Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 684-688

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Secure Virtual Application in Virtual Environment

[1]Anand, R., [2]Nalini, L., [3]R. Sangeetha

[1]Assistant Professor, [3]CSE, Saveetha School of Engineering, Saveetha University Chennai, India.
[2]Professor (CSE), CSE, Arulmigu Meenakshi Amman College of Engineering, Kancheepuram Chennai. Tamil Nadu, India.

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Virtualization, Virtual application, Security

ABSTRACT

The aim of the study is security in the virtual environment is the foremost concerns where it can be categorized by three means, namely hypervisor based security, virtual machine based security and application based security. The analysis of application based security is scrutinized in this paper. In different virtual environments of application access and application hosting there prevails the complexity. Hence virtual security and virtual privacy practice are adopted in order to overcome the complexity issues in virtual environment. The mathematical model for security concerns of virtual application in virtual environment is implemented and proved. Application virtualization technology does not alter the applications in any way; rather it just delivers the applications in a virtual environment. Hence the flaws in the applications get delivered as well. This vulnerability and security issue of virtual application in the virtual environment is examined.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Anand, R., Nalini, L., R. Sangeetha., Secure Virtual Application in Virtual Environment. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 684-688, 2015*

INTRODUCTION

The physical security systems are designed neither to protect the new components of the virtual system developed nor the virtualization architecture (Anand 2012 *et al*). Despite the virtual systems, the physical systems depend on the traditional security networks, which defend the systems. Network inspection plays a major role in the secure physical systems. Whereas, for the security of virtualization systems, the network inspection does not matter much.

Virtualizing the system gets to many significant changes to security. Some of them are a strong virtual network build, which secures the system; the hypervisor system, which acts a threat surface to the systems; a powerful virtual administrator for the system to split up the roles for each function of the system(Anand 2012 *et al*).

The basic goal of this virtualization system is to bring about a positive approach to the impact of security over systems. Virtualization improves the security factor by making the systems more difficult to access by the third person environment (Anand 2012 *et al*). It helps the system recover from complications in security system, the unwanted exposal of information to the unauthorized people. It also helps in managing the physical counterparts of the virtual and physical systems, hence, involves in overcoming the challenges in the security of the systems.

Virtual machines are rapidly replacing the physical machines to emulate hardware environments that share hardware resources. Virtual machine provides better security than physical machines by providing an additional layer of isolating hardware. But virtual environment has security issues where the user of single virtual machine in virtual environment with N number of virtual machines, can monitor or access other virtual machine(Barrere *et al*).

When a guest is loaded into a virtual machine (VM), the hardware that gets detected is the simulated hardware via the hypervisor, not the actual hardware itself. The hypervisor is the component which is responsible for emulating specific hardware configurations to guest operating systems (.Chen, Zhen *et al*). It is capable of creating multiple simulated environments, or multiple VMs, which permits us to run multiple operating systems that may have slightly different hardware requirements. The guest OS is abstracted from the true hardware, adding a component of versatility (Hsin-Yi Tsai *et al*).

The virtualization techniques thereby has security issues like definitional issues concerning what compromises a virtual environment and, thus, the threats posed to that environment; the management of applications and operating systems

Corresponding Author: Anand, R., Assistant Professor, Saveetha School of Engineering, Saveetha University Chennai, India.
E-mail: nowhereanand@yahoo.com

within virtual machines (VMs); and the use of a virtual administrative network to manage virtual hosts(Jingzheng Wu *et al*). The ultimate goal is for virtualization administrators to secure the entire virtual environment, not just a hypervisor or management appliance in isolation (Kun Huang *et al*).

The hypervisor is a program, running on the host, so if it is compromised, all VMs it controls and the host itself are accessible to the attacker. The hypervisor converts instructions for the guest OS into instructions for the host OS. If there is any issue with guest OS, it may also lead to a problem with hypervisor.

Attacks are one of the major concerns in a virtual environment they can occur in three layers (1) Network (2) Transport (3) Application

Network/Transport layer attacks or Transport layer attacks are launched using TCP, UDP, ICMP packets (Papagianni *et al*).

The attacks are of the following categories,

- Flooding attacks
- Echo based attacks
- Protocol based flooding attacks
- Broadcast based attacks

In this paper, we focus on application level attacks and how they can be prevented in a secure manner.

Application Level Attacks:

In virtual environment, attacks mainly occur in the application layer. This type of attacks are HTTP Protocol based attacks, which may have certain attacks like Session based attacks, Request based attacks, Multiple HTTP method based attacks, Faulty application and Slow-request response attack.

In the virtual environment, all the applications are installed in the virtual server. Every client can send request to the virtual server and can access the application using HTTP Session. Every application can comprise streaming from server to the client. When multiple user wants to access the same application.

In virtual environment multiple application are present in which multiple users can access the same application. Since multiple users are accessing the same application, this environment is vulnerable to session flooding attacks which may also get affected and attacked by HTTP request &response. In this type, session connection request rates from the attackers are more than the legitimate users. Because of this, the server resources get exhausted and this leads to DDO's flooding attack. Attackers generally use botnets for these type of attacks. Since each bot can generate a large number of valid requests (more than 10req/sec), there is no need for employing large number of bots for making the attack successful. HTTP request/response attacks are non-spoofed attacks(SoaresBoaventura *et al*) . Many attacks occur as day to day activities in the internet, of which 2 attacks have mainly increased as follows :(1) DDOS attack (2) SQL injection. This attack mainly focuses on 3 areas (1) Public sectors (2) Industries (3) Organization. China maintains its position on the main source DDOS attacks.

