Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 51-56, 2015

The Mitigation of Threats and Risks in the Process of Virtualization by Securing the Hypervisor Control Factor

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

[1]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.
[2]Department of Computer Sciences, University of Technology, Baghdad, Iraq.
[*,a]*alishawket1@gmail.com*, [b]*samad@utem.edu.my*

Abstract – *A study was undertaken in order to be able to understand the threats and the risks to the hypervisor's control of the virtual machines on the virtual platform. The study undertaken has clearly shown that even though a probability exists, the level of trust of clients and service providers helps to reduce the levels of risks and threats to the virtualized platform. A test bed was created and a network of (un) modified hosts were subjected to security disruptions and intrusions. The hypervisor has been used so that it can be observed and recreated. The test bed used the hypervisor as an instrument to gather the information. The information gathered across was an entire heterogeneous LAN that was generalized for the experiment. This helped in the observation process and control of the behavior of the virtual machines. The main security events were logged which was a new process that the hypervisor was enabled with for the experiment. It showed that the hypervisor can intercept a system call before it is allowed to enter.*

Keywords: threat and risk, virtual machine, service provider

1.0 INTRODUCTION

The hypervisor is the component that controls the virtualization process and the virtual machines though the functions of emulating the physical system on a virtual platform. The process of virtualization is the method by which the business processes are made more efficient and rapid decreasing the time taken. It also provides vast resources of information that are essential in today's global business environment. The hypervisor has the capability of connecting the virtual machines or the guest operating systems without changing the properties and the patterns of behavior of the entire process of virtualization. The hypervisor enables the integration of business processes and allow scalability in large proportions that are beneficial for the organizations that have migrated to the cloud system. Virtualization is the foundation of the cloud computing system, and this foundation has been made possible by the functions of the hypervisor. Many critics have tried to create a No-Hypervisor environment, but have been unable to do away with the functions of the hypervisor even if they have been able to do away with the component on an experimental basis. This shows that the hypervisor is a component which has a possibility of being intruded but the

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 51-56, 2015

probability is low and hence the risk is low. The experiment that had been undertaken is to show that the hypervisor as a singular unit can be modified by increasing the security control of the hypervisor in order to increase the security functions of the entire virtual platform. The experiment conducted showed the ability of the hypervisor to interrupt calls before entry into the gateway. The aim of the experiment was to show that modifications to the hypervisor are possible to increase the functionalities of the hypervisor to secure the entire cloud computing system [9].

2.0 BACKGROUND

The process of Virtualization provides a way technique for sharing resources in all the virtual machines simultaneously. This is done by hardware & software partitions, emulation, time sharing and scalability. The hypervisor interacts with the physical operating system and emulates the system providing the functions to several virtual machines at the same time securing each virtual machine from one another and their communication. What the virtual layer does is to provide the support for infrastructure to the abstract layer. The three types of virtualization that exists till today are para-virtualization, full virtualization and hardware based virtualization [2]. This has increased the hypervisor as a target for intruders to control in order to be able to infect an entire virtual platform and take control of all the virtual machines that a particular hypervisor is controlling. This is why the security control if increased in the hypervisor itself will not only secure all the virtual machines, isolate the virtual machine that has been infected, it will also be able to keep the physical system safe from breaches since the hypervisor has direct to the physical operating system in order to be able to provide the resources to the virtual machines and the operating systems of guest machines [1].

3.0 EXPERIMENT

The hardware that has been used for the experiment was able to run five physical machines. Each machine had 2 Dual Core Xeon -=Dempsey processors. The technology that was used was Intel – IVT x8 &6 for the virtualization and 8GB for the RAM. The entry and the exit of the Virtual Machines (VMs) was provided by IVT. These states were managed by disrupting the system with system calls and transitions. Instructions were trapped in a guest machine and relayed to the hypervisor. The access to I/O devices was managed as per the procedure that is listed below:

The virtualization software was the KVM (10, 11), this is a module that can be loaded: load for Linux versions 2.6.20 and later KVM was found to leverage IVT to put a hypervisor that had a lesser code base than the normal hypervisors e.g VMWare (15), Xen (2). KVM expanded the traditional two modes of a UNIX process – both the user and the system to 3. The inclusion was the owner of the guest- host process. This experimented was repeated thrice to ensure that the results that were recorded from observation of the experiment were reliable and could be used to confirm that the increase in the controls of the hypervisor allows an incremental level of security for the entire cloud computing system [5]. The VM emulated the hardware x86, it showed the possibility of being able to implement a virtual Ethernet which would reduce the current security risks that are being faced. This assisted in understand how the network based intrusion spreads throughout the entire network. The hardware that has been used for the experiment was able to run five physical machines. Each machine had 2 Dual Core Xeon -=Dempsey processors. The virtualization technology that

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 51-56, 2015

was used was Intel – IVT x8 &6 for the virtualization process and 8GB was used for the RAM. The entry and the exit of the Virtual Machines (VMs) was provided by the IVT. These states were managed by disrupting the system with system calls and transitions. Instructions were trapped in a guest machine and relayed to the hypervisor. The access to I/O devices was managed as per the procedure that is listed below.

