International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 6 (2013), pp. 533-538
© International Research Publications House
http://www. irphouse.com /ijict.htm

Hypervisor Security - A Major Concern

[1]Nancy Arya, [2]Mukesh Gidwani and [3]Shailendra Kumar Gupta

[1]Computer Science, Jagannath University, Jaipur.
[2]Computer Science, Jagannath University, Jaipur.
[3]Dept. of Physics, University of Rajasthan, Jaipur.

Abstract

In the last few decades, the world of computation moves for the cloud computing. Cloud computing is a new delivery model for enabling convenient ,on-demand network access of the computing resources .The cloud computing is one of today’s most exciting technologies, because it can reduce the cost and complexity of applications, and it is flexible and scalable. Virtualization is one of most important element that makes cloud computing. A key Part of virtualization is the all -powerful hypervisor which manages the physical platform and can access all of its resources. Security is the biggest problem in virtual environment. The security of a virtualization is heavily dependent on the hypervisor. If the management environment is compromised, all the virtual machines can be easily copied and modified. Furthermore, attacks from the management environment easily bypass the security mechanisms present in guest virtual machines due to the higher privilege level of the management operating system. Virtual Machine Monitor also called Hypervisor can be unsecure for the guest virtual machines. This paper looks at the hypervisor environment security attacks, possible solutions and precautions against these attacks to maintain security.

Keywords: Cloud Computing, Virtualization, Virtual Machine Monitor, Hypervisor.

1. Introduction

Cloud computing is model that makes reference to the two essential concepts: ‘abstraction’ and ‘virtualization’ to increase the capacity and capability of IT by providing on demand. Security is the major concern for this system, because the services of cloud computing is based on the sharing. Virtualization is one of most important element that makes cloud computing. Virtualization is a term that refers to the abstraction of computer resources. The purpose of virtual computing environment is to improve resource utilization by providing a unified integrated operating platform for users and applications based on aggregation of heterogeneous and autonomous resources. The main component of virtualized system is hypervisor and is responsible to enforce isolation between virtual machines and resource management of the hardware. Hypervisor is the software which permits multiple guest virtual machines to run concomitantly at the same server. The security of a virtualization is heavily dependent on the individual security of each component, from the hypervisor and host operating system to guest operating systems, applications and storage. Hypervisor is the main controller of any access to the physical server resources by virtual machines. Any compromise of the hypervisor violates the security of the virtual machines because all virtual machines operations become traced unencrypted[3]. Security breach in the host machine can result in major compromise of the whole infrastructure [6]. Attacker might take advantage of the vulnerability in virtual machine monitor [4]. Hypervisor is the single point of failure. So, the hypervisor also needs to be carefully monitored for signs of compromise. Hypervisor security can be breach by various malicious attack. Considering malicious intruders, there are many kinds of possible attacks, such as client-server architecture attacks and browser based attacks. These attacks includes session hijacking, man-in-the-middle attack, flooding attack, Malware-Injection attack. Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. It is used to refer to the theft of a cookie used to authenticate a user to a remote server . A flooding attack is an attempt by a hacker to a flood on target system A flooding attack occurs when an attacker generates bogus data, which could be resource requests or some type of code to be run in the application of a legitimate user, engaging the server’s CPU, memory and all other devices to compute the malware requests. The servers finally end up reaching their maximum capacity, and thereby offload to another server, which results in flooding. In Man-in-the-middle attack, attackers can place themselves in the communication’s path, there is the possibility that they intercept and modify communications. In a malware injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the hypervisor. Considering the above attacks, one of the main focuses of hypervisor is its security. This paper, focus on some major security attacks on hypervisor in cloud computation and solutions against these attacks. The rest of this paper is organized as follows. In the next section, related work are described. In Section III some security issues and the root causes are elaborated upon, followed by some approaches to solve these problems. Finally the conclusion is presented with future work and improvements in Section IV.

2. Related Work

The main objective behind this work is the discovery of security risks that virtualized environments face, and the security attacks which is possible on hypervisor environment. Isolated cloud environment is used to perform attack on some hypervisor environment security. TYPE I hypervisor is used to perform this work. Type I (Native, Bare Metal) hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems. The Citrix Xen Server and Microsoft Hyper-V hypervisor are examples of Type I hypervisors. Since, hypervisor is responsible for creation and management of virtual machines. By attacking on hypervisor ,attacker can gain access to all guest machines that is running on host machine . Security can be related to the number of client-server domain. Basically work related to the following notions of attack surface areas [1]:

- **Service-to-User**: This is the common server-to-client interface, thus enabling (and being vulnerable to) all kinds of attacks that are possible in common client-server-architectures as well such as man-in-the-middle, cloud malware injection attack.
- **User-to-Service**: This is the common environment a client program provides to a server, e.g. browser-based attacks for an HTML based service attacks on browser caches and sessions.

3. Security Attacks and Solutions

This section focus on specific problems for various kinds of attacks in the cloud: a) Session Hijacking, b) Man-in-the-middle attack c) Flooding attack, d) Cloud Malware-injection attack. This section describe each of these prime security issues in cloud systems, depict their root causes and approaches to mitigate such attacks to ensure the integrity and security of cloud systems.

Session Hijacking problem and solution: Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress. If any client associates with cloud using hypervisor, then client will use services of hypervisor. To access services, client authentication (login and password) is must .After login, session id will generate. Attacker can hijack that session by cookie stealing. This can be very severe problem if attacker hijacks the session of host machine (on which hypervisor is running) and can get all access to all guest virtual machines which is running on host machine. If the management environment is compromised, all the virtual machines can be easily copied and modified. So, Session id should be regenerate frequently in the small time duration after a successful login. This prevents session fixation.