In previous years, the attacks on governmental targets had an increase of nearly 30%, foe industries 18.8% and foe organization 12.5% when compared to 2012 in which it clearly notifies the DDOS attacks has been increased in the year 2013.

Network and transport layer based are infrastructure based attacks which has increased 17% when compared to the year 2012.

Application based an attack that is layer 7 had an increase of 28% in the previous year.

A DDOS occurs when many computers attempt to access the same service simultaneously overwhelming the capacity of the server to respond.

This paper mainly focus on three area's

- Secure virtual environment
- Vulnerability Assessment
- Attack Detection

Security mechanisms should prevent threats in addition to stopping threats. This plays a vital role in multitenant virtual and cloud environments. Servers are the most obvious shared resource within virtual and cloud environments However, network and storage devices also utilize a variety of virtualization techniques to enable physical resource sharing. Storage area networks are common elements within cloud computing environments. They are all intended to provide secure resource sharing; they must still be tested to ensure inter-tenant security. Hypervisors also have internal virtual switches for sending traffic between VMs on the same host. This reduces traffic on network interface cards NIC but also adds some complexities and additional security risks. Network engineers must ensure that traffic destined for one VM cannot be leaked to other VMs.

Fig1,Applications from cloud server before deployed to the clients should be processed in order to provide security. The fig shows the model of deploying the applications to the client in a secured manner. Vulnerable applications are easily prone to threats. Hence analysis of vulnerability of an application is vital. Once after the vulnerability of the application is analyzed, the application is virtualized for the audit manager to provide security. Security policies are implemented for an application that is provided as a service. Important process in providing security to the application is that, it is virtualized before proving as a service.

Secure Communication Model in Virtual Environment:

In a virtual environment, all the systems applications are isolated. They communicate in a secure manner,

In fig2,

Vm_n ->Virtual machine monitor.

$Vm_1, Vm_2, Vm_3 - >$Virtual machines or Guest OS

$A_1, A_2, A_3 - >$Applications

$A_{11}, A_{12}, A_{13}, A_{21}, A_{22}, A_{23}, A_{31}, A_{32}, A_{33} - >$Virtual Applications or Instance of applications

Overall Secure Communication model in virtual environment is given by,

$$Vm_m = \sum_{i=1}^{x} Vm_i$$

$$= \sum_{j=1}^{x} [A_i - \sum_{j=1}^{x} A_{ij}]$$

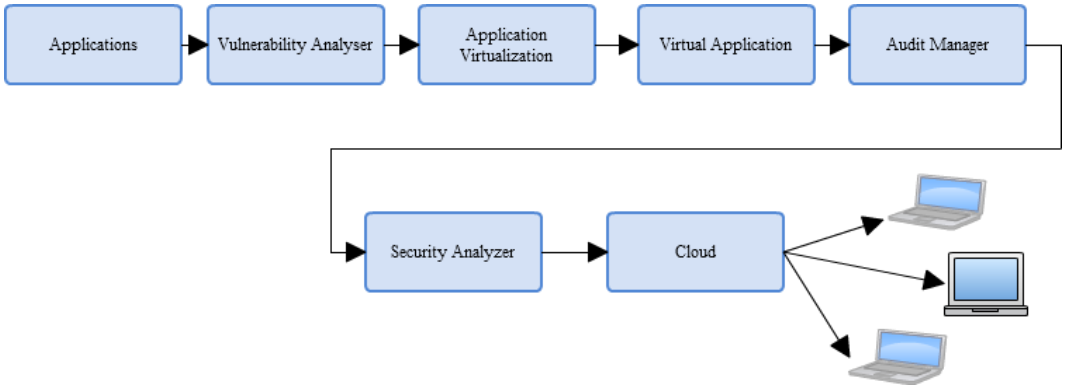

Fig. 1: Vulnerability Assessment of Virtual Application.

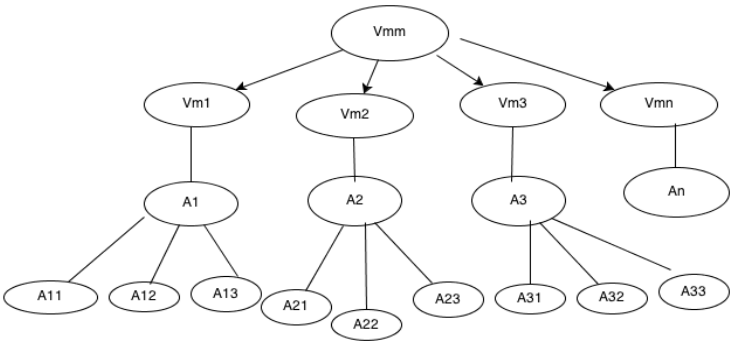

Fig. 2: Tree Structure of Virtual Environment.

Detailed Model:

In this model we can take 3 Vm's, 3 Applications and virtual applications,

$$Vm_m = Vm_1 + Vm_2 + Vm_3$$

Virtual machine monitor contains Vm_1, Vm_2, Vm_3.

In

$$