A Comprehensive Approach to Secure Cloud Architecture Design

Mr. David R. Johnson[1] and Ms. Emily W. Taylor[2]
[1]Assistant Professor, Department of Computer Science, Stanford University, California, USA
[2]Assistant Professor, Department of Computer Science, Massachusetts Institute of Technology, Cambridge, USA

ABSTRACT

In today's life Cloud Computing play a very important role for the data storage and the various internet based services. Cloud provider offers a Infrastructure as a service to its customer. In current scenario ,with the global consideration there is raise in need of a more secure environment, as many applications/services uses cloud as a basic element .With the advancement of new technologies in the field of communication there is also advancement in the attacks on particular services which is a bigger concern to avoid losses in terms of infrastructures ,financial data ,personal data .So with these concern there is a need of a secure architecture design for cloud based environment which can be helpful to both ,cloud service provider and customer of customers. This paper aims to analyze the attacks in cloud environment and describes how different types of attacks are counteracted by the proposed techniques.

Keywords: Security architecture, Infrastructure as a Service, Privacy and Security.

I. INTRODUCTION

Cloud Computing is a technology where cloud service providers make available resources to their customers to perform their computing tasks. Three types of services proposed by NIST on cloud such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[1]. The required infrastructure Iaas offers as a service. The client need not purchase the network resources, servers, or data center. The main advantage is that customers need to pay simply for the time period they use the service. As a result customers can achieve a much faster service delivery with less cost [2].

In general the customer in the cloud can run different types of application and operating systems in their virtual machines. As the customer's operating systems and applications can be potentially huge and complex so they may include security vulnerabilities. These vulnerabilities broken by attacker to create different type of attacks. Belonging to other customers these attacks can be targeted against the cloud infrastructure and virtual machines. Generally cloud service provider do not offer any type of security to their customers Amazon [3] states that the security of customers virtual machine is the responsibility of the customers. Thus customers have to make their individual arrangements for securing their virtual machines in cloud environment. Customer can use anti-virus and detection of host based intrusion security tool to secure their virtual machine but some limitations occur due to these security tools. In addition several customers may not be able of securing their customers virtual machines. Thus there is a need for the cloud provider to offer security to such type of customer.

II. ATTACKS ON VIRTUAL MACHINE IN CLOUD ENVIRONMENT

2.1 VM Escape

Virtual machines are permitted to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host. It means, the virtual machines are intended like that a program running in one virtual machine cannot communicate either with programs running in other VMs or with the programs running in the host. But in actuality the organizations compromise isolation.

VM Escape is the attack in which VM runs malicious code into VMM and get complete information about the host and its operating system. Attacker breaks the process of virtual machine and directly interacts with the hypervisor. A hypervisor is also called as Virtual Machine Monitor. It is located between the guest operating system and the hardware.

2.2 Guest to Guest Attack

Virtual machine communication refers guest-to-guest attack [4]. On the same hypervisor attackers use one virtual machine to control or access other virtual machine. This type of attack can happen without comprising the hypervisor layer. A malicious virtual machine is able to potentially access other virtual machines through shared resources, network connection and shared memory. For example, if a malicious VM find out where an additional VM's assigns memory lies, then it could write or read to that location and interfere with the other's operation. Figure 1. Shows guest –to-guest attack.

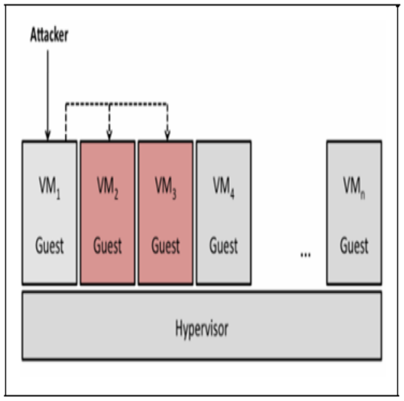

Figure1:- Guest-to-guest attack on VM2 and VM3

2.3 IP Spoofing

Using spoofing technique an intruder can break the security of the system. IP spoofing is the technique that hacker used to VM that packet is coming from trusted IP address and not from malicious one. There are various ways to put an end to the spoofing packets. And these ways are as described as follows:

Ingress/Egress filtering at the origin: Along with ingress/egress filtering, the network operator makes setting to their routers to dribble any packet whose IP address is from unallocated address space or any bongos address. Reverse Path Forwarding feature [8], can be used to drop the packets whose source address is not mentioned in the forwarding table.

Trace back: This technique is used to determine the source of attacker traffic in the Internet. This feature can be added to the capabilities of the routers in two different ways. First is the way to involve stamping the traffic packets with a signature of the routers they pass through [9]. Second way involves sending samples of the packets to the special collector for analysis [10].

