2012 IEEE Eighth World Congress on Services

IDS based Defense for Cloud Based Mobile Infrastructure as a Service

Sanchika Gupta
Department of Electronics and Computer Engineering
IIT Roorkee, India
Roorkee, India
sanchigr8@gmail.com

Susmita Horrow
Department of Mathematics
IIT Roorkee, India
Roorkee, India
hsusmita4@gmail.com

Anjali Sardana
Department of Electronics and Computer Engineering
IIT Roorkee, India
Roorkee, India
dr.anjalisardana@gmail.com

Abstract— **Cloud Computing has emerged as one of the rapidly growing technology. Cloud has gained popularity owing to its advantages like cost-effectiveness, pay per use, scalability and ease to upgrade. In spite of all these benefits, the risk of security is preventing many organizations to adopt cloud environment. Unless cloud become resilient to the security threats owing to the change in the computing environment, it is impossible to get the full benefit of cloud. Switching to new computing environment has added different aspects to security besides the security threats present the traditional computing environment. Hence there is a need of different security framework in order to make cloud resistant to various security threats.**

This paper presents an IDS framework for cloud to provide security from the IaaS based attacks. The IDS has got two separate modules for network based attacks and host based attacks. This paper discusses the prototype of the framework and evaluation of the framework.

Keywords- Cloud Computing, Private Cloud, Security, IDS

I. INTRODUCTION

Cloud Computing is dominating the IT market today. Independent research firm called Forrester Research in their report "Sizing the Cloud", expects the global cloud computing market to reach $241 billion in 2020 compared to $40.7 in 2010. The blue paper issued by Morgan Stanly titled as "Measuring Cloud Impact: The Coming Server Squeeze" shows cloud computing as a promising technology to dominate the market in next few years. According to the survey over next three years, 50% growth in public cloud workload is expected.

In spite of all these benefits, many organizations are hesitating to adopt cloud environment because of the risk of security. Changed computing paradigm has introduced many security aspects. Unless cloud becomes resilient to these security threats, it is impossible to get the full benefit of cloud. According to the survey conducted by Fujitsu in 2010, security and stable operation ranked highest among the user concerns. In the changed environment of cloud, the user performs its computational tasks using the computational resources residing in the vendor's premises. Hence enforcing security on the information in the distributed environment is very difficult as compared to the standalone system. Again, sharing of computational resources, storage, services and applications with other users put the privacy of user data under the risk.

Mobile Infrastructure as a Service has gained popularity [13][14]. This system provides infrastructure as a service so that it can be accessed by the mobile devices from any place. Hence this is called mobile infrastructure as a service. Due to mobility feature, the architecture becomes more prone to security threats. In this paper, we discuss the threat model for mobile infrastructure as service and propose a IDS framework to make the infrastructure more robust against attack.

The rest of the paper is organized as follows. Section II describes the threat model. Section III gives the proposed IDS architecture. Section IV discusses the implementation of a proof of concept for the proposed IDS followed by the evaluation of the system in Section V. Section VI concludes the paper.

II. THREAT MODEL

Security in Cloud Environment has two aspects. From the cloud consumer's point of view, security means the retention of confidentiality, privacy and integrity of the data that are present in the cloud provider's premises. Whereas the duty of cloud provider is to maintain the trust level of the cloud consumer as well as to protect its own infrastructure from network based and virtualization based attacks originating either from the outside of the infrastructure or inside the infrastructure. In other words the cloud consumers whose machines are running in the cloud provider's premises are also considered as potential attacker. Hence the attacker to the cloud infrastructure can be categorized as External Enemy and Internal Enemy. External Enemies are those entities which are not related to the cloud provider. Their intention is to hamper the normal

978-0-7695-4756-5/12 $26.00 © 2012 IEEE
DOI 10.1109/SERVICES.2012.45

work flow of the cloud provider. For example, they may launch DDoS attacks so that the cloud provider may be unable to render its service. Internal Enemies are the cloud consumers who work on the virtualized resources provided by the cloud provider. They may act as attacker by running malicious code in virtual machine provide to them to gain root access.

External attacker can harm the infrastructure by launching attacks like DDoS attacks, Session Hijacking and other network based attacks so that the cloud infrastructure cannot provide service reliably and efficiently. On the other hand,internal attacker has access to the virtualized resources of the cloud provider. A malicious user can take this as an opportunity to run malicious code. The following section discusses some of the security issues originating from the malicious VM.

1. VM monitoring from another VM: As VMs are linked to the host machine by a virtual switch, the intruders might use ARP poisoning to redirect the packets going to or form the other VM for sniffing.

