed is based on storage virtualization and operating system virtualization. The virtualized storage units are deployed in a virtualization infrastructure such as VMWare or Virtual Box. The file manager is logically divided into virtual disks that are deployed in the main operating system. The clients communicate to the virtualized storage units using the TCP/IP protocol on the network layer. The diagram below summarizes the proposed model.

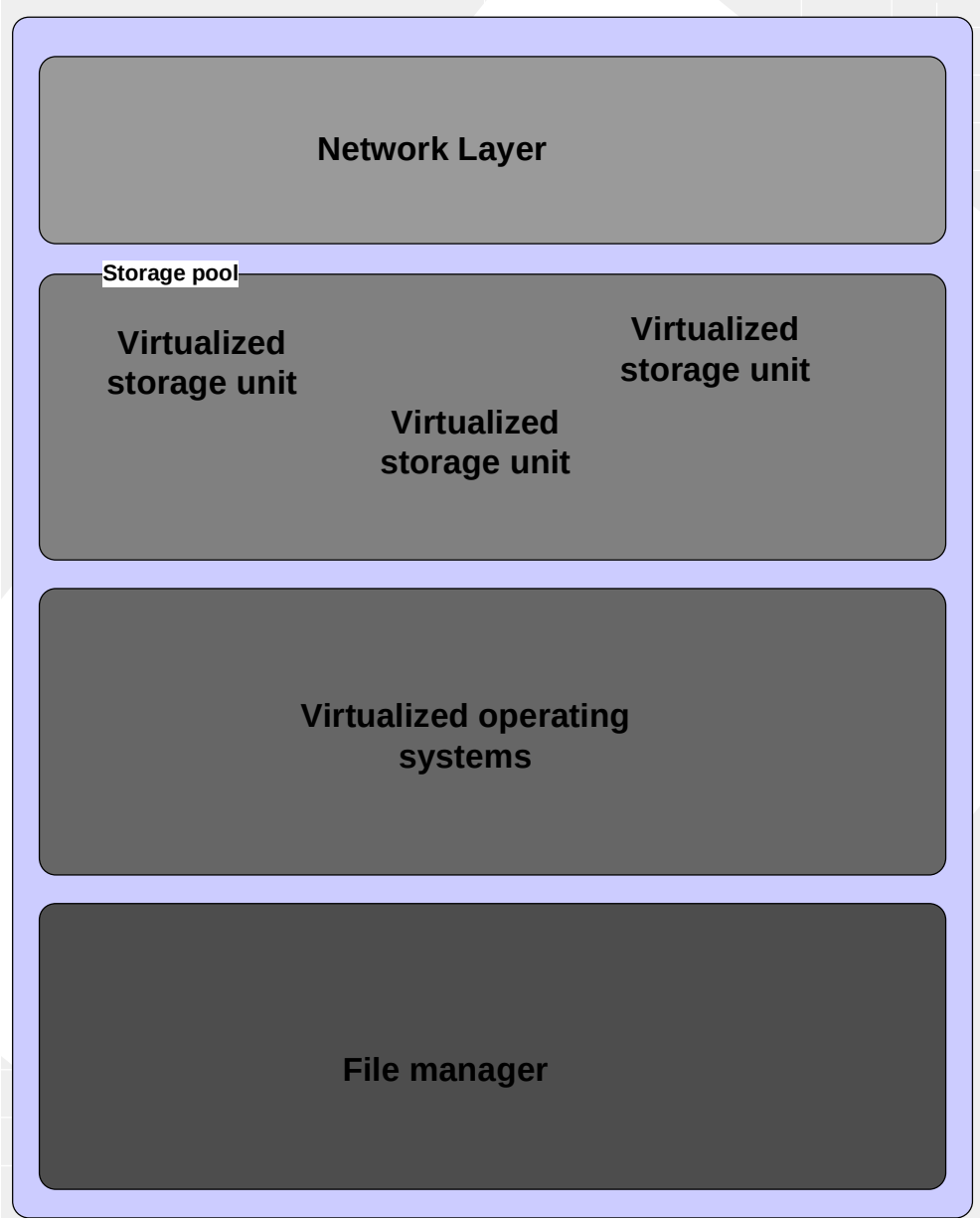

Fig 2.0: system model

3.3 SECURITY LAYER DESIGN

The security architecture discussed in this paper employs cryptographic capabilities issued by the file manager and checked by drives with minimal hardware support. It was run and tested on a model called VISSM.

