International Journal of Engineering & Technology, 7 (2.24) (2018) 478-483

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Vulnerabilities of Virtualization Technique

Saravanan N[1], Umamakeswari A[2]

School of Computing, SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India;
**Corresponding Author Email: saranindia@gmail.com*

Abstract

Cloud computing is a computing model for delivering resources in a convenient manner from a shared pool. The resources provisioned and released on an on-demand basis with minimal intervention of service provider. Cloud Computing is becoming the platform for all kind of web based services. Virtualization is the key concept to adopt the cloud computing. Virtualization offers many benefits comparing to real physical machine implementation infrastructure. Even though virtualization provides lots of benefits, it is also brings several security vulnerabilities. This paper presents the security breaches of various virtualization techniques that are applied in virtual machines, in which health care records maintained.

Keywords: *Virtual Machine Security, Isolation attacks, VM vulnerabilities, VM Security, Vulnerability Survey.*

1. Introduction

Cloud computing is a computing model for delivering convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The cloud computing model implemented with the support of virtualization. Virtualization is the technique, which will separate the operating system from the physical hardware. These isolated machines will be called as Virtual Machines (VM) [2]. Virtual machines are the software implementation of the machine, which will perform all the activities like physical machines. This can be treated as the main role of virtual machine in the cloud. This virtual machine can be broadly classified into two based on the usage, they are i) system virtual machine ii) process virtual machine. System virtual machine will be performing the activities like operating system. Process virtual machine will be designed to run a single program. Multiple virtual machines can be executed on single physical hardware with various guest operating systems and its application. This kind of operation will give the illusion to the end users that they have been allocated and they are working in a dedicated physical infrastructure. The software that provides the opportunity to run multiple operating systems in a single physical hardware will be called as hypervisor or virtual machine monitor or virtual machine manager. With the help of virtualization the resource sharing benefits has been achieved. The proper isolation is another benefit that should be realized in such a way that one virtual machine vulnerability should not affect the neighboring virtual machine and the underlying hardware. Figure 1 gives the overview of virtual machine environment.

There are many reasons to say the need for virtualization and those reasons are server consolidation, sandboxing, multiple execution environments, and multiple operating systems and virtual hardware. Security issues related to physical environment will also be applicable apart from the security issues that are specific to virtualized environment. In this paper several security breaches of virtualization techniques are discussed.

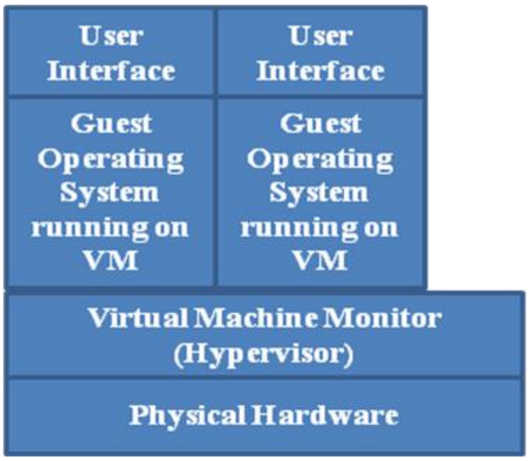
User Interface
User Interface
Guest Operating System running on VM
Guest Operating System running on VM
Virtual Machine Monitor (Hypervisor)
Physical Hardware

Fig. 1: Overview of Virtual Machine Environment

In datacenter based on the requirement this technology can be classified into seven types [2]. They are Storage Virtualization (StoreV), Network Virtualization (NetV), Management Virtualization (ManageV), Desktop Virtualization (DeskV), Presentation Virtualization (PresentV), Application Vitualization (AppV).

2. Virtualization Vulnerabilities

There are some vulnerabilities and threats that are specific to virtualization [3,4]. The description about the different virtualization vulnerabilities can be seen in Figure 2.

