IMPROVING VIRTUAL MACHINE SECURITY THROUGH INTELLIGENT INTRUSION DETECTION SYSTEM

Ambikavathi C
Sathyabama University, Chennai, Tamilnadu, India
ambika_vathi@yahoo.co.in
http://www.sathyabamauniversity.ac.in

Dr.S.K.Srivatsa
Prathyusha Institute of Technology and Management,
Chennai, Tamilnadu, India
profsks@rediffmail.com

Abstract

Virtualization is the key feature of cloud computing which facilitates sharing of common resources among cloud users. As cloud computing is a shared facility and accessed remotely, it is vulnerable to various attacks. The shared resources may be exploited by the attackers through vulnerabilities. Virtualization technology is implemented by instantiating a virtual machine to each cloud user based on their requirements. Many virtual machines are instantiated on a single physical infrastructure. Although this virtualization technology is more beneficent for the users by means of low cost and for service providers by means of better utilization, it has several risks, in which security is the major one. Benefits of virtualization go beyond the cost savings. By better planning and management virtualization risk can be mitigated. The proposed work secures virtual machines by creating VM profiles, packet monitoring and by conducting periodic centralized vulnerability scans. It is consistent because both signature based and anomaly based IDS are combined. It is efficient because only the VMs affected by infected packets are scanned for vulnerability.

Keywords: Cloud Computing; Intrusion Detection System (IDS); Virtual Machine (VM); Vulnerability scanning.

1. INTRODUCTION

Cloud computing is emerged as a new computing platform for both the IT people and other common users because the needed computing resources can be gained at low cost. Also managing and utilizing the resources are turned into easier task. Provision and releasing of resources are done by service providers with minimal effort. No need to invest more capital expenses either for server, storage, network, hardware or software needed for business or IT industry. Cost reduction and other benefits are achieved by means of sharing, but the same sharing yields to security risks. In IaaS cloud users has the authorization to install their own developed applications and software which leads to malware installation.

Virtualization is the fundamental technology for cloud computing used to accomplish the provision of resources. Cloud computing virtually and dynamically distributes the computing and data resources to a variety of users, based on their needs. Virtualization was first implemented as a way to control IT capital and operational expenditures. Resource utilization is another major benefit gained by this computing model. The base of cloud computing lies over virtualization technology that provides a way of dynamically allocating virtual instances of physical resources, including memory, processor, storage and other computing resources. Many virtual machines are instantiated on a single physical infrastructure. VM specific attacks are penetrated into physical machine and other VM's since all created virtual machines run concurrently on the same physical machine.

1.1. *Cloud Architecture*

The cloud architecture can be divided into three layers which are the System Layer, the Platform layer and the Application layer as shown in Fig. 1 depending on the service models (IaaS, PaaS, SaaS) of cloud [7].

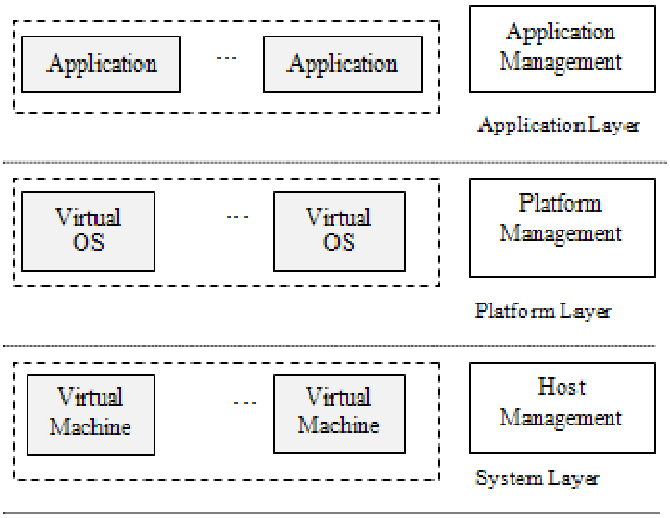

Fig. 1. Cloud Computing Architecture

1.1.1. System Layer

It is the lowest layer in the cloud architecture which includes virtualized hosts and networks. Service model delivered at this layer is referred to as Infrastructure-as-a-Service (IaaS). IaaS completely changes the way developers deploy their applications. Instead of spending big with their own data centers or managed hosting companies or services and then hiring operations staff to get it going, they can just get a virtual server running in minutes and pay only for the resources they use.