The figure below illustrates a detailed design layout of a virtual secured system

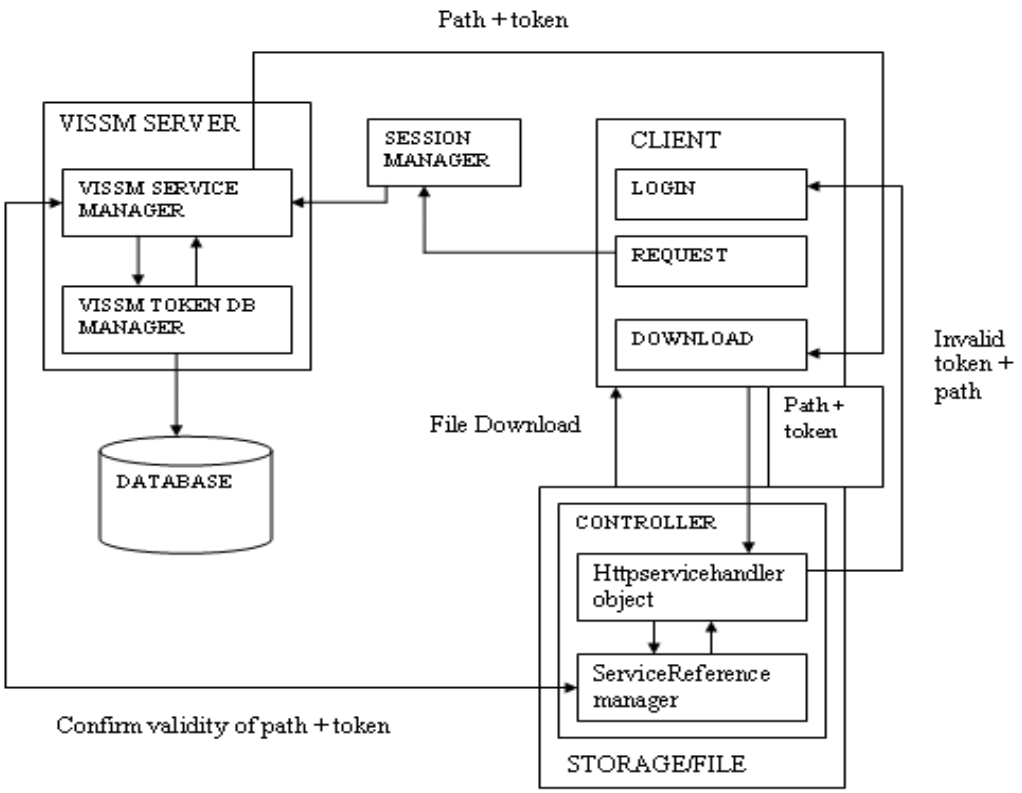

Fig 3.0 showing a VISSM system

Fig 2.4 above is a communication between the file server and the client. The user first log into the web server client interface and then will be prompted to select the file to be downloaded from a list of files provided if he successfully logs in. If the file requested for is valid then the request hits the server and the server generates a time-stamped time-limited token appended with the file location storage path, this is handled by the file server section called VISSM SERVICE MANAGER Object. Then on receiving the token the VISSM TOKEN MANAGER object is tasked with the responsibility of updating the database on the date and time the token was issued. Then the client receives the token and the path to the file location, as a download event leading the client to the remote controller in the file storage disks, where the client can download the file as many time as possible as long as it remains valid. At this point the **Http-service-handler** object is invoked and receives the request capability presented by the client, on receiving this capability (the path and token), it forwards it to a SERVICE REFERENCE MANAGER object which subsequently forwards the issued token and path back to VISSM TOKEN MANAGER object whose sole work is to check the validity of the token and return VALID/INVALID to the SERVICE REFERENCE MANAGER. If the token has expired INVALID is returned and the **Http service handler** Object forces the client to login in afresh, otherwise if the token is marked as VALID then the client will be allowed to DOWNLOAD the file directly without involving the file server.