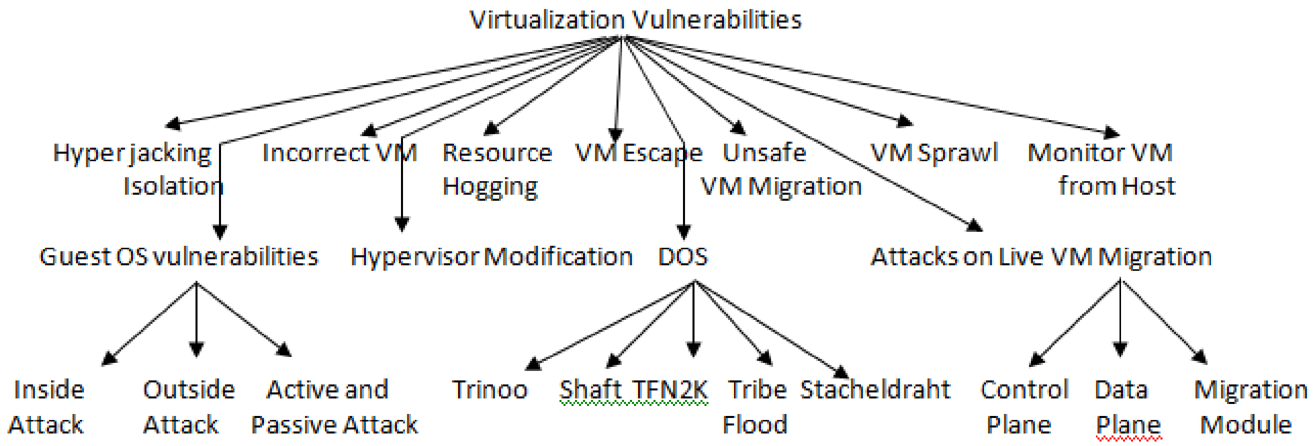

Fig. 2: Taxonomy of virtualization

2.1 Hyper-jacking

In Hyper-jacking [5] attack, the whole control over the hypervisor will be taken. As a result of this attack, the control of the guest operating systems on the guest virtual machine, virtualization server and the host operating system will be taken. Traditional security mitigation techniques may not be fruitful because the security measures that are running on the guest VMs or sever may do not know that host operating system itself has been compromised. If hyper-jacking has to be succeeded by an attacker, he needs to have processor that can do hardware-assisted virtualization to access the host. Attacker may convince the admin or user to install some malicious code to attack the hypervisor. Example for hyper-jacking are SubVirt [6], BluePill [7] and another one is Vitriol [8].

2.2 Incorrect VM Isolation

Virtual machine isolation can be classified into four major types as a) Process virtual machines, b) Hardware virtual machines, c) System virtual machines, d) Hosted virtual machines, and referred in Figure 3. In process virtual machines the proper isolation can be seen between the process and the operating system environment. Isolation policies are supported by runtime component.