1.1.2. Platform Layer

It is the second layer in the architecture and includes virtualized operating system as well as runtimes and APIs. Service model delivered at this layer is referred to as Platform-as-a-Service (PaaS). This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service.

1.1.3. Application Layer

This layer is the top level of the architecture which provides virtual applications. Service model delivered at this layer is referred to as Software-as-a-Service (SaaS). Applications are remotely hosted by the application or the service provider and made available to the customers on demand, over the Internet.

1.2. *Intrusion Detection Issues in Cloud*

Cloud computing is an environment in which many virtual machines are instantiated on a single physical infrastructure. Being a traditional technology, Intrusion detection system contributes more to the world of security. Since cloud is a distributed environment several issues arise in the deployment of Intrusion Detection System which are:

- Analysis of huge logs

  Systematic examination of logs should be done for achieving high detection efficiency. However the efficiency is decreased because of enormous logs. Evaluation of log files provides a critical layer of defense.

- Drop of packets

  During packet monitoring which is done by IDS, packets are compared with rule set. IDS would be very busy so that packets may be dropped due to timeouts.

- Ciphered data

  Data is transferred to the cloud after encryption. Encrypted data may hide malicious code or data which cannot be checked for vulnerability.

- Vulnerable IDS

  Intrusion Detection System itself is vulnerable because it performs poorly in defending themselves from attacks.

The proposed Intelligent Intrusion Detection System overcomes all these above mentioned issues. Rest of the paper is organized as follows. Section II discusses about the related work done to increase the virtual machine security in cloud Environment. VM specific attacks are discussed briefly in Section III. Section IV, presents the

proposed work and Section V contains the conclusion and Future work. Finally it concludes with references at the end.

2. RELATED WORK

2.1. Profile Based Network IDS

Profile based network intrusion detection approach is a signature cum behavior based network intrusion detection system. The concept is of creating a VM profile database that will describe the attack patterns that needs to be looked over on the VM specific traffic. This database also contains the attacks in a ranked manner which will ensure timely detection as the patterns will be searched in the traffic in a ranked manner. The profile is updated for new attack patterns and synchronizes attack pattern parameters.

Unknown or new attacks cannot be detected by this approach is the major drawback.

2.2. Increasing VM Security

This research article[6] proposal increases the virtual machine security, based on two components: a first component called Update Checker to identify outdated packages, can check either running or dormant virtual machine images efficiently. A second component called Online Penetration Suite scans virtual machines for software vulnerabilities using established security techniques. OpenVAS and Nessus are the two scanners used by this approach. It can identify flaws in software components listening on the network.

The problems in this approach are the Update Checker checks only the software installed using package management system of current Linux distributions and Online Penetration Suite uses only two scanners.

2.3. Mirage

Mirage[11] is an Image Management System which manages the VM Images. It has an access control framework to regulate the sharing of VM images, image filters to remove unwanted information in the image, a provenance tracking mechanism to track the derivation history of an image, and a set of repository maintenance services.

The limitations of this approach are usage of filtering and simple pattern matching technique which never provides 100% accuracy.

2.4 NICE

A VM profile is created with the information about their state, services running, open ports, number of other connected VMs and other comprehensive information such as vulnerabilities, alert, traffic. This information is collected from the NICE system components which are Attack Graph Generator, NICE-Agent and Network Controller. An Attack Graph is constructed to find the virtual machine state (stable, vulnerable or exploited)

This research doesn't address how to reduce the false negative rate.

2.5 cvaframe Framework[12]

This research specifically targets on dormant virtual machine images. The framework is built on the top of the existing tools Metasploit and OpenVAS. It is implemented in an existing cloud service 'OpenNebula'. This system is able to find vulnerabilities and exploits hiding in dormant virtual machine images.

2.6 Security Architecture for VM[1]

A Security architecture is proposed having the components such as Entity validation, Intrusion detection Engine(IDE) and Dynamic Analyzer. The Entity Validation component detects the attack traffic with spoofed source address, fine granular detection of process and secure logging of new entities in the virtual machines. The IDE component is used for detection of known attacks and detection of suspicious behavior monitoring the incoming and the outgoing traffic of virtual machines. Dynamic Analyzer is used for detection of suspicious processes running in the virtual machine, detection of zero day attacks, fine granular isolation of malicious entities (processes/applications) that are generating the attack traffic, and sharing of information about suspicious behavior and attack signatures between multiple analyzers in a distributed environment.