- Virtual Machines that are Inactive
- The lack of awareness of virtual machines
- The sprawling of virtual machines
- The communication traffic in virtual machines
- The migration of system to the cloud computing system which is dependent upon virtualization for the immense scalability of the cloud system and the lightning speed of the cloud computing system.

The Non-I/O code was allowed to run, in guest mode, and system mode and was used solely for the purpose of transition between modes and to issue special instructions. Since Linux-KVM is capable of hosting any unmodified x86-based operating system the test bed supported all operating systems that were used for the experiment:

- Windows
- Linux
- NetBSD.

4.0 RESULTS

The experiment clearly showed that this was a situation where the hypervisor when it is disrupted or I/O instructions are changed does not recognize the messages. On the other hand it does have the capacity to intercept the messages, if the modification are made then it will be simple for the hypervisor to create blocks intermittently in different areas of the process path which will act like a filter or a sieve to ascertain that any undetected codes at one place does not go undetected in another area of the pathway.

$$\textit{Minimize} \quad \sum_{i\in N}\sum_{j\in F_i}(pb_{ij} - pi_{ij})\cdot\alpha_{ij} + pi_{ij}\cdot y_{ij}$$

$$\textit{Subject to} \quad \sum_{k\in M} d_k \cdot x_{ijk} \le cap_{ij}\cdot\alpha_{ij} \qquad \forall i\in N,\ \forall j\in F_i$$

$$\sum_{i\in N}\sum_{j\in F_i} x_{ijk} = 1 \qquad \forall k\in M$$

$$\sum_{j\in F_i} y_{ij} \le 1 \qquad \forall i\in N$$

$$\alpha_{ij} \le y_{ij} \qquad \forall i\in N,\ \forall j\in F_i$$

$$x_{ijk}\in\{0,1\},\ y_{ij}\in\{0,1\},\ \alpha_{ij}\in[0,1]$$

where,

N= the set of physical servers

Fi = to the frequency for each server i ∈ N.

M= the set of application that are run on the cluster.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 51-56, 2015

Capij= the maximum capacity of the server i which is running at the CPU Frequency = j ∈ Fi.
pbij and piij = busy/idle-active power cost

This is so that the server i can run at frequency j where αij = the utilization of server i at j frequency. For every application k ∈ M, dk to represents workload demand of the application.

'The decision variables = xijk is a binary variable that denotes whether server i uses frequency j to run application k =(xijk = 1), or not which is = (xijk = 0); yij is a binary variable that denotes whether server i is active at frequency j (yij = 1), or not (yij = 0).'

5.0 DISCUSSION

The risks and threats to the virtualization process was seen from situations such as VM Sprawl, the virtual machine communication traffic, and the migration process. It was also found that during the communication between virtual machines the interception was done though intrusion by entering the virtual machine operating system and capturing the communication either at the point of sending or at the point of opening by the receiver. The warning systems in and around the hypervisor create the detection system which closes the gateway before any calls can pass though the gateway. The hypervisor memory has a way of detection of all security risks and threats that has been written in the memory. Therefore reaching the memory of a hypervisor is a prime target for all penetrators and intruders which they are unable to penetrate till date showing that the probability is low [4]. Rewards have been announced that are large sums of money for anyone that can penetrate the hypervisor. The reason why the experiment was carried out is to increase the strength of the control powers in the hypervisor as a method of prevention in case of an eventuality. The immense scalability and the data locations being spread out over a wide geographical; region makes it difficult to pin point the penetrator and to take physical custody of the individual. However if the hypervisor is secured and the controls for a secure environment are increased in the hypervisor itself, it will be able to handle all security requirements without any complications or changes in the properties of the transaction, information and processes as is seen in the virtualization process [6].

