Penerbit Akademia Baru

Advanced Research in Computing and Applications
ISSN (online): XXXX-XXXX | Vol. 1, No. 1. Pages 1-5, 2015

Hypervisor Security Issues in Cloud Computing: The Need to Mitigate the Risks

A. S. Thiab[*,1,a]*, and A. S. Shibghatullah*[2,b]

[1,2]Optimization, Modelling, Analysis, Simulation and Scheduling (OptiMASS) Research Group, Fakulti Teknologi Maklumat & Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[1]Department of Computer Sciences, University of Technology Baghdad, Iraq.
[a,*]*alishawket1@gmail.com,* [b]*samad@utem.edu.my*

Abstract- *A study was undertaken to study the risks and the threats to hypervisor intrusion. Experiments were carried out, and a review of literature was undertaken in order to be able to understand the depths and the methods of threats and intrusion that could cause security breaches in the hypervisor. The results of the experiment showed that in two experiments the results were similar and in the other three similar experiments carried out the results varied. As a result it was clear that there are perceived threats to the hypervisor but there are also possible ways to mitigate the threats as a method of prevention of any type of intrusion into the hypervisor. The hypervisor is the key to shared resources in the cloud computing system.* ***Copyright © 2015 Penerbit Akademia Baru - All rights reserved.***

Keywords: Hypervisor, Intrusions, Risks, Cloud Computing

1.0 INTRODUCTION

The purpose of the advanced technology in Information Technology is Cloud Computing. The purpose of this form of computing is to enable shared resources that are accessible from many locations simultaneously. This is considered to be the technology on which all future business will be dependent but at the same time there are different types of security breaches that occur because of the advancement in technology where intruders and penetrators try to stay ahead of real time technology. The hypervisor is the component of the cloud computing system which emulates the physical infrastructure and controls as set of guest machines that are created called virtual machines that operate of an abstract platform [9]. The benefit of virtualization is that it brings with it the speed and the scalability of the entire cloud computing system which is why the hypervisor has been considered to be an important part of the cloud computing system that is essential not as a component but is essential because of the functions of the component that are critical for the cloud computing system [8].

The service providers provide the cloud computing services through the internet which is a vast space of open communication and hence the security these are real threats and not perceived threats.

2.0. TYPES OF INTRUSIONS

Having studied and carried out experiments with the hypervisor several types of intrusions were found to occur when the processes of the hypervisor was disrupted during the experiments carried out. The types if intrusions that surfaced were basically six different types of attacks.

2.1 Attacks from Insiders

These are attacks that occur when an insider user o the service provided by the cloud computing service providers commits a fraud or makes an unauthorized intrusion in a system where originally no access has been granted to the user by the system.

2.2 The Flooding Intrusions

This is a form of intrusion where there is a Denial of Service (DoS) created whereby the receiver is flooded with mail of different packets which are usually TCP, ICMP or UDP. Sometimes it can me a mixed combination of all three types.

2.3 Root Attacks

The attacker gains a legitimate access to a person's account by finding out the password. The vulnerabilities are intruded upon and used or exploited for personal gains of the intruder. By this method the attacker is able to gain root level access to the host or the virtual machine to infect the virtual platform [6].

2.4 The Port Scanning Attacks

This method provides a list of all the open ports, closed ports and the filtered ports when scanned. The intruders use the open ports to enter and relay messages of intrusion or infection that will enable them to get control of the system. In this form of attack all the details become vulnerable. For example the IP address, the MAC address, gateway filtering, firewall regulations and the router details can be exposed to the intruder [8].

2.5 Attacks on the Virtual Machines or the Hypervisor

By breaking into the lower layer hypervisor it is possible for an intruder to gain control of the virtual platform which is managed and controlled by the hypervisor. This means than there could be a security risk to the physical infrastructure as well as the hypervisor is connected to the physical infrastructure in order to be able to emulate the processes on the abstract platform [4].

2.6 Attacks form back Door Channels

These attacks make a Virtual machine a zombie tool and gain access to the resources of individual and the confidential information of corporations. As a result the financial losses can be heavy for the individuals and the corporations. This is done through a DDoS attack from the back channels where the access is gained by remote access tools [7].

3.0 RISKS TO THE HYPERVISOR

3.1 Man in the Middle Attack

This is the form of intrusion that could occur where the control of the hypervisor will be in the hands of another individual and thus the intruder will have full control of the entire platform [5].

3.2 Disruption of Service

In this form of attack the attempt is to infect a virtual machine and then direct the communication though the attackers machines whereby all packets go through the intruders machine and it can be changed or deleted by the intruder at will [3].

4.0 THE EXPERIMENT WITH LIVE MIGRATION

While perfdomring the lexpoeriemtn with live migration with the hypervisor some unnatural network behavior was observed. The hypervisor environment consisted of:

5-node Windows Server (2008) R2 SP1: HyperV- Failover Cluster that hosted 14 guests machines, the network configuration for each host each on separate subnets was 1 NIC for host management, 1 NIC for Cluster Shared Volume (network), 1 NIC for Cluster heartbeat,1 NIC for Live Migration (network),2 NICs for host iSCSI with Dell Equal Logic HIT Kit for MPIO,1 NIC for Hypervisor switch and2 NICs for iSCSI within Hypervisor guest machines.

The behavior pattern that emerged was not a stable pattern that has been observed 2 guest machines clustered using Microsoft Failover Clustering to provide HA file server and each guest resided on separate Hypervisor hosts.

