Detection of Malware and Kernel-Level Rootkits in Cloud Computing Environments

Hinna Hafeez
MPhil Computer Science
Kinnaird College Lahore.
hinnahafeezsh@gmail.com

Najia Nasir
MPhil Computer Science
Kinnaird College Lahore.
Najiaajmalnasir@gmail.com

Abstract:
This paper provides detailed comparisons between different studies based on the topic, “detection of malware and kernel level rootkit in cloud computing environment”, and on the basis of these comparisons, different findings are provided and in the end, this paper provides suggestions to improve different techniques of the detection.

Paper 1:

Rootkit Detection on Virtual Machines through Deep Information Extraction at Hypervisor-level [a]

By: Xiongwei Xie & Weichao Wang, Paper Published in 2013.

Overview:
The first step of an attacker is to attack system’s rootkit, rootkit is basically a collection of tools which is used to run programs; once the rootkit is accessed the attacker can get the administrative control of the system. [1]
Such attacks are very dangerous, the formation of virtualization creates a new technique for the detection of such attacks, and the paper recommends the approach which uses rootkit in detection and prevention. The rootkit which will be designed for the virtual machines to not only detect but also prevent from malware by using information extraction and reconstruction techniques at the hypervisor level.
With the help of important components of virtual machine i.e kernel symbol table, the hypervisor can reconstruct the virtual machine execution state and can get the important information e.g running programs/ processes, active network connection & open files etc. With the help of cross checking of the components, the important information is fetched:
1: Concealed information
2: The anomaly connections among them
The method used in the above paper is executed in Xen 4.1 Linux VMs
The paper implemented given approach in Xen 4.1 with Linux VMs. Results of the experiments showed that the hypervisor can efficiently reconstruct the semantic view of a VM’s memory and detect the rootkits. The access of the hypervisor is only to the high level data structures which has very limited impacts on the performance of VM.
Today’s computer systems are more insecure as compared to the early system, because of the excessive use of internet, today’s systems are more exposed to threats, the severity varies from mild to severe, some threats are detectable some are not, the threats which cannot be detected are more dangerous than the one which can be detected. These are known as stealth attack. The most crucial component that can be attacked is rootkit, so the stealth attack to rootkit is the most severe attack in the recent era.
In such attacks rootkit is the target and the malicious program hides itself to not to be detected and get the administrative control of the system. In these attacks rootkits hide their existence from the anti-malware programs.
Rootkit detection is classified into three groups:
1: the first group analyze and characterize the behavior of rootkit with the help of Hookfinder, K-Tracer, Panorama
2: the second group tries to detect rootkit through some indicators that are unveiled by the interruption with the help of SBCFI, kernel integrity of OS monitoring for the change detection & Copilot
3: the third group design to secure rootkit from changes the OS kernel, author presents a method that uses the static analysis to identify instruction sequence of malicious actives based on their signature. The host based rootkit mechanisms have their limitation e.g there are many effectively secure rootkits which are capable to detect and remove antimalware, Agobot is one of them, it not only can detect but also remove more than 105 types of malware program in victim machine.
There are systems for rootkit detection in VM i.e VM watcher, VMI , UCON , it effectively maintains low level access to the system and makes sure that access cannot be compromised by the internal process of VM.

Although the detection is on detailed level but still some data remains unexamined and some malware remains undetected, VM watcher compares the name of the process, the attacker changes the name of the malware process with the name of other process and to hide itself from detection. Some software packages also contain some hidden components so their hidden goals. The technique proposed by the paper is based on detailed level information extraction and on crossed verification at hypervisor level.

The hypervisor can only perceive or observe the raw memory pages of VM so the need was to provide semantic view of VM's memory for the states information i.e running processes, kernel level modules, network connections and open files then check execution states and cross verify both with this approach. Hidden malware can be identified with this and the gap between the VM view and hypervisor view can be minimized. The verification identified the mismatches they executed in their approach in XEN which presented trivial performance impact over the virtual environment.

Findings:

The approach is basically based on the view difference between hypervisor and VM, paper proposed to give the same access to hypervisor as the VM has. It's good in a way that it can verify both as VM and hypervisor. Both are viewing same files processes so they can detect hidden malware with this ability and with the help of mismatched files.

- One point arises that is it safe to give this much access to hypervisor?
- Can hypervisor not be a threat for the system?

Limitation:

This approach is executed in Linux, not tried on the window.

