Grenze International Journal of Computer Theory and Engineering , Oct 2015

Hypervisor Forensics: State of the Art and Research Challenges

Romika Panwar[1], Kapil Dev[2], Mukesh Kumar[3] and Noor Mohammad[4]
[1] Graphic Era University/CSE, Dehradun, India
Email: romikapanwar@gmail.com
[2-4] Guru Ram Dass Information and Management Technology/Computer department, Dehradun, India
Email: {kapilchaudhary69, mukesh777kumar, noormohddcs}@gmail.com

***Abstract*—Cloud Computing is the emerging technology in IT which aims more and more users to be part of it. Cloud computing is a revolution in IT the way resources are utilized and managed. It is an emerging and prosperous field for both academically and industrially. With its wide acceptance today security is a vital concern. Technique running at the back of Cloud computing is virtualization in which virtual machines simultaneously operates and application that controls and managed them is hypervisor. Many models for security of virtualization have been proposed for the protection of resources but still virtualization is being vulnerable to many attacks. Hypervisor forensics is a post approach to investigate and analyze security threats at hypervisor level. This research field will be beneficial for reducing crime rate at network level and improve security. This paper aims to understand some of the proposed model and identify research gap and challenges to provide better awareness of hypervisor forensics. The benefit of this work is that it depicts the state-of-the art in hypervisor forensics.**

***Index Terms*— Hypervisor, Hypervisor Forensics, Cloud Forensics, Virtual Machine Monitor.**

I. INTRODUCTION

Cloud computing is a network oriented environment for sharing resources and computation. Technically, it is a collection of virtualized computing resources or virtual machines and the environment is called virtualization. Virtual machines are responsible for the execution of the multiple instances of isolated operating system (guest OS) on a single physical machine (host OS). Application layer which acts as an interface between the host physical machine and guest operating system is the hypervisor. Responsibilities of hypervisor is to allocate resources to the guest OS and is done by the set of virtual hardware devices (memory, CPU) whose jobs are then scheduled on the physical hardware. Virtualization can be categorized into many forms based according to the computing architecture layer like Java virtual machine [1] or Dalvik virtual machine [2] come under application virtualization. Another category is operating system virtualization like Virtual Box [3], VMware, Xen [4] , Kernel virtual machine[5]. And Full virtualization which Cloud computing strictly follows. Recent survey [6, 7] depicts that number of well known hypervisor brands deployed in data centers are expanding with a multi-Hypervisor strategy becoming the norm. Under this VMware has a total presence of 81% and 52% of data centre use it as a primary Hypervisor followed by Xen (81% presence, 18% as primary), Kvm (58 % presence, 9% as primary [6, 7]). With the rising popularity of

Grenze ID: 01.GIJCTE.1.1.536

virtualization technology, the issue about security and acceptance are also growing [8]. However hypervisor has also unfortunately introduced unfamiliar security threats like kernel level root kit [9], malware spreading during migration of virtual machines or aid future detection [9].

Hypervisor forensics is the methodology of post investigation of attack to find the evidence and source of the attack. It comes under Cloud forensics. Data acquisition and log evidence in Cloud computing environment is differ from the traditional digital forensics methodologies [10] due to its elasticity and scalability of resources. This Paper is design to provide better awareness of hypervisor security and its forensics methodologies with the research gap and challenges. We surveyed the various proposed models of hypervisor security and its forensics. The research challenges are then explained and identified.

This paper is categorized as follows. Hypervisor security and its issues in Section 2. Intrusion Detection Techniques for Hypervisor based System in Section 3. Surveyed on Hypervisor based attacks in Section 4. Hypervisor forensics is explained in detailed in Section 5. *State of the Art* In Section 6 .We concluded the research challenges in Section 7 and in Section 8 future work is highlighted.