When the process was near completion the guests in the process were live migrated and the process was completed 99% after which the status changed to ‘pending’ as it was nearing completion. The pending status remained for several seconds: (~ 4 to 5) before it changed back to “Online” and the process was able to reach completion.

During the process time, a continuous ping of the guest being migrated consistently dropped (3 pings) when the status was in “Pending” status.

When the System Event- log was reviewed on the host immediately after migration the following error surfaced twice out of the five times the experiment was carried out. The errors that surfaced are:

1. Event ID 7: errors from the iSCSIPrt source stated that the initiator was unable to send an iSCSI PDU. Error status was seen in the dump data.
2. Event ID 1135; errors from Failover - Clustering stated that the other cluster node (which was not live migrated) had been removed from the cluster. The event log on the non-migrated node reported that the migrated node had also been removed from the cluster. After (~ 30 to 50 seconds), the cluster reported that the migrated node as available again. Even though the cluster manager reported it as down, the RDP connectivity was kept live. When there is no gap that creates a security threat the a Live Migration does not show this pattern of behavior where the change of status from “Pending” to “Online” happens nearly instantly within 1 second and it only ever drops 1 ping. It is never more than 1 ping or less than 1 ping.

3. The problem may not specifically be tied to the clustered guests as the same Event ID 7: errors were seen on non-clustered standalone guests when the process of Live Migration had been completed. The cluster made the issue more noticeable.
4. The disabled TOE, RSS and all other monitoring tools reported on all HyperV hosts and guests, the following:
   netsh int tcp show global > c:\text.txt
   - Querying active state...
   - The TCP Global Parameters
   - ----------
   - Receive-Side Scaling State : disabled state
   - Chimney Offload State : disabled state
   - NetDMA State : enabled state
   - Direct Cache Access (DCA : disabled state
   - Receive Window Auto-Tuning Level : disabled state
   - Add-On Congestion Control Provider : (ctcp)
   - ECN Capability : disabled state
   - RFC (1323) Time-stamps: disabled
5. Similar disabled settings on each individual network adapter on all HyperV hosts and guests were seen.
6. The relevant hot-fixes for HyperV and Failover Clustering were applied and observed.
7. The network binding order was also verified
8. The verification of the network prioritization for the Hypervisor- Failover Cluster - guests using the proper network for the Live Migration was also verified.
9. The tested of disabling firewalls at the host and the guest levels was done.
10. This behavior pattern was not isolated when migrating to or from any of the Hypervisor host

It was the pending status that created the security gap in the hypervisor functions (~30 to 50 seconds) via the iSCSIprt errors. If this behavior pattern can be stabilized it will minimize the risk of security threats in the hypervisor [2].

5.0 CONCLUSION

The conclusion that can be drawn is that there is a risk to the perceived threat in the hypervisor but since it shows ‘pending’ during the completion process it is evident that the intrusion is taking place at that point of time which is why the process completion was delayed. In those few seconds that the system was intruded data could have been taken out while the status online would show ‘pending’ and the process would only be concluded after the system intrusion process would be over. There is only a single gateway to gain access to the hypervisor and the hypervisor memory which is an important and critical part of the hypervisor. The wishful target of intruders is to be able to take control of the hypervisor and eventually move it to an infected server from where all the data can be downloaded. No intruder has yet been able to penetrate the current security levels of the hypervisor but increasing the levels of security to create further preventive measure for the future is a practical stand point that needs to be taken. The other important aspect of the hypervisor is that it is critical to the process of virtualization and a new design architecture that can incorporate further security measures will increase the safety of the entire cloud computing

system and encourage more secure levels of communication with layered security processes in the hypervisor. At each level the risks will be mitigated even before it reaches the hypervisor creating multiple barriers to detect any type of intrusion that could affect the process of virtualization, the virtual machines operating systems and the live functions of the hypervisor. Preventing an intrusion through advance planning is a better option than to be dealing with an intrusion and trying to find a solution to resolve the issue.

REFERENCES

[1] G. Ackoff, B. Leslie, OKL4 Microvisor: Convergence Point of Micro Kernels & Hypervisors, University of New South Wales, 2010.

[2] I Blake, P. Gerard, The Information System as a Competitive Weapon. Communication of the ACM 27 (1984) 1193-1201.

[3] L. Barroso, U. Holzle, The Case of Energy Proportional Computing. Computer Journal 40 (2007) 33-37

[4] S. Chien, The Moderating Effect of Employee Computer Self Efficacy On The relationship between ERP Competence Constructs and ERP Effectiveness. Journal of Electronic Commerce Organization 7 (2009) 65-85.

[5] V. Grover, S. Jeong, A. Segars, Information Systems Effectiveness: The Constructs, Space and Patterns of Application, Information and Management Journal 31 (1996) 177-199.

[6] G. Heiser, B. Leslie, OKL4 Microvisors: Convergence Point of Micro Kernels & Hypervisors, University of New South Wales (2010).

[7] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, A Survey of Intrusion Detection, Techniques in Cloud, Center for Cyber Security Sciences, City University, London, 2014.

[8] J. Nikolai, Y. Wang, Hypervisor Based Cloud Intrusion Detection System, International Conference of Computing, Networking and Communications, (2014).

[9] M. Trend, Hypervisors Bring New Capabilities and New Risks, Simply Security, 2009.