2.7 Internet IDS

Amirreza Zarrabi., et.al. [7] proposed Cloud Intrusion Detection System Service(CIDSS) which is built around the software as a service model for providing security to any cloud based user. The CIDSS architecture is proposed which consists of light weight IDS agents integrated inside the protected network and a central detection engine unit. The concept of grouping is introduces for the flexible integration of IDS agents in to multiple network segments. Virtual Private Network(VPN) is utilized as a means of grouping and information exchange facility. A standardized interface is designed to provide a view of result report for users.

2.8. Multithreaded IDS

Ms.Parag K.Shelke, et al. [4], proposes a multithreaded NIDS model for distributed cloud environment, based on three modules: capture and queuing module, analysis/processing module and reporting module. The capture

module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set.

2.9. ANN Based IDS

Swati Ramteke., et.al. [13] proposed a novel approach for ANN-based IDS, FC-ANN, to enhance the detection precision for low-frequent attacks and detection stability. The general procedure of FC-ANN approach has the following three stages. In the first stage, a fuzzy clustering technique is used to generate different training subsets. Based on different training sets, different ANNs are trained in the second stage. In the third stage, in order to eliminate the errors of different ANNs, a meta-learner, fuzzy aggregation module, is introduced to learn again and combine the different ANN‟s results.

2.10. Trust Based IDS

Amira Bradai., et.al. [14] proposed a trust based intrusion detection system, it aims to detect possible attacks in different locations: at the user side and IaaS cloud. Enterprises should not trust their applications to IaaS providers and rely on the security processes put in place by providers. Commercial offers don't give visibility to IaaS users of advanced security primitives such as Intrusion Detection and Prevention (IDS/IPS). For this, we need to adopt a pair trust evaluation model based on three parameters: cooperativeness, honesty and efficiency.

3. PROPOSED WORK

In the proposed system intelligence is added to IDS through selected rule/signature set, securing VM images and conducting periodic scans. Selection of rule set is done based upon the factors, number of occurrences of the signature and last detection time. Hackers use the virtualized infrastructure as a launching pad for new attacks. Offenders can install vulnerable software on their VMs, which essentially contribute to loophole in cloud security. There is a challenge to found an efficient vulnerability or attack detection and response system for identifying attacks accurately and minimizing the impact of security breach to cloud users. When dealing with virtual machine security it is must to protect virtual machine images.

The proposed system is developed to improve the virtual machine security level by securing the virtual machines through VM profiling, packet monitoring and vulnerability scanning. VM profile is created for each virtual machine with its details such as OS type, CPU, RAM size, IP address, login credentials etc. Packet monitoring is done for all incoming packets to check whether the packet contains any malicious code or data. The vulnerable and exploited virtual machines can be identified by conducting periodic vulnerability scans.

Intelligent Intrusion Detection System(I-IDS) works at virtualization layer. (i-e) I-IDS is deployed on each virtual machine instantiation. A management Schema is centralized to ensure all virtual machines offer the same level of protection. Infected packets are detected by combining two IDS techniques, signature based to identify known attacks and anomaly based to identify unknown attacks.

It provides the following security management features:

- Controlled Access
- Coverage across all IP protocols
- Design policies for each Network Interface
- Detection of reconnaissance scan on VMs
- Integrity
- Prevent DDOS attacks
- VM isolation

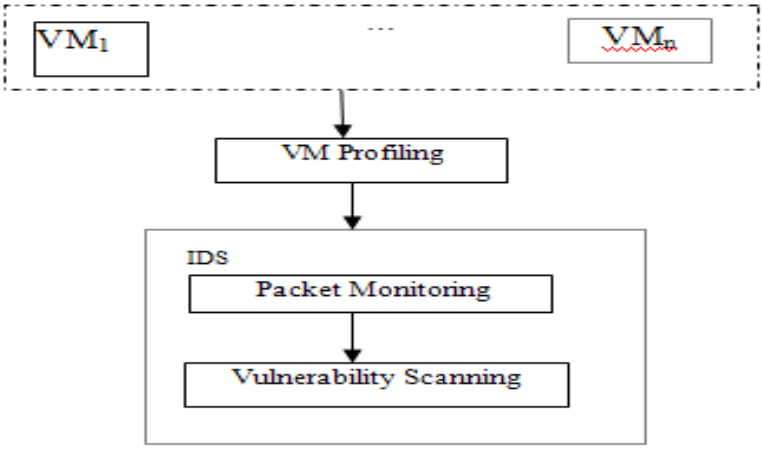

Fig. 2. Proposed Architecture

3.1. *VM Profiling*

Whenever a VM instance is created, the details of that VM such as OS type, storage size allocated, CPU usage, IP address, applications running and login credentials are stored as a profile in database, which is used later by Analyzer to identify the vulnerable and exploited VMs. Optimization of log inspection rules can ease the detection of suspicious behavior and ensure timely awareness.