II. Virtual Machine Security

Virtualization in Cloud has two categories virtual machine and hypervisor. However virtualization concept is not new in earlier days it came as a bare metal virtualization (native virtualization) at that time it has several security vulnerability which are now being migrated to cloud environment. Before going to the detail study of hypervisor forensics its security issues should be understood earlier. Therefore we discussed the key issues of hypervisor security and its threats in this Section

A. Hypervisor Security

Several virtual machines are associated in a virtualized cloud environment and as far as security is concern these virtual machines have their own security zones which are not being access by other virtual machines having its own security zone. According to the NIST [11], Hypervisor is an abstraction layer that decouples host machines from guest machines. So hypervisor is the centralized controlling agent of all the virtual machines and has its own security zone. There are many security zones in a virtual environment but these ones exist within the same physical infrastructure that only exist within a single security zone as it is like a traditional security system[4]. This can be vulnerability in hypervisor security when an attacker will occupy the full hypervisor realm. Virtual escaping [12] is another way to take hypervisor full control from the virtual machine level. To overcome from virtual escaping, if several APIs are being created to control and disable this operation within VMs, it will also degrade the performance of the system. So it is a vital issue to work on.

B. Strength Of Hypervisor-Based Systems

The Hypervisor is a centralized management system of virtual resources, apart from that it has the capability to secure the cloud system. So for implementing secure API's hypervisor is the best platform in the cloud system due to the following reasons

1. Hypervisor is on the upper layer of physical hardware in cloud system hierarchy model. So to access the physical system hypervisor is the only way to access so security in cloud system lies at hypervisor level.
2. Hypervisor being an interface can perform as a firewall and will be able to prevent suspicious user's approaches to the share physical hardware [13].
3. The Hypervisor separates the guest OS and the host OS and physical hardware so if any attack bypass the security of guest OS the hypervisor monitor it.
4. Hypervisor is capable of network monitoring in cloud environment as it acts as a controller between the guest OS and shared physical hardware [13].

C. Weakness of Hypervisor-Based Systems

1. Single point-of-failure is the vital issue in the hypervisor system as only single hardware manages all the shared hardware resources in the cloud environment. Reason of failure can be any successful attack (rootkit, DDos, Flooding attack etc) or overloading in the hypervisor which will affect the VMs and shared hardware devices.
2. Hypervisor has more security risks from wrapping attacks which performs the duplication of user-name and password between web browser and cloud server [14]. We will discuss this attack in the next section
3.

III. CONVENTIONAL INTRUSION DETECTION TECHNIQUES FOR HYPERVISOR BASED SYSTEM

The hypervisor controls the translation between the VMs and shared hardware resources. So IDSs can be use in hypervisor as it can detect and analyze the attacks efficiently than the same IDSs performing on the guest OS because it cannot monitor events in Cloud only it can be within its VM. However if cloud provider performs the features only then it is possible for guest OS to monitor cloud events [15]. In cloud environment IDSs can be used in the form of Host Intrusion detection systems HIDS [23] and Network Intrusion Detection systems NIDS [22]. However there are some attacks which only meant for IDSs and if the attacks succeed the entire cloud system is in threat because all the relevant information then be access by the attacker which the NIDS has gathered containing sensitive data of cloud user's. So encryption methods to prevent access data is prefer by cloud users. As a result NIDS can't examine the information due to the encryption so it can become less efficient. So if the attacker and victim are in the same cloud NIDS can't be able to probe it.

May be NIDS be the best solution in hypervisor but one major problem is that it can't be used for monitoring encrypted data.

IV. ATTACKS ON HYPERVISOR SYSTEM

The Hypervisor allows users to be isolated from the other ones in a cloud environment even when they are served by same physical resources. Apart from this secure feature there are several attacks which can harm to the hypervisor. As cloud is designed to provide services to all legal users and also it also give services to users that have some malicious purposes. So there are some of the attack at hypervisor level which are as follows:

WRAPPING ATTACK : This type of attack can be a threat to hypervisor in virtual environment. When a user makes a request to the web browser from his/her virtual machine a message called SOAP(Simple Object Access Protocol) is generated. This attack with the cross site scripting then duplicates the authentic user account and password during login phase so that attacker can affect the SOAP messages that are exchanged during setup time of web browser and web server.

DATA STEALING: Security threats at hypervisor in virtualization system are the data stealing by authorised administrator without leaving the trace of any volume of data. To overcome from this problem login in hypervisor as an administrator create some data replication schemes by applying some policies like RAID and mount the disk image onto the hypervisor and deletes the original copy and lost[17].