2. Communication between host and VM: Communications between VMs and host flow between VMs through shared virtual resources like virtual network. All network packets coming from or going to a VM pass through the host and host is generally able to monitor network traffic of its hosted VMs. Hence a malicious VM can potentially access other VMs through shared memory, network connections and any other shared resources without compromising the hypervisor level.

3. VM Escape: This is the most dangerous threat to virtualization environment. It generally due to certain vulnerabilities present in the virtualization software. In this case, an improperly configured VM could allow code to completely bypass the virtual environment and obtain full root access to the physical host. This would result in a complete failure of the security mechanisms of the system. This phenomenon is called as *VM escape*. Researchers from BlackHat organization have shown feasibility of such kind of attack. Examples of such kind of attacks are CloudBurst, and Virtunoid which are based on VMWare and KVM hypervisor respectively.

4. VM Rootkits: This is based on the phenomenon of VM Escape. VM Rootkits are new classes of rootkits that are hypervisor aware which take the advantage of exploits and features of hypervisor softwares. These can compromise the hypervisor to gain control over the installed VMs, the physical system and hosted applications. HyperJacking, BLUEPILL, Vitriol, SubVir and DKSM are well-known attacks that target the virtual layer at run-time. These VM-Based Rootkits (VMBRs) are capable of inserting a malicious hypervisoror modifying the installed hypervisor to gain control over the host workload. In case of Xen Hypervisor, besides hypervisor, a privileged VM is in charge of the administrative tasks. This VM is also a potential target for hackers target to exploit vulnerabilities inside that VM to gain access to the hypervisor or the other installed VMs. In Bluepill attack, the rootkit launches a malicious VM puts the host operating system into the virtual machine and the malicious VM gains the access of the system.

5. VM Hopping: In this type of attack, an attacker on one VM gains access another victim's VM and monitors the victim's resource usage, modify its configurations and delete stored data, endangering the VM's confidentiality, integrity and availability. For this attack, the attacker and victim VM must be running on the same host. The attacker must know the victim VM's IP address. Thomas Ristenpart et al [15] have shown the feasibility of such kinds of attack where an attacker can obtain or determine the IP address using standard customer capabilities. Furthermore, multi-tenancy makes the impact the impact of a VM hopping attack potentially larger than in a conventional IT environment.

III. PROPOSED IDS ARCHITECTURE

The figure 1 shows the proposed architecture of the IDS for cloud system. The security framework has the following components:

1. Monitoring Module
2. Detection and Classification Module
3. Response Module
4. Security Manager

The first three components reside in each cluster node and the component Security Manager resides inside the controlling node. The modules residing each cluster node take care of the events happening inside the virtual machine it is hosting. Placement of Security Manager in the front end gives

A. *Monitoring Module*

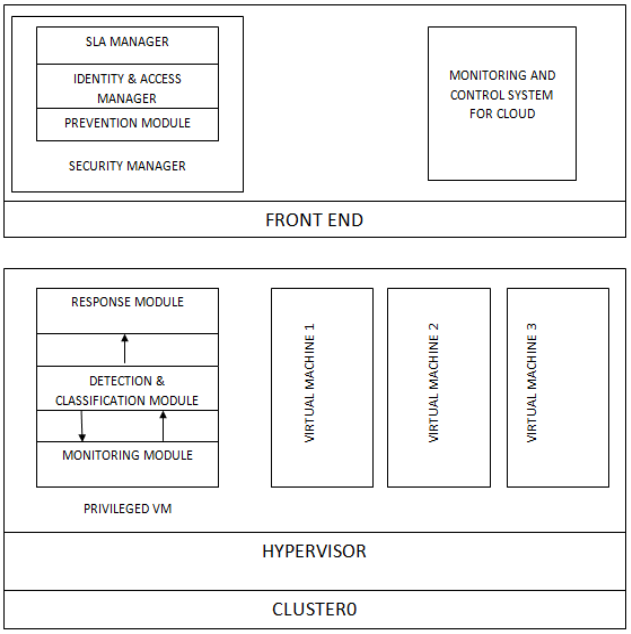

Figure 1: Proposed IDS Architecture

The job of this module is to gather information about the events and pass the information to the detection module and classification module. Two kinds of monitoring modules are deployed. One kind of monitoring module is called network monitor module. It is responsible for gathering information about network traffic. The other kind of monitoring module gives information about the virtual machines. For network monitoring Wireshark is used and for monitoring virtual machines, a virtual machine introspection tool, libvmi is used. The information gathered from the both the module are sent to the Detection and Classification module.

B. *Detection and classification Module*

The information regarding the events is fed to the Detection and Classification module. This module would analyse the information and decide whether the state of the system is normal or compromised. If any attack is detected, then this module will classify the attack and invoke the Response Module to take appropriate action.