To mitigate the packets at the destination: To alleviate the DDOS attack, TCP intercept concept is used. In TCP intercept, the router uses 3-way handshake on behalf of destination server to check whether the source host is genuine [11]. The router makes a connection on behalf of the client, if the connection with the client is established successfully. The router here acts as a TCP slicer, which means it joins the two connections together but transparently.

2.4. Denial of Service

In virtual machine architecture the host and guest machines share the physical resources such as memory disk, CPU, and network resource. Therefore it is possible for a guest virtual machine to enforce a denial of service attack to other guests residing in the same system. In virtual environment denial of service attack described as an attack when a guest machine gets all the possible resources of the system. For this reason, the system denies the service to other virtual machines. The VM making request for resources, because no resource available for other virtual machines. So the solution for this to prevent a guest consuming all the resources is to limit the resources allocated to the guests. Modern virtualization technologies propose a mechanism to limit the resources allocated to each virtual machine in the environment. Therefore the fundamental virtualization technology should be properly configured, which can then prevent one guest consuming all the available resources, thereby preventing the denial of service attack [12].

III. RELATED WORK

Folios Tsifountidis and Dr Geraint [6] Virtual Machine Introspection (VMI) technique is used to overcome VM-Escape attack. In this technique they constructed a separate virtual machine which manage all other virtual machines and keep the resource allocation strategies. This technique was based on a dedicated VM responsible for managing and protecting all other VMs. All virtual machine first communicate with special VM and after that this special VM communicate with VMM i.e. .hypervisor. As all security operations were performed with the VMM's assistance, the monitoring process incurs little performance overhead. The security VM is isolated from the other guest VMs and runs with higher privileges than the guest VMs. This adds an extra layer of protection against malware attacks that originate in the unprivileged VM. Figure2 from [6] depicts the VMI's topology within the infrastructure.

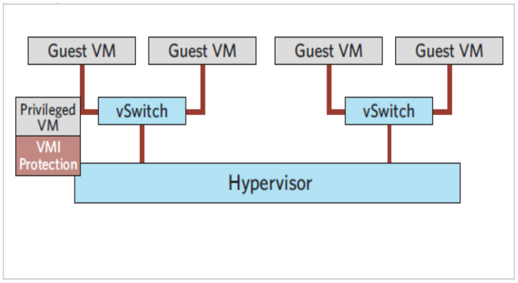

Fig.2. Virtual Machine Introspection

Anat Bremler-Barr Hanoch Levy [7] examined the packet-spoofing problem of the Internet and proposed Spoofing Prevention Method (SPM), which was used for filtering spoofed IP packets. SPM can be use as another method by networks routers to get rid of or condense spoofing attacks. The method implemented using a simple key mechanism, to be used by the participants of SPM. They analyzed the benefits of SPM and demonstrated that it forms and cost-effective solution since a network that elected to deploy it can derive significant relative benefits to its servers as well as to its clients, and thus has the incentive to invest in its placements. Also, this advancement is considerable even when SPM is only deployed by a fraction of the Internet networks and even if it is deployed without ingress/egress filtering.

Udaya Tupakula, Vijay Vardharajan [5] proposed Baseline Security Architecture model, where Cloud provider provides security as a service to its customer with its infrastructure. There are two components used in this architecture i.e. SPAD (Service Provider Attack Detection) and TSAD (Tenant Specific Attack Detection). The main objective of SPAD component is to make sure that the customer's virtual machine will not send any type of malicious files with spoof files to the host. This mechanism is use to prevent attacks from the customer virtual machine with change address. A TSAD component is use to detect tenant to tenant attack. Their proposed architecture is useful to resist various types of attacks and provide the security to the cloud provider's infrastructure as well as tenant's infrastructure. In this paper main contribution of author designed security architecture, where cloud service provider gives security as a service to its customer

C. Yu, et al [13] PSVM Model. Virtual machine security issues have been the center of attention. The permissions of established administrative domain Dom0 are very large, as a result that the user's privacy is threatened. One time the attacker compromises Dom0 means it can threaten the total virtualization platform. This paper introduced a privilege separation virtual machine security model (PSVM). Dom0's privileges are divided into two parts: First responsible for managing the user's privacy i.e., operations concerning the user's privacy form a DomU management domain, residual form Thin Dom0. For this virtualization platform for server side and users need mutual authentication. This scenario prevented unauthorized users and forged Virtualization platform invading system. The privacy of user's is in its own management for preventing the Virtualization platform snooping. Even if the management domain is compromised, it affects only one user.