D-DOS ATTACKS: DDos attacks typically works on the flooding of IP packets at specific network for the purpose of damaging the computer system resources. In cloud environment DDos attacks has a greater potential to disrupt the cloud infrastructure having the large amount of VM's and its controller called hypervisor. If a hypervisor doesn't provide sufficient resources for its VM's then chances of affecting the system by DDos increases. But problem arises when a user inside a cloud does a bot-net type DDos attack.

CLIENT TO CLIENT ATTACKS: In Cloud environment a virtual machine having malicious characteristic could infect all the virtual machines in the same environment. The biggest security risk in a virtualized environment is when a virtual machine having malicious feature could infect all existing virtual machines in the same realm. In this type of attack the attacker acquire administrator authorization at infrastructure level and through that puts malicious content from one VM which then lead to disrupt other VM's and from there escaping the hypervisor and accessing the cloud environment which can be accessible from VM level. Hence major risks in the hypervisor and virtualized environment are client level attacks. SQL injection [18], spoofing attacks [19] are some of the examples.

VULNERABLE INTERFACES AND API's: In cloud environment, the cloud service provider (CSP) releases software interfaces or API's even for hypervisor upgradation software patches have been used for smoothly working at infrastructure level. So vulnerable interfaces and API's can lead to the security issues of confidentiality, availability and data integrity [19] at hypervisor level.

V. HYPERVISOR FORENSICS

Forensics is defined as applying proven methodology for collecting of evidences and analysis of a crime scene. Here is some forensics realm in IT.

A. Digital Forensics

Digital forensics is defined as proven methodology towards the collection, identification, validation, and analysis of digital data logs for the purpose of further criminal investigation [20].

B. Network Forensics

Network Forensics [21] is a subclass of digital forensics relating to the monitoring and analysis of network traffic for the purpose of crucial information collection authentic evidence or intrusion detection [19]. Its main function is to analyze the data from network traffic by capturing of packets through firewalls, intrusion detection system or devices like routers [22]. Some popular network forensics tools are Wireshark [21], snort [21], TCP dump [21] , and many more. According to e.s Pilli [21], network forensics follows the steps of preparation, detection, incident response, collection, examination, investigation and presentation.

C. Cloud Forensics

Cloud Forensics is the sub branch of network forensics .As cloud runs on a network and all its equipments like network devices like (hubs or switches) or applications like hypervisor are also works in network forensics platform. Cloud Forensics involves collecting crucial information from cloud for the purpose of investigation [24].

D. Hypervisor Forensics

Hypervisor (Virtual Machine Manager or "VMM") is an abstraction layer between guest OS and physical devices , so all data that has to be processed from guest OS has to be pass through hypervisor before physical devices (e.g. CPU, NIC....) assessment. The use of this data at hypervisor can be used as a log evidence for hypervisor forensics."Virtual machine introspection (VMM)" terminology is generally used in Hypervisor based forensics. And that data must be used in intrusion detection purposes. As far as there is the accessibility to the hypervisor it will be suitable for investigating in cloud environment.

VI. State Of The Art

In this section, after going through a literature survey we present the state-of-the art in hypervisor forensics in three categories. Forensics methodology on various known hypervisor, research gap and challenges.

A. Forensics Methodology On Various Known Hypervisor

In this section we have explained different approaches of Hypervisor forensics in common hypervisors

XEN

Xen [4] is a popular Para virtualized system under this a LibVMI framework runs under DOM0 region for the purpose of direct memory access of virtualized hardware. Xen main function is to translate specific address which is generated by an application in DOM0 region into physical address. This address then reverts back into DOM0 address space. So data structure generated by that pointer is the process ID offset, executable name offset. To acquire all information about each application processes useful memory addresses have to be mapped in between DOM0 and DOMU address region. Each entry of the process in the list has to be mapped from memory region of DOM0 [24]. This procedure comes under virtual machine introspection and LibVMI allows investigation to access information about process .However memory mapping procedure is hidden for users of programming library.

KVM

Kernel virtual machine (KVM) [5] is an open source project for Linux X86 platform that works on full virtualization concepts. Here in this virtual machine whole management of virtual hardware allocation is done by QEMO [25]. However, LibVMI [25] also offers features to obtain forensically memory dumps . Patches are available to only for (QEMU-KVM 0.14.0). Also "KVMsec" [83] project is introduced to increase the security of guest VM against malware and rootkits attacks. Its main feature is that it can collect crucial data on guest machine.