The security goal in VISSM model is to:

(i)Protect the integrity and confidentiality of communication involving network attached storage and the clients.

(ii)Deliver the scalability and aggregate bandwidth potential of the VISSM architecture.

The separation between issuing and verifying capabilities enables the separation of file storage from file management —they may be done by machines separated by distance and with only indirect communication. Access rights control is managed through the cryptographic information stored in the security capabilities.

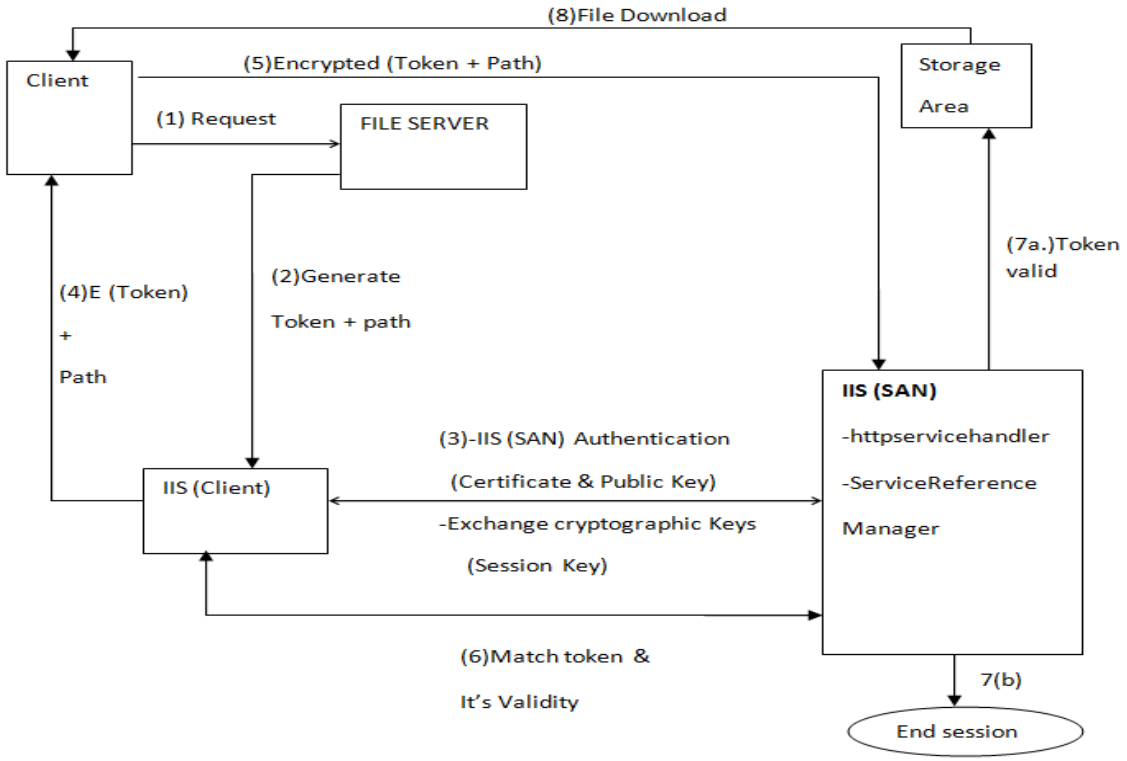

Fig 4.0 SSL control flow diagram

Secure sockets layers (SSL) allow encryption of the data and provide a secure communication link between the client and the server. This technology is provided by the IIS security implementation framework; for the VISSM technology to be effective two IIS servers are used, first one residing in the storage area for encrypting the data and the token and the second one residing in the client side for decrypting the token and storage path provided by the File server. The framework works as follows;

(1) Client requests for a file.