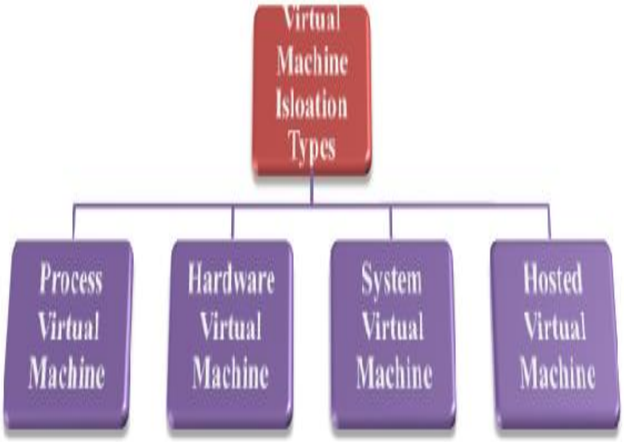

Fig. 3: Virtual machine isolation types

In Alta's [9] research project shows how to run multiple processes within the same virtual machine. Dynamo RIO [10] provides one technique to provide isolation. In hardware virtualization the virtualization-assisted hardware will be utilized to achieve virtualization so that the performance improvements can be realized comparing to software based virtualization. With the adoption of hardware virtualization the security can be improved. Example for this kind of virtualization is Intel VT-x [11], AMD-V, and KVM [12]. System virtual machines will be acting as replica for underlying platform. Virtual machine monitor will be running with highest privilege level and will share the required hardware resources to the guest operating systems that are running on the top of hypervisor. In pure-isolation mode also this system virtual machine can be implemented [13]. In that pure-isolation mode the sharing of any resources will not be happening, this is very much similar to physical machine isolation. Though this pure-isolation mode is very secure but not practically can be implemented for desktop-like environments. Example for such kind is IBM's PR/SM system [14], XEN [15], sHype [16], VMware GSX server [17], Nexus [18]. In this hosted virtual machines, the virtualization layer will be running like an application process on the top of operating systems. An operating system can be installed on the host and that operating system will be called as guest operating system. The guest operating system may run with different architecture or with the same architecture. In the hosted virtual machine the virtual machine monitor will not be running at the highest level but still hosted virtual machine will be acting and following the isolation process same as system virtual machine approach. Example for this kind of hosted virtual machine is Simics [19], Microsoft virtual pc, Qemu [20], VMware workstation. Like physical machines virtual machines should also be isolated from each other.

2.3 Resource Hogging

One VM guest operating system may consume more number of CPUs will lead to starving of resources for the remaining VMs to function on the same hypervisor. The resources that might be consumed are network, memory and CPU. This kind of attack is called resource hogging.

2.4 VM Escape

Guest operating systems that are running on guest virtual machine should be properly encapsulated and properly isolated. If the guest operating system breaks out the boundary and interacts with the host or hypervisor then that kind of attack will be called as VM-Escape [21].

2.5 Unsafe Virtual Machine Migration

In case of demand, virtual machine can be migrated from one physical host to another host. Once the migration has been done then the proper security policies has to be employed in the new physical host also, if not then the attack may happen on the new physical host, migrated virtual machine or the neighbor virtual machines on the same hypervisor. When migration occurs an attack may hijack the device module process or hypervisor. As a result of an attack if the process has been hijacked, the information of VM like OS kernel, the applications and services and the data that are getting entered in the keyboards can also be accessed.

2.6 VM Sprawl

The reason behind sprawling to happen is that lack of control over the management of virtual infrastructures. Virtualized Server creation will be easy and it will be faster also, so the problem arise like unnecessarily the virtual servers will be created and the infrastructure will be wasted. To perform some testing process some virtual machines may be created after the completion of works also that may be continued without destroying those virtual machines. The license cost for that much of virtual machines that are created unnecessarily would be wasted. Undestroyed virtual machines may yield some kind of security issues too.

2.7 Denial of Service

Different kinds of denial of service [22] attacks have been determined in different hypervisors. Denial of Service will lead to halt the specific guest operating systems or remote host services. If hypervisor or host itself compromised then all the guest operating systems will become idle. The attacker targets a specific slave using their details and it will be submitted to the master. This process is shown in Figure 4.

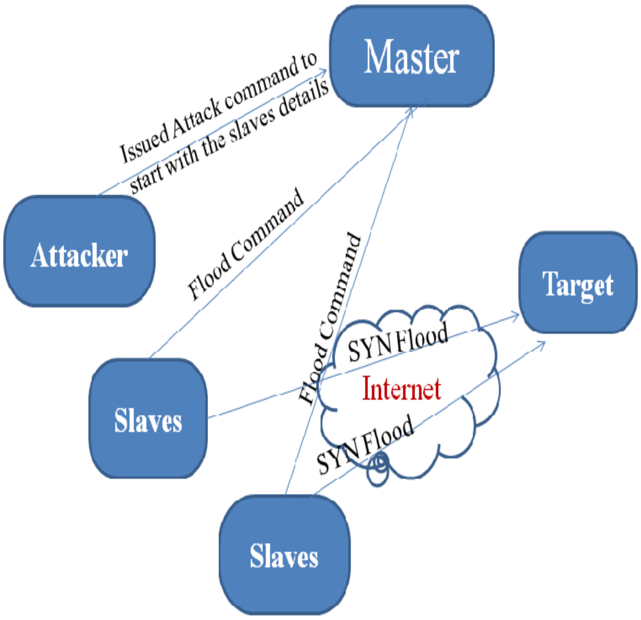

Fig. 4: Denial of Service (DOS) attack

Here some of the techniques used by an attacker to halt remote host service referred in Figure 5.