- It provides two-way security between the host and guest in virtual environment.
- It works well against malicious virtual machine. Major advantages of this project that it comprises of multiple modules working in host and guest kernel level.

VMware ESXi

Garfinkel and Roesenblum [26] proposed a VMI-based Intrusion detection system (IDS) called Livewire. This prototype is designed for upgrading VMware workstation on Linux X86 platform to gain access to memory CPU registers. Another security solution for VMware is introduced in 2008 name Vmsafe program [85]. It provides some unique features i.e. it provides some API's programs that enables the developer to develop some security product for VMware. Vmsafe provides some third party API's which get into the operation with hypervisor to analyze and eliminate virus, Trojans, key loggers, or any rootkit attacks. Also Cloudsec project [27] a research agreement between Telenor and SINTEF has develop a security aspects that any organization should consider when dealing with cloud services. Cloudsec provides access to physical memory of VMs through Vmsafe API's. It is not mandatory to install security inside VMs. In the framework low-level information (bytes) is mapped into high-level data structures that allow the detection of Dynamic kernel object manipulation (DKOM) and Kernel object hooking (KOH) rootkits. Thus the approach corresponds to the out-of-band delivery model.

VII. Research Challenges In Cloud Computing

By analysis of digital and cloud computing forensics investigation studies it is obvious that nature of hypervisor is in contrast as compare to digital forensics. None of the application and framework for digital data collection is feasible in cloud and hypervisor models. On the basis of digital study in forensics methodology in digital environment the following problems are identified. In this section we are on a deep look of the issues that investigators should face.

A. Identification

Cloud has a distributed environment so at hypervisor level identification of feasible sources of evidences is a tedious task. Accessing the log evidences is the first issue in identification stage which consists of checking system status and log file. However, this is not possible in hypervisor level because client is limited to the API's. At IaaS level it is limited partly applicable. At hypervisor level data loss in volatile storage is a challenge of forensic investigation. Where there is no evidence. Such volatile data storage policy in virtual environment may lead to loss of evidences in a case when a criminal force to power off the machine [28].

B. Collection

Collecting evidences is the main issue in computer forensics investigation and it is not completely possible to in distributed computing environment i.e. cloud computing. Computer forensics works with seizing the evidences from physical devices. And due to the virtual environment of the cloud collection of log evidences is a difficult task. However, in IaaS system using the snap-shot of VMs can hold to pause the status and investigate the system [29, 30].

C. Preservation

Evidence is the only proof of some criminal activities and any crime to the trustworthy or relation of the evidence makes it of no use. So preserving the evidences is another issue in forensics investigation.

D. Analysis

Analysis of data is also an essential setup of cloud and hypervisor forensics. Especially in cloud system where it required more attentive examination of objects and log evidences at wide level. This is an additional issue of hypervisor forensics due to the limitation in log evidence processing [31].

E. Reporting

Reporting is the last step of forensics investigation at hypervisor level. In computer forensics it is not difficult to decide the court and the case would be brought in the country. But when it comes of distributed network or wide virtual environment it is more complicated issue related to the crime location, physical availability as cloud resources are shared between multiple Countries and different locations. This typically confuses investigators to decide about the legal system [31].

VIII. Conclusion and Future Work

This paper presents the state-of-the art in hypervisor forensics after defining hypervisor security and differentiating it with digital forensics, network forensic and cloud forensics. Some of the phases are also discussed which comes under forensics investigation in cloud environment. There is a great requirement for updating digital forensic investigation methodology as updating of technologies in today's era will make it of no use. Research challenges describe in this paper are surveyed and listed with issues. As development of hypervisor forensics is in initial stage we hope our research work will provide better understating of techniques and challenges of hypervisor forensics.

We will propose some framework for hypervisor forensics having all the phases cover with some respective tools for each phases in future work.

REFERENCES

[1] Java virtual machine, (2014), [online]. Available: http://en.wikipedia.org/wiki, [Oct,17,2014].

[2] Dalvik virtual machine, (2014),[online]. Available: http://en.wikipedia.org/wiki, [Oct, 18, 2014].