3.2. *Packet Monitoring*

Packets flowing through the cloud network should be examined for signs of malicious activity. Packet monitoring for finding the infected node is done by checking the incoming packets, whether it contains any malicious code or data by means of combining two IDS techniques, signature based and anomaly based. Signature or misuse based IDS rely on the definition of misuse patterns(known attacks). It works by comparing the incoming packets with a database of malicious threats and signatures. If a match occurs, the IDS declare that packet as infected packet and the node as infected node, and it is forwarded to the vulnerability scanner.

Anomaly based IDS analyzes the network for unknown or new attacks. It works by comparing the sending data rate of each machine with a threshold value. If the sending data rate is more than the threshold then that machine is declared as 'suspect'. The increase in sending data rate may lead to deploy DDOS attack. Threshold value depends on false positive rate.

3.3. *Vulnerability Scanning*

Vulnerability is “A security flaw or weakness in an application or system that enables an attacker to compromise the target system. A compromised system can result in privilege escalation, denial of service, unauthorized data access, stolen passwords and buffer overflows” [12]. Exploit is “A program that takes advantage of a specific vulnerability and provides an attacker with access to the target system” [12]. Vulnerability is a bug in software or application created by developer, that bug can be taken as an advantage by the attacker to exploit the system or service. So these vulnerabilities should be detected by security administrator before an attacker misuses it.

Vulnerability scanning is done at the hypervisor level by vulnerability scanner, a tool that scans the entire system for known vulnerabilities stored in a database. The virtual machines affected by the infected packets are only taken into account for vulnerability scanning. So that time is saved by not scanning all machines in the distributed cloud environment. OpenVAS [6] is a versatile and powerful open source automated vulnerability scanner, used by the proposed approach. Scanning is done periodically in a centralized manner. Finally it reports the list of VMs which are stable, vulnerable and exploited.

4. IMPLEMENTATION

The proposed system is implemented using OS-SIM(Open Source – Security Information Management)[8] which comprises of traffic analyzers, vulnerability scanners and intrusion detection systems and VMware for creating virtual machines. The virtual machines are created using VMware [16]. A VM profile is created for each virtual machine as shown in Fig. 3. The traffic analyzer of OS-SIM does the packet monitoring and reports the details of infected packets such as the source IP address, destination IP address, source port, destination port, data etc as shown in Fig 4. The traffic analyzer compares packets with the selected rule set. Vulnerability scanning is done periodically by the vulnerability scanner of OS-SIM.

4.1. *PSEUDO CODE FOR VM PROFILING*

(1) InitializeComponent()
(2) for each virtual machine vm do
(3) add ip-addr, ram, os, cpu, login-details to vm-profile
(4) update status periodically

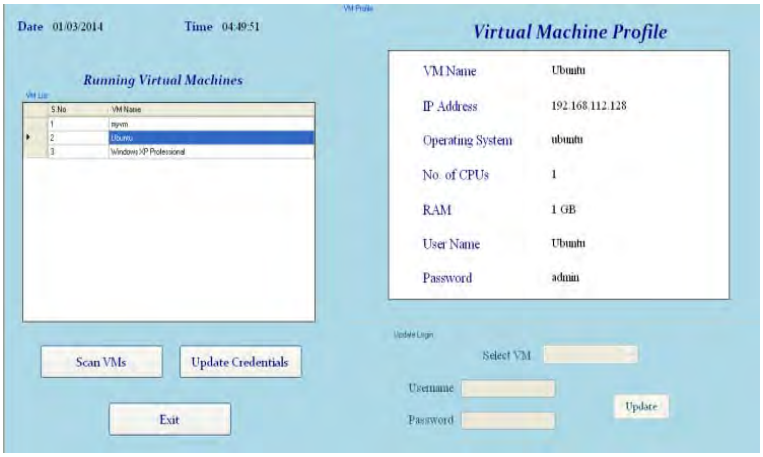

Fig. 3. VM Profile

4.2. *PSEUDO CODE FOR PACKET MONITORING*

(1) load selectedrule_set
(2) for each packet in network do
(3) get src_ipaddr, src_port, data
(4) compare data, data rate with rule-set
(5) if match occurs
(6) Packet is infected
(7) else
(8) forward the packet