(2) The FILE SERVER generates a token + path is passed to the IIS client.

(3) The client IIS (IIS (client) and storage area IIS (IIS (SAN) initiate a session. The IIS (SAN) sends out its public key and the certificate. The client IIS then checks three things from the certificate; that the certificate comes

from a trusted party, that the certificate is currently valid, and that the certificate has a relationship with the site from which it's coming. The IIS (client) then generates a randomly selected symmetric key, encrypts it with the public key of the IIS (SAN) and sends the symmetric key to it IIS (SAN). The two systems can then communicate using symmetric-key encryption. Once the session is finished, each IIS server discards the symmetric key used for that session. Any additional sessions require that a new symmetric key be created, and the process is repeated.

(4) IIS (Client) encrypts the token using the session key generated in (3) above. The encrypted token together with the path E (Token + path) is passed to the client application.

(5) Client passes Encrypted (Token +path) to the IIS (SAN)

(6) IIS (SAN) confirms validity of the token

(7a) If token is valid the storage area network is allowed to release the file

(7b) If the token is not valid the session has expired and so ends.

(8) The file is downloaded from the storage area network to the client.

Public-key encryption takes a lot of computing resources, so this system blends public-key and symmetric key encryption for secure performance of the system.

4.0 Conclusion

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 environment. One of the key issues 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 o]wn merits and demerits; each virtualization deployment is different depending on the need for the virtualization. It is common that any single virtualization technology will not provide shield to all the security issues arise. However, 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 consideration all the possible security issues that puts the virtual machines at risk. Finally carefully design the virtual environment with the help of correct virtualization technology that matches the goals. Majority of the security issues presented here concerns the security of the host and the hypervisor. If the host or the hypervisor is compromised then the whole security model is broken. Attacks against the hypervisor becoming more popular among the attackers realm [1]. Therefore after setting up the environment, care should be taken to

ensure that the hypervisor is secure enough to the newly emerging threats, if not patches has to be done. Patches should be done frequently so that the risk of hypervisor being compromised will be avoided [3].Virtualization is a powerful solution to reduce the operational costs in today's computing but if done wrongly, it becomes a threat to the environment. While implementing, exaggerate the security model to with stand the attacks. And as mentioned earlier keep monitoring for new developments that emerges in this field and continue to stay up to date.

References

[1]E. Messmer. Security in the 'virtual machine'? *NETWORKWORLD*, April 2006. *http://www.networkworld.com/weblogs/ security/012014.html.*

[2] A. Mann. The pros and cons of virtualization. *BTQ*, 2007. http://www.btquarterly.com/ ?mc=pros-cons- virtualization\&page= virt-view%research.

[3] K. J. Higgins. Vm's create potential risks. Technical report, darkREADING, 2007. *http: //www.darkreading.com/document.asp? doc_id=117908.*

[4] M. Jones. *Discover the Linux Kernel Virtual Machine*. IBM. http://www-128.ibm. com/developerworks/linux/library/ l-linux-kvm/.

[5]J. Kirch. Virtual machine security guidelines. *The center for Internet Security*, September 2007. http://www.cisecurity.org/tools2/vm/ CIS_VM_Benchmark_v1.0.pdf.

[6] VMware. *VMware security center*. http://www. vmware.com/support/security.html

[7] Jenni, S A Survey on Virtual Machine Security, Helsinki University of Technology, 2007

[8] R. Naraine. Vm rootkits: The next big threat. *eWeek*, March 2006. *http://www.eweek.com/ article2/0,1759,1936666,00.asp.*

[9] ZablonO, 2009 *Multiple agent co-ordination in a virtualized environment,* A thesis presented at the CSI University of Nairobi.