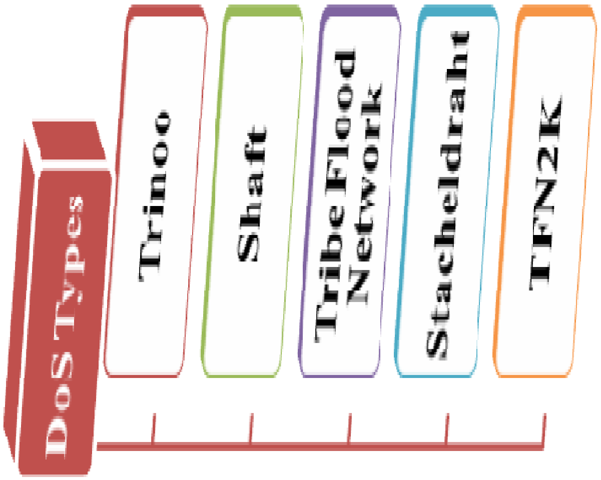

Fig. 5: DOS types

2.7.1 Trinoo

Here TCP will be used for performing the communication process between the master control program and the attacker, likewise the UDP packets will be used for having the communication process between the master control program and the attack daemons. This is a kind of flooding attack. It uses UDP packets to flood against the target victim.

2.7.2 Shaft attack

Here the attacker and the master controlling program will be communicating via TCP telnet program. Since this Shaft attack utilizing UDP packets for communicating with the attack daemons and the master control program, so this shaft attack may be treated as the derivative of Trinoo attack. The appreciable feature that can be stated for this shaft attack is that dynamically it can change the master controlling server and the ports, so the tools utilized to detect this attack will be very difficult.

2.7.3 Tribe Flood Network Attack

Here the communication between the control master and the attacker will be carried out with the help of command line user interface. The attack daemon and the control master will be communicated with the packets of ICMP echo reply. This TFN may inculcate SYN flood, UDP and ICMP flood attacks too.

2.7.4 Stacheldraht

Stacheldraht follows the activities of TFN but it is slightly deviated from the TFN in a manner that, it uses encrypted TCP connection to communicate between master control program and the attacker. TCP and ICMP will be used for conducting the communication between attacking daemon and the master control program. SYN flood, UDP flood, Smurf and ICMP flood attacks may also implemented by the attacking daemon for this attack.

2.7.5 TFN2K

Between the attacker and the master control the communication will be encrypted using algorithm called key based CAST 256. The communication between an attacking daemon and the control master will be using TCP, UDP and ICMP or all the three. SYN, ICMP floods and smurf will be utilized by this attacking daemon.

2.8 Monitor the Virtual Machine from Host

Host machine will be acting, as the control point to virtual machines and it will perform the communication with all the virtual machines that are running on that system. Host can perform the operations like starting, shutting down, restarting the virtual machines. Host can perform some more activities like copying the data from the existing virtual machine's virtual disks; it can also modify the allocated resources for the virtual machines. Here if the host itself has been compromised the attacker itself will perform all the above stated activities that can be done by the host.

2.9 Hypervisor Modification

Isolation of virtual machines between guest machines will be done by the hypervisors. If the hypervisor is not behaving properly then the security breaching on the virtual machine will happen for sure. SHype can be treated as one of the existing solution to secure the hypervisor.

3. Attacks on Live Virtual Machine Migration

Lot of state transfers will happen through the network during the Live Virtual Machine migration process. Sensitive information may get migrated; at this instance simple secure channel alone will not be helpful to solve this problem. The network related attacks [23] like ARP spoofing, ARP flooding, DNS poisoning and route hijacking may happen in live VM migration as given in Figure 6. Apart from passive attacks like spoofing attacks, hacker may perform active attack like man-in-the-middle attack.