IV. PROPOSED SYSTEM

In this proposed work we are trying to design a secure architecture to provide a security to the customer's virtual machine in cloud environment. Virtual machine can face various attacks as discussed in section III, out of which VM Escape attack & IP spoofing attack can be avoided by using Virtual machine monitoring introspection technique and spoofing prevention method.

4.1 VM Creation

Module 1 actually involves the setup of the application. The VM creation is performed in this task. We need to build the VM monitor tool i.e. VMM. We used the three entities like cloud service provider i.e. host, tenants refer as cloud customer and virtual machine monitor VMM also called hypervisor.

Hypervisor present between the host OS (cloud provider) and the guest OS (VM).It is software that maintain the communication between the VM and the hardware and keep the information about the cloud provider and its tenants.

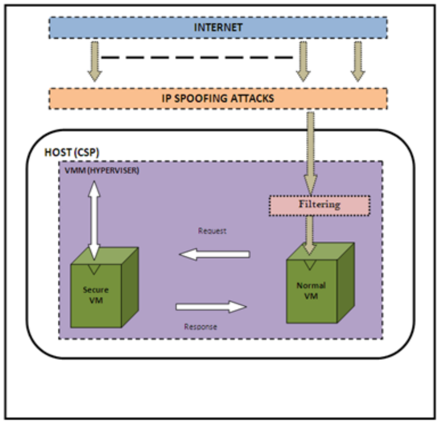

Figure 3 System Architecture

4.2 VM Escape and Host Intrusion

In this module we apply virtual machine monitoring introspection technique. For this method we created a normal VM and Secure virtual machine. First normal VM communicate with the secure VM and after that secure VM communicate with the hypervisor. VM escape attack is possible from normal virtual machine so we just stop the code execution of normal VM like operating system information, network information.

4.3 IP Spoofing

In this module we show IP spoofing attack. To show this type of attack we will simply send few files from one project to our VM and we will change the source IP of that packet and send to virtual machine. The VM has to respond to it and we need to maintain the reaction and we need to apply Egress filtering technique to check the validity of IP address at destination end.

Egress filtering is divided into two categories which are Probabilistic Packet Marking and Deterministic Packet Marking. We are using Deterministic Packet Marking technique. In this technique host address is calculated from IP address by splitting IP address into bits. The host in spoofed IP address is different and long.

4.4 Analysis

The performance of our method with existing scheme in term of execution time and development cost will be performing.

V. CONCLUSION

In this paper we proposed a secured architecture where a cloud provider provides a security to the tenant's virtual machines in cloud environment. The paper has described how the VM Escape and IP spoofing attacks can be avoided by the proposed architecture. Thus we can see how the various types of attacks on cloud can be avoided by using proposed system which increases the security while using the cloud environment

REFERENCES

[1] *P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.*

[2] *Cloud Computing - Concepts, Architecture and Challenges Yashpalsinh Jadeja, Kirit Modi 2012 Intenational Conference on Computing, Electronics and Electrical Technologies [ICCEET].*

[3] *"AWSsecurity center".Available:http://aws.amazon.com/security .*

[4] *Jenni Susan Reuben, "A Survey on Virtual Machine Security," in TKK T-110.5290 Seminar on Network Security 2007-10- 11/12.*

[5] *Vijay Vardharajan , Udaya Tupakula "Security as a Service Model for Cloud Environment" , IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 11, NO. 1, MARCH 2014*

[6] *Fotios Tsifountidis and Dr Geraint Price, "Virtualisation Security: Virtual Macine Monitoring and Introspection," Royal Holloway Series 2011.*

[7] *Anat Bremler-barr , Hanoch Levy, "Spoofing Prevention method" , In Proc. IEEE INFOCOM 2005.*

[8] *Cisco IOS, "Unicast reverse path forwarding," 1999.*

[9] *Stefan Savage, David Wetherall, Anna R. Karlin, and Tom Anderson, "Practical network support for IP traceback," in SIGCOMM, 2000, pp. 295– 306.*

[10] *Steve Bellovin, Marcus Leech, and Tom Taylor, "Icmp traceback messages," Tech. Rep., February 2003, http://www.ietf.org/internet-drafts/draft-ietf- itrace-04.txt.*

[11] *Cisco IOS, "Configuring tcp intercept (prevent denial-of-service attacks)," 1997.*

[12] *J. Kirch. Virtual machine security guidelines. The center for Internet Security, September 2007.http://www.cisecurity.org/tools2/vm/ CIS_VM_Benchmark_v1.0.pdf.*

[13] *C.Yu, et al., "Protecting the security and privacy of the virtual machine through privilege sepration," in Proc 2013 Int. conf. Compt.Sci.Electron. Eng.*