C. *Response Module*

The job of this module is to take appropriate action regarding the threat detected by the detection module. The action may include sending warning message to the virtual machine user, suspending the virtual machine or shutting down the virtual machine.

D. *Security Manager*

The security manager is responsible to take care of the security components residing in the controlling nodes. The

Security manager components have got two sub components such as 1.SLA (Service Level Agreement) Manager, 2.Identity and Access Manager, 3.Prevention Module.

1) SLA Manager: This deals with the policies agreed upon by the customer and vendor.

2) Identity and Access Manager: This component deals with the customer membership, authentication, authorization and access control.

3) Prevention Module: The job of this module is to make the system more resistant to future attacks. This module deals with the management of patch of virtualization software as well as the cloud computing software. Zero day attack signatures are updated in the module and these signatures are distributed over the signature database like Detection and Classification module.

IV. IMPLEMENTATION

A. *Implementation of Private cloud*

For this work, a private cloud was deployed in a computing laboratory with 20 computers. One of the computers was made front end and other computers were treated as clusters. The aim was to build a secure private cloud to provide mobile IaaS with existing hardware. The private cloud is deployed using an open source cloud computing tool kit OpenNebula.

Table 1 gives the specification of the available computing resources.

TABLE 1

SPECIFICATIONS OF THE COMPUTER SYSTEM TAKEN

Operating System	Ubuntu 11.10
File Sharing	NFS
Hypervisor techniques used	KVM
RAM	2 GB
Hard Disk	300 GB
Processor	Core2 Duo

B. *Implementation of proof of concept of IDS architecture*

As a proof of concept, a monitoring and response module have been implemented for network based attacks. For this a network based attack TCP SYN Flood attack was chosen. Here the goal is to protect our infrastructure from the outside SYN Flood attack and prevent the virtual machines running in our premises to launch such kind of attack. For this, we have developed a network monitoring module using libpcap library. This module keeps track of the network traffic flowing through the particular interface. Then we developed a detector to detect the SYNFlood attack based on the algorithm proposed by Gavaskar et al [16]. The algorithm is explained in the figure 2.

The following data structures were used:

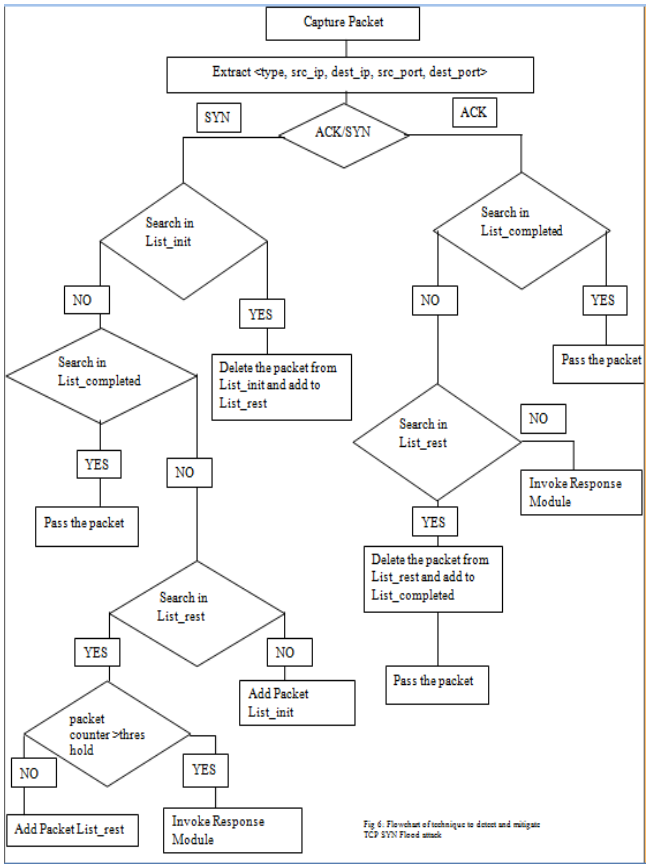

Figure 2: Flow chart of working of SYN Flood filter

struct packet with data members: <type; src_ip; dest_ip; src_port; dest_port; count >
*struct list_node with data members: < packet item, packet *next>*
*struct list with data member: <list_node *head>*

Three lists are maintained to store the state of the TCP connections.
List_init: Keeps track of the first SYN packets of each TCP connection
List_completed: Keeps track of the TCP connections which have completed three way handshaking
List_rest: Keeps track of rest of the SYN packets

The response module is designed as a script which contains set if iptable rules. Here as a response to attack, we are dropping the packets from the malicious source.