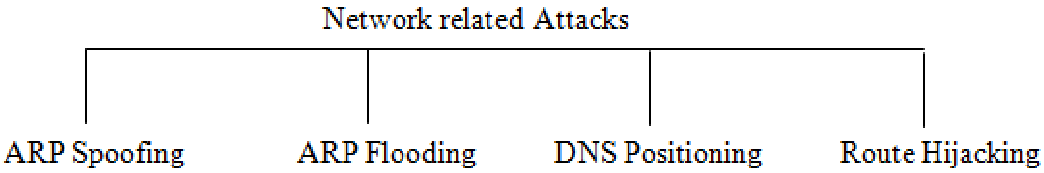

Fig. 6: Network Related Attacks

The malicious virtual machine can introduce attacks to other virtual machines in its host and subsequently for the virtual machines that are on the same Local Area Network. However the hardware firewall can only safeguard the virtual machine before and after the migration process and are sightless about virtual traffic. Thus virtual firewalls are used to secure virtual machines, which are predominantly deployed at virtual machine monitor under the control of cloud provider. These attacks may bring down the performance so that Intrusion Detection System can find these kinds of active attacks.
Live Virtual Machine migration threats can be classified into three types [24], Control Plane threat, Data Plane threat, and Migration module.

3.1 Control Plan Threat

If an attacker can have the control over the control plane of Virtual Machine Monitor then he can influence the live migration process and can gain the control over the guest operating systems. So, initiation and managing of virtual machine migration have to be properly authenticated and it should be protected from tampering. The loopholes in the control plane are shown in Figure 7.

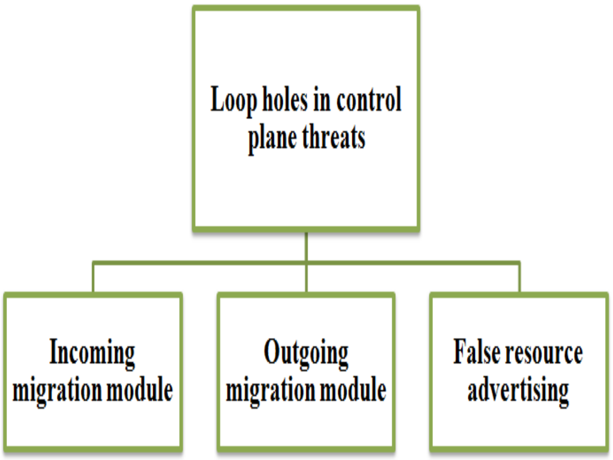
Loop holes in control plane threats
Incoming migration module
Outgoing migration module
False resource advertising

Fig. 7: Loopholes in the control plane threat

3.1.1 Incoming Migration Module

An attacker may initiate unauthorized incoming migration process to the attacker's machine to gain control over the guest virtual machines.

3.1.2 Outgoing Migration Control

An attacker may initiate higher number guest virtual machines for migration to the victim VMMs will lead to the victim to stops its functionality.

3.1.3 False Resource Advertising

An attacker may falsely advertise his resources to make the migrator to migrate the virtual machine to this compromised Virtual Machine Monitor. If the attacker got then that migrated virtual machines can be ruled.

3.2 Data Plane Threats

Melvin Ver. [25] explains how pocket sniffing are happening using the tool like wire shark to reveal the sensitive information in plain text. In migration process data that are getting migrated must be protected against passive and active attacks. Passive attacks will lead to leakage of sensitive data and an active attack will lead to compromise of whole setup. Example for active attack is that man-in-the-middle attack. The pictorial representation of that attack has been shown below in Figure 8.

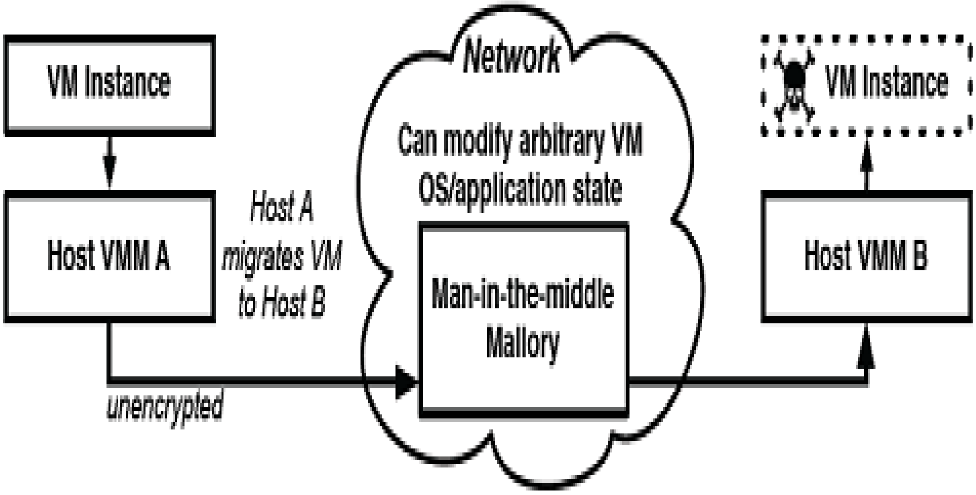
VM Instance
Host VMM A
Host A migrates VM to Host B
unencrypted
Network
Can modify arbitrary VM OS/application state
Man-in-the-middle Mallory
VM Instance
Host VMM B