Recommendations:

This approach is good enough and explained in detail. One recommendation is to link this approach with artificial intelligence for the better detection which is also mentioned in the paper for further enhancement, it will make it more effective

Terms/ Key words:

Hypervisor: Virtual machine manager
Anomaly: abnormality, irregularity
Xen 4.1 Linux VMs:
Stealth attacks: attacks that remain undetected by the client computer [2]
HookFinder : It provides the information about the underlying hooking mechanisms that attacker used.
SBCFI: state based control-flow integrity
VMI : methodology used to inspect the low level VM states.
UCON: stands for usage control model

Paper 2:

Malware Detection in Cloud Computing Infrastructures [b]

By:

Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Andreas Mauthe and David Hutchison
Journal is published in 2015

Overview:

This paper is based on the key concept of the security of cloud that it should not only detect net based threats but also make cloud capable of handling new challenges that target cloud infrastructures. The paper has discussed an online cloud anomaly detection approach, compared detection components etc the paper claimed of the detection of malware and DoS attacks. Authors not only evaluated the system level data but also covered the network level data depending on attack type and showed that their detection approach based on components monitoring per VM is applicable to cloud and its flexible detection system which can detect malware without any knowledge of their functionalities or underlying instructions.

Cloud datacenters are used in private, public and commercial level so it should be able to handle all types of cyber-attacks , the properties of cloud e.g. transparency and elasticity of its services made it vulnerable, clouds dependency on IP network makes it vulnerable. Current approach is based on resource intensive deep packet inspection (DPI) which relies on payload information whereas the proposed approach is based on per flow Meta statistics, derived from packet header and volumetric information which is packet and byte etc count. Their approach targets the cloud and also integrates with infrastructure for the detection and also for the remediation, at infrastructure level they targeted the cloud nodes and network infrastructure that provides the connectivity within the cloud and with external services.

Cloud services are provided with one or more VMs which are interconnected, cloud services are divided into three categories:

Software as a service; it has most control and gives limited access to the user

Platform as a service (PaaS); it gives the choice to the user of execution environment, deployment tools but not the ability to be the administrator of their own operating system.

Infrastructure as a service (IaaS); it provides the most control , the user has the ability to install and administer their own choice of OS and run anything on the provided virtualized hardware, it is more sensitive and bit difficult to secure IaaS, the paper mainly focused this cloud service and the techniques are also applicable on the other services.

The paper discussed the approach that uses one class Support Vector Machine (SVM) algorithm and provides its effectiveness, tested this approach on malware and DoS in controlled environment.

Used malware samples were Kelihos and Zeus.

The experiments are performed on cloud. These experiments have used the implementation of the concepts which are based on Virtual machine. The results of the experiments have shown that online detection of the anomaly takes less time for the bulk of the data per VM with the help of SVM approach. Accuracy rate of these approaches is more than 90%.
The detection of malware in actual cloud is related to VM live-migration, SVM specific parameter estimation is used for better detection, they evaluated overall system, network based or joint datasets

Findings:

- Computational cost is not very high for this approach.
- They used the sub modules of architecture's cloud resilience managers which are used in the detection at the end system.

Limitation:
The methodology overall worked well and also improved the efficiency of the cloud but it worked more efficiently on joint dataset than the other cases.
Recommendations:

- This approach is good when the system is online; offline mode techniques should also be secure and efficient.
- For joint dataset it needed to be improved.
- Datasets are basically under process so data mining techniques can be made more efficient

Paper 3:

Title:
Detection of Malware and Kernel-level Rootkits in Cloud Computing Environments [c]
By:
Win, Thu Yein and Tianfield, Huaglory and Mair, Quentin
Published in 2016
Overview
Virtual machines is used to store or process data of client machine, these virtual machines are targeted by cyber-attacks e.g. VENOM (use to access hypervisor)
Approaches to malware detection is classified into distributed and hypervisor-based malware detection , distributed is VM agent running into the guest VM , remote monitoring server is monitoring its behavior , use single point of control for the attack detection , it needs signature database .
Hypervisor based malware detects malware within the guest by hypervisor, it protects the results , it makes it infeasible for deployment in production house .
The paper present novel virtualization security system , combined system call monitoring and system call hashing in guest kernel with SVM based external monitoring on host . with this approach malware and rootkit detection protect the guest against attacks without any extra burden

Findings:
Paper presented rootkit and malware detection systems to protect the virtualization infrastructure against cyber-attacks in cloud environment

- Approach used system call hashing and SVM together in VMI.
- It makes sure that the internal guest VM state can be accurately achieved.
- In also handles the offline SVM case.
- Offline SVM classifies/allows quick attack classification.

Recommendations:

Some additional calls can be added for achieving accuracy to attach detection in guest VM.
Data mining algorithms can also b applied for the detection and tracking.
Attacks should be logged for avoiding in future.
Artificial techniques can improve the efficiency of the given approach.

References:

1:http://searchmidmarketsecurity.techtarget.com/definition/rootkit

2: http://www.thewindowsclub.com/prevent-stealth-attacks-internet

A:
http://webpages.uncc.edu/wwang22/Research/papers/Xie-SPCC-13.pdf

B:
https://www.researchgate.net/publication/282545100_Malware_Detection_in_Cloud_Computing_Infrastructures

C:
http://ieeexplore.ieee.org/document/7371497/?reload=true