Man-in-the-Middle(MITM) attack problem and solution: This attack is carried out when an attacker places himself between two machines .The man-in-the-middle attack uses a technique called ARP spoofing/ARP poisoning to trick machine A into thinking that it is communicating with machine B computer and vice versa . When data is exchanged between two virtual machines ,one attacker machine is placed in the path of communication of virtual machines. This causes network traffic between the two computers to flow through the attacker’s system, which enables the attacker to inspect all the data. ARP spoofing is a technique whereby an attacker sends fake spoofed messages onto a receiver. ARP spoofing was performed to forward the incoming request to attacker's machine port. By attacking on one virtual machine ,attacker can gain access to host machine and other guest machines. So, hypervisor should use Intrusion Detection Systems (IDS) to detect ARP Poisoning attacks.

Flooding attack problem and solution*:* When an attacker has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the host machine to seized the services which can destroy the system and network and it also can occupy the computer resources such as CPU, ram, buffer, and network bandwidth. By using different attacks and scripts, large amount of traffic can be send on host machine to slow down the services.TCP SYN Flooding attack is the most popular attack for this. Normally when a client attempts to start a TCP connection to exchange a series of messages between various machines which normally runs like this:

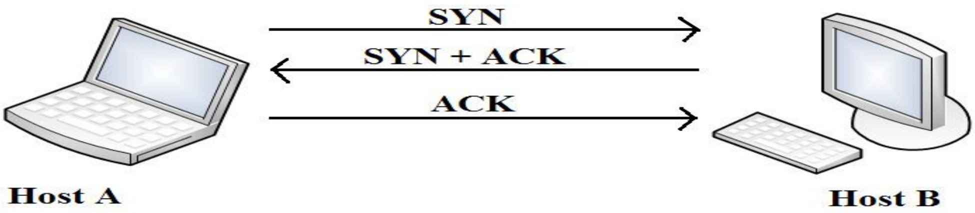

Figure 1: TCP Three Way Handshake.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol. A SYN flood attack works by not responding to the server with the expected `ACK` code. The malicious client machine can either simply not send the expected `ACK`, or by spoofing the source IP address in the `SYN`, causing the server to send the `SYN-ACK` to a falsified IP address - which will not send an `ACK` because it knows that it never sent a `SYN` .If the hypervisor is locally breached, attacker can easily get access on guest virtual machines. So, Hypervisor should check the assignment of instances to the host machines regularly. One of the main tasks for the defense mechanism is to monitor the TCP control packets that comes in and goes out of the domain. In order to detect SYN flooding attacks at its early stage, the proposed approach based on the fact that the number of SYN packets, SYN/ACK packets and ACK packets which are forwarded by source are equal in normal network traffic. Furthermore host machine connect guest virtual machines to Internet, so it can quickly detect some suspicious address whether can be attained.

Cloud Malware injection attack problem and solution: Malware injection is an attack method where hackers insert malicious code into applications to gain access to a user's computing resources, applications, or databases. The attacker then performs tasks like manipulating data, stealing personal information, or further spreading the bogus code. If the attacker is successful, then the hypervisor service will suffer from eavesdropping. Virtual machines installed on the hypervisor can also be affected by malicious attacks. This attack related to web service attack in which attacker can scan all the ports of host machine and virtual machines to find out which port service is open and then attacker can misuse those services. So, Hypervisor should not allow malicious or vulnerable machine in its template (environment). If any vulnerable ports or vulnerable machine is found, then hypervisor should inform owner of that machine and request to block all the vulnerable ports.

4. Conclusion

Cloud computing is revolutionizing how information technology resources and services are used and managed. As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. This paper depicted some crucial and well known security attacks of different security notions that can be possible on hypervisor. This paper also proposed some potential solutions and precautions to maintain security.

In the future, research should aim to provide new architectures, policies and techniques to maintain security on higher level for hypervisors**.** The concepts have discussed here will help to build a strong architecture for hypervisor security in the field of cloud computation. This kind of structured security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computing concept for industrial as well as future research farms. Lastly, this paper gives a strong theoretical concepts for security in order to build a more generalized architecture to prevent different kinds of attacks.

References

[1] Overview *of Attacks on cloud Computing, Ajey Singh, Dr. Maneesh Shrivastava, IJEIT, Volume 1,Issue 4,April 2012.*

[2] Kazi Zunnurhainand, Susan V. Vrbsky, Security Attacks and Solutions in Clouds.

[3] Anas BOUAYAD, Asmae BLILA T, Nourel houda MEJHED, Mohammed EL GHAZI, Cloud computing : security challenges, 2012 IEEE.

[4] Saketh Bharadwaja, Weiqing Sun, Mohammed Niamat ,Fangyang Shen, Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System, 2011 Eighth International Conference on Information Technology: New Generations.

[5] Akhil Behl, Emerging Security Challenges in Cloud Computing, 2011 IEEE.

[6] Qian Chen, Rajat Mehrotra, Abhishek Dubeyy, Sherif Abdelwahed, Krisa Rowlandz, On State of The Art in Virtual Machine Security, 2012 IEEE.

[7] Jyotiprakash Sahoo,Subasish Mohapatra,Radha Lath, Virtualization: A Survey On Concepts, Taxonomy And Associated Security Issues, 2010 IEEE.