Fig. 8: Security loopholes in VM migration

3.3 Migration Module

Attacker can subvert the Virtual Machine Monitor so that attacker will get the full control over the Virtual Machine Monitor, so that migration module has to be secured and proper migration policies to be maintained by the administrator.

4. Guest OS Vulnerabilities

The Guest OS vulnerabilities attack the computer operation will be disturbed, will gather sensitive information and will get privilege to access private computer system. Malwares will be primarily utilized for attacking the guest operating systems to steal the personal information, business related data and may be some financial data also. Infected virtual machines will be used for sending emails or used to perform distributed denial of service attack also. Attacks that may happen against guest operating system are shown in Figure 9.

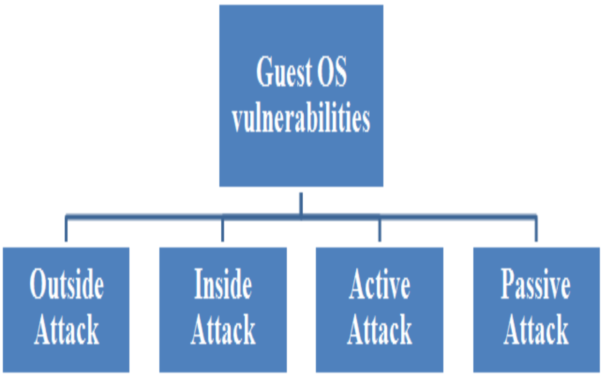

Fig. 9: Guest OS vulnerabilities

4.1 Inside and Outside Attack

An unauthorized outside user may tries to penetrate to access the system by crossing the perimeter through Internet. An attacker can be novice or a structured criminal. Inside attack an authorized malicious insider who is leading the life inside the perimeter will be utilizing the system in a way that is not been authorizing to perform.

4.2 Active and Passive Attack

In active attacks the allocated system resources itself will be altered or made to halt the whole operation of the resources. In passive attacks the system resources will not be altered or will not be halted from performing any kind of operations but the information will be stolen to perform some other activity.

5. Conclusion

Virtualization is a powerful technology to accomplish different kinds of optimizing activities. If this technology has not been implemented properly then this may yield many kinds of security threats. Everybody has to understand the fact that virtual machines are the resemblance to the physical machines so the attacks that are inescapable for physical hosts that are applicable to virtual machines also, apart from the attacks that are special to this virtualization technology. Hypervisors will be acting as one more abstraction layer between physical hardware and the malicious attackers in the guest operating systems. Hypervisor will also monitor all the virtual machines that are running so that attacks can be minimized. If the hypervisor itself has been compromised then all will end up in vein. Actually virtualization is not purely unsecure but will have the possibility for more number of breaches if that has not been implemented properly. Both the host and the guest operating systems are to be secured. Still some more unexplored vulnerability areas are there and those to be explored.

References

[1] Definition of Cloud computing, http://www.nist.gov/itl/cloud/

[2] Danielle Ruest, Nelson Ruest, "Virtualization: A Beginner's Guide", McGrawHill, 2009, Page 30.

[3] Bernd Grobauer, Tobias Walloschek, and Elmar Stocker, "Understanding cloud computing vulnerabilities", IEEE Security and Privacy, 9(2) 50-57, March 2011.

[4] Anand. R, Sarswathi. S, Regan.R, "Security issues in virtualization environment", IEEE International Conference on Radar, Communication and Computing (ICRCC), 2012.

[5] Chunxiao Li, Raghunathan, A., Jha, N.K., "A Trusted Virtual Machine in an Untrusted Management Environment", IEEE Transactions on Services Computing, Volume: 5, Issue: 4, 2012.