[3] Sun-Oracle,(2014), " Virtual Box 8.2", [online]. Available: http://www.virtualbox.org, [Oct, 16, 2014]

[4] Xen, (2014), [online]. Available: http://www.xenproject.org, [Oct, 21, 2014]

[5] Linux, (2014), "KVM 4.2 ", [online]. Available: http://www.linux-kvm.org, [Oct, 15, 2014]

[6] Nexenta Hypervisor Survey. http://www.nexenta.com/corp/nexenta-hypervisor-survey.

[7] Is the Hypervisor Market Expanding or Contracting? http://www.aberdeen.com/Aberdeen-Library/8157/AI-hypervisor-server-virtualization.aspx.

[8] National vulnerability database. http://web.nvd.nist.gov/view/vuln/search.

[9] J. Levine, J. Grizzard, and H. Owen. Detecting and categorizing kernel-level rootkits to aid future detection. IEEE Security Privacy Magazine, 4(1):24 {32, January { February 2006}

[10] Heiser J. Remote forensics software. Gartner RAS core Research Note G00171898; 2011.

[11] National Institute of Standards and Technology,(2014), [online] Available: http://en.wikipdeia.org/wiki, [Oct,20,2014]

[12] Virtual machine escape, (2014), [online] Available: http:// en.wikidpedia.org/wiki, [Oct, 20,2014].

[13] T. Ristenpart and e. al, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the16th ACM conference on Computer and communications security, Chicago, IL, November 9-13, 2009.

[14] "Securing Virtualization in Real-World Environments," White paper, 2009.

[15] Rosenblum M. and Garfinkel T. Virtual machine monitors: current technology and future trends. Computer, 38(5):39–47, May 2005.

[16] Renato J. Figueiredo, Peter A. Dinda, and J. Fortes. A case for grid computing on virtual machines. In ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems, page 550, Washington, DC, USA, 2003. IEEE Computer Society.

[17] J. Mutch, (2010), "How to Steal Data from the Cloud," [Online].Available:http://www.cloudbook.net/resources/stories/how-tosteal-data-from-the-cloud, [Oct. 15, 2014]

[18] SQL injection, (2014), [online]. Available: http://en.wikipedia.org/wiki, [Nov, 02, 2014].

[19] Spoofing Attacks, (2014), [online]. Available:http://www.veracode.com/security/spoofing-attack, [Nov,01,2014]

[20] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," Digital Investigation, vol. 2, no. 2, pp. 147-167, 2005.

[21] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and Research Challenges," Digital Investigation, vol. 7, no. 1/2, pp. 14-27, 2010.

[22] Network Intrusion Detection Systems [Online] Available : http://wikipedia.org/ [Nov,04,2014]

[23] Host Intrusion Detection Systems [Online] Available: http://wikipedia.org/ [Nov,04,2014]

[24] Xen security,(2014) [online]. Available: http://support.citrix.com/article/CTX126531[Nov,08, 2014]

[25] LibVMI,(2014)[online].Available:http://code.google.com/p/vmitools/wiki/LibVMIIntrodution [Nov,10,2014].

[26] M. Rosenblum, E. Garfinkel, S. Devine, and S. A. Her- rod. Using the simos machine simulator to study complex computer systems. Modeling and Computer Simulation, 7(1):78–103, 1997.

[27] Cloud Security Project [Online] Available: https://www.cloudsec.co/[Nv,21,2014].

[28] Cheng Yan, "Cybercrime forensic system in cloud computing", Image Analysis and Signal Processing (IASP), 2011 International Conference on , vol., no., pp.612-615, 21-23 Oct. 2011, [URL] http://ieeexplore.ieee.org/search/srchabstract.jsp?arnumber =6109117

[29] Patrick, (2010), "Security in a Public IaaS Cloud Part 3: Data Storage ", [Online]. Available: http://www.cloudsigma.com/blog/15-security-in-the-cloud-data- storage, [Oct. 15, 2014]

[30] F. Xinwen, L. Zhen, Y. Wei, and L. Junzhou, "Cyber Crime Scene Investigations (C2;SI) through Cloud Computing," in IEEE 30th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2010, 2010, pp. 26-31.