6.0 RECOMMENDATIONS

The results and the possibilities of the hypervisor security being strengthened has been proved by the experiment that has been conducted. As a result, some of the ways to minimize the current security threats to the hypervisor which will automatically increase the strength of the security capabilities of the hypervisor are:

Operations on a Multi- Hypervisor Environment

This will permit the process of virtualization to be more transparent to all the hypervisors in the virtual platform. It will be able to track any malicious code in any one of the hypervisors in the multiple hypervisor platform and the detection will be immediate irrespective of the language that has been used by the intruder. This also creates the possibility of being able to shout down one hypervisor and move the operations to another hypervisor immediately without a break in the processes that could disrupt communications or business functions that are of critical nature.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 51-56, 2015

The scope of this environment is also extensive as that one hypervisor can be dedicated to one virtual machine only in a simpler form so that while the other virtual machines are running on a regular basis the hypervisor will have the capability to be able to channelize the communication relay of only one virtual machine through it closing all possible fronts of attach on the virtual machine or the small hypervisor in any form as for all practical purposes both the virtual machine and the single operation hypervisor will remain undetected to the cloud computing environment in general [7].

The Combination of Two Different Types of Architecture

A combination of architecture has also been seen to work effectively against all types of intrusion to the virtualized platform. This was tested by using two regular hypervisors and one smaller hypervisor with a smaller code base so that any hi -fi intrusion was not possible. The normal virtual processes were carried out on the regular hypervisor which handled five machines. The small code hypervisor connected to one of the virtual machines that was required for critical functions of business and communication. It was found that both the small code hypervisor and the virtual machine running on it went undetected and there were no disruptions possible despite making repeated attempts to disrupt the process. This was also due to the fact that the small code hypervisor did not understand the complexities of the malicious malware and was unable to entertain the request [8].

Securing the Hypervisor with Different Levels of Security

A further study into the possibilities of securing the hypervisor was undertaken and from this it was also found that different levels of security classifications could be incorporated into the hypervisor so that the security breaches were less likely to occur decreasing the probability percentage to almost 0. At the different levels of the pathway in all the virtualized processes the levels of security would be dependent upon the access level and the authorization levels written into the hypervisor which would be difficult to surpass once the hypervisor was operational. At each level the packets would get filtered so that the intrusions though the data stack would be minimized and virtually none -existent.

This would be very effective in a surrounding where the environment was a multi hypervisor environment as the processes of isolation will be very rapid and the speed of a communication was also seen to act as a deterrent for intrusions because the intrusion packets are normally designed to replace at the time of sending a communication or at the time of opening the communication. However the in process relays may be possible to insert a malicious malware but it is not possible to remove and change the existing the software of the system. Unless an intruder can make the changes it is not possible to infect any virtual machine or the hypervisor on the virtual platform to gain access and control of the platform of at least one machine.

Small Code Bases for the Hypervisor

If the hypervisor has a small code base it was found that the levels of security were increased making the hypervisor virtually impregnable and solid as a component. This small code base makes the hypervisor simpler and smaller and this supports the ability of the hypervisor to remain undetected in a hostile environment [10].

7.0 CONCLUSION

This provides the evidence and the ability that there is immense scope and possibilities for'*The Mitigation of Threats and Risks in the Process of Virtualization by Securing the HypervisorControl Factor.'* The main issue is to study the hypervisor possibilities in connection with the functions of the hypervisor before the possibilities is studied by focusing on the structure of the hypervisor. It is the functional aspects of the hypervisor that needs to be secured.

REFERENCES

[1] R. Adams, The Emergence of Cloud Storage and the Need For a New Digital Forensic Process Model, Working Paper, Murdoch University (2013).

[2] N. Alam, Surveys on Hypervisors, School of Informatics and Computing, IndianaUniversity, Thesis Final paper (2006) 2-6.

[3] N.G. Arya, G. Mukesh, S. Kumar, Hypervisor Security a Major Concern, International Journal of Information and Computer Technology 3 (2013) 533 – 538.

[4] B. Brener, Proof of Concepts Heighten Malware fears, (2006).

[5] D. DuChamp, S. Lee, G. Angeli, A Hypervisor Based Security Test Bed, Computer Science Department, Steven Institute of Technology (2014).

[6] V. Grover, R. Seung, H. Albert, Information Systems Effectiveness: The Constructs, Space and Patterns of Application, Information and Management Journal 31 (1996) 177-199.

[7] R. Hashizume, G. Daniel, M. Fernandez, B.E. Fernandez, An Analysis of Security Issues for Cloud Computing, Journal of Internet Services and Applications 54(1) (2013) 5.

[8] Hay, I.U. Salman, How to Tackle Security Vulnerabilities in Hyper Based Cloud Servers, Cloud Tweaks, (2013).

[9] A. Kumar, S. Siwani, Guest Operating System based Performance Comparison of VMware & Xen Hypervisor, International Journal of Science, Engineering & Technology 2(5) (2014) 286-297.

[10] N. MacDonald, Yes, Hypervisors Are Vulnerable, Article, Gartner, www.blogs.gartner-com, Gartner Research Center, (2011).