[6] S. T. King, P. M. Chen, Y.-M. Wang, C. Verbowski, H. J. Wang and J.R. Lorch, "SubVirt: Implementing malware with virtual machines," Proceedings of the IEEE Symposium on Security and Privacy, 2006. pp. 314-327.

[7] J. Rutkowska, "Subverting Vista Kernel for Fun and Profit", Symposium on Security for Asia Network, SyScan and Black Hat Briefings, 2006.

[8] D.D.Zovi, "Hardware Virtualization Rootkits", http://www.theta44.org /software/HVM_Rootkits_ddz_bh-usa-06.pdf.

[9] P. A. Tullmann, "The Alta operating system", Master's thesis, University of Utah, Dec. 1999.

[10] Derek Bruening, Evelyn Duesterwald and Saman Amarasinghe, "Design and implementation of a dynamic optimization framework for Windows", 4th ACM Workshop on Feedback-Directed and Dynamic Optimization (FDDO-4), December 2000.

[11] Intel Virtualization Technology: Hardware Support for efficient processor virtualization. URL: ftp://download.intel.com/technology/itj/2006/v10i3/v10 - i3-art01.pdf

[12] KVM White Paper. URL : http://www.qumranet.com/art_images/ files/8/KVM_Whitepaper.pdf

[13] James E. Smith, Ravi Nair, "The Architecture of Virtual Machines", Computer, vol.38, no.5, pp. 32-38, May, 2005.

[14] Certification Report for Processor Resource/System Manager (PR/SM) for the IBM eServer zSeries 900, BSI-DSZ-CC-0179-2003, 27 February 2003, Bundesamt fur Sicherheit in der Information stechnik: Bonn, Germany. URL:http://www. commoncriteriaportal.org /public/files/epfiles/0179a.pdf

[15] Barham, P., Dragovic, B., Fraser, K., Hand, S. , Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. 2003, "Xen and the art of virtualization", Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, USA, October 19 - 22, 2003.

[16] R. Sailer, E. Valdez, T. Jaeger, R. Perez, L. van Doorn, J. L. Griffin, S. Berger, "sHype: Secure Hypervisor Approach to Trusted Virtualized Systems", IBM Research reports.

[17] J. Sugerman, G. Venkitachalam, and B-H. Lim, "Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor," Proc. General Track: Usenix Ann. Technical Conf. Usenix Assoc.2001, p.1-14.

[18] Emin Gun Sirer, "Nexus: A New Operating System for Trustworthy Computing", TRUST (Team for Research in Ubiquitous Secure Technology), Washington DC, January 2006.

[19] Simics. URL: http://www.virtutech.com

[20] Fabrice, B., "QEMU: A Fast and Portable Dynamic Translator", USENIX 2005 Annual Technical conference, FREENIX, pp. 41-46, 2005.

[21] Ken Owens, Securing Virtual Computer Infrastructure in the Cloud, SavvisCorp, 2009.

[22] Shea. R, Jiangchuan Liu, "Performance of Virtual Machines under Networked Denial of Service Attacks: Experiments and Analysis", IEEE Systems Journal, Volume 7, Issue 2, June 2013.

[23] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M.Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, Oct. 2012.

[24] J. Oberheide, E. Cooke, and F. Jahanian, "Empirical exploitation of live virtual machine migration", Black Hat Security Conference, Washington, DC, February 2008.

[25] M. Ver, "Dynamic load balancing based on live migration of virtual machines: Security threats and effects", Thesis report Rochester Institute of Technology, B. Thomas Golisano College of Computing and Information Sciences (GCCIS), Rochester, NY, U.S.A, 2011.

[26] S.V. Manikanthan , T. Padmapriya "An enhanced distributed evolved node-b architecture in 5G tele-communications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018.

[27] S.V.Manikanthan and D.Sugandhi " Interference Alignment Techniques For Mimo Multicell Based On Relay Interference Broadcast Channel " International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume- 7 ,Issue 1 –MARCH 2014.

[28] T. Padmapriya, V.Saminadan, "Performance Improvement in long term Evolution-advanced network using multiple imput multiple output technique", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, Sp-6, pp: 990-1010, 2017.