V. EVALUATION

E. *Evaluation of Performance of the proposed IDS*

To evaluate the system we launched TCP SYN Flood attack and measured the CPU utilization for each time interval of 30 seconds. We marked the time when the CPU is exhausted. To generate TCP SYN Flood attack, we have used a tool called" hping3." It is a network tool able to send custom TCP/IP packets. Then we started our monitoring and response module and the launched attack. The CPU utilization in this case is also measured for the interval of 30 seconds. Figure 3 shows the comparison. It shows that during attack, without IDS the CPU gets exhausted. But when the IDS is used, the CPU utilization becomes normal.

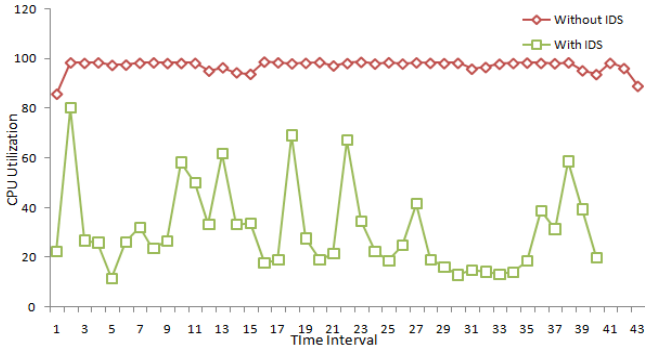

Figure 3. Graph showing comparison of CPU utilization using IDS and without using IDS

VI. CONCLUSIONS

In this paper, we have proposed and evaluated the IDS based Defense for Cloud Based Mobile Infrastructure as Service. As a proof of concept, we have implemented network filter for TCP SYN Flood attack. The future work is directed to implement this for real time environment and evaluate for other type of attacks.

ACKNOWLEDGMENT

We are grateful to all the persons involved in mailing lists, development and documentation of OpenNebula project.

REFERENCES

[1] A.T. Velte, T.J. Velte and R. Elsenpeter, *CloudComputing – A Practical Approach*, Wiley Publishing,Inc. 2011.

[2] B. Sosinsky, *Cloud Computing Bible*, McGraw-Hill Companies, 2010.

[3] (2011) The OpenNebula website [Online]. Available :http://www.opennebula.org/

[4] (2011) OpenNebula Workshop. [Online].Available: http://hpc.uamr.de/wissen/opennebula-workshop/OpenNebula workshop.

[5] R.S. Montero, "Building Clouds with OpenNebula 1.4," CESGA Santiago de Compostela, Spain, January 2010.

[6] R.S. Montero," Deployment of Private and Hybrid Clouds Using OpenNebula/ RESERVOIR", Open Grid Forum 28, March 15-18, 2010.

[7] M. A. Morsy, J. Grundy, and I. Miller, "An Analysis of The Cloud Computing Security Problem," in Proc. APSEC, 2010 Cloud Workshop.

[8] A.S. Ibrahim, J. Hamlyn-Harris, and J. Gurundy, "Emerging Security Challenges of Cloud Virtual Infrastructure," in Proc. APSEC, 2010 Cloud Workshop.

[9] H. Tsai, M.Siebenhaar, A. Miede, Y. Huang, and R. Steinmetz, "Threat as a Service? Virtualization's Impact on Cloud Security", IT Professional, vol. 14, no. 1, pp.32-37.

[10] F. Sabahi, "Cloud Computing Security Threats and Responses", 3rd International Conference on Communication Software and Networks (ICCSN), IEEE,2011, pp.245-249.doi:dx.doi.org/10.1109/ICCSN.2011.6014715.

[11] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou," Security and Privacy in Cloud Computing: A Survey," in sixth Int. Conference on Semantics, Knowledge and Grid (SKG), pp.105-111,Nov. 2010.doi:dx.doi.org/10.1109/SKG.2010.19.

[12] W. Dawoud, I. Takouna, and C. Meinel," Infrastructure as a service security: Challenges and solutions," in 7th International Conference on Informatics and Systems (INFOS), pp.1-8, March. 2010.

[13] S. Horrow, S. Gupta, and A. Sardana, "Implementation of Private Cloud at IIT Roorkee: An Initial Experience", in International Workshop on Cloud Computing & Identity Management(CloudID 2012). in press.

[14] S.Horrow, S. Gupta, A. Sardana, and A. Abraham,"Secure Private Cloud Architecture for Mobile Infrastructure as a Service", in 8th IEEE World Congress on Services (IEEE Services 2012).in press.

[15] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", in Proc. Sixteenth ACM Conf. Computer and Communication Security (CCS 09), ACM Press, 2009, pp. 119-212.doi:dx.doi.org/10.1145/1653662.1653687.

[16] S. Gavaskar,R.Surendiran and Dr.E.Ramaraj"Three Counter Defence Mechanism for TCP SYN Flooding Attacks", International Journal of Computer Applications (0975 – 8887) Volume 6- No.6, September 2010.