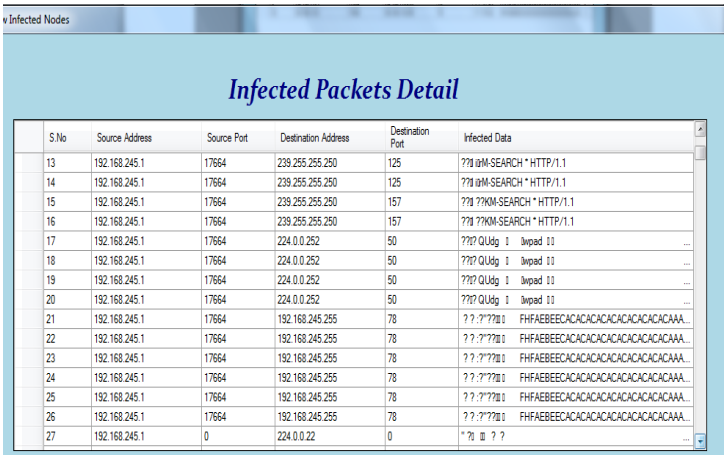

Fig. 4. Infected Packets

4.3. *PSEUDO CODE FOR SELECTED RULESET*

(1) Begin
(2) N = 0 # number of current signatures
(3) Query the database to retrieve the set of signatures detected, S
(4) for every signature f in S do
(5) Freq = number of occurrences of f
(6) LTime= last detection time of f
(7) if N <= MaxNum and Freq >= MinFreq and Ltime>=ValidTime then
(8) Remove the signature from the secondary database
(9) Add the signature in multiple IDS
(10) N = N+1
(11) end if

(12) end for

(13) End

5. CONCLUSIONS AND FUTURE WORK

Security plays a central role in preventing service failures and enhances data availability. While considering performance security need not be sacrificed. Virtualization expands the set of security vulnerabilities. In this paper we focus on the security of virtual machine which is the base for cloud computing model. Intelligent Intrusion Detection System minimizes the potential for vulnerability exploitations. Virtual machine security is improved by creating VM profiling, packet flow monitoring and conducting centralized periodic automated vulnerability scans. Integrating multiple intrusion detection technologies and getting best of each leads to intelligence. The potential to compromise a virtual machine (VM) hypervisor is reduced. In future the proposed work can be evaluated by various metrics.

References

[1] Abhishek Bichhawat, Udaya Tupakula, Vijay Varadharajan, "Security Architecture for Virtual Machines" Springer, 2011.
[2] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing Jeongkeun Lee, Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013
[3] Muhammad Zakarya & Ayaz Ali Khan, "Cloud QoS, High Availability & Service Security Issues with Solutions", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012
[4] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.
[5] "Agentless Security for Vmware Virtual Data Centers and Cloud", Trend Micro White paper, 2012
[6] Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin and Bernd Freisleben, "Increasing virtual machine security in cloud Environments", Journal of Cloud Computing: Advances, Systems and Applications 2012
[7] Amirreza Zarrabi, Alireza Zarrabi, "Internet Intrusion Detection System Service in a Cloud" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012.
[8] http://sourceforge.net/projects/os-sim/
[9] Sanchika Gupta, Padam Kumar and Ajith Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment", International Journal of Distributed Sensor Networks, Feb 2013.
[10] Hanqian Wu, Yi Ding, Chuck Winer, Li Yao, "Network Securitry for Virtual Machine in Cloud Computing"
[11] Jinpeng Wei and et. al, "Managing Security of Virtual Machine Images in a Cloud Environment" CCSW, 2009
[12] Mika D.Ayenson, "Cloud Vulnerability Assessment" Project report, April 2012.
[13] Swati Ramteke, Rajesh Dongare, Komal Ramteke, "Intrusion Detection System for Cloud Network Using FC-ANN Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2013.
[14] Amira Bradai and Hossam Afifi, "Enforcing Trust-based Intrusion Detection in Cloud Computing Using Algebraic Methods", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover,2012.
[15] Michael Gregg et al, "10 Security Concerns for Cloud Computing", Global Knowledge white paper.
[16] VMware, Virtualization for Desktop & Server, http:// www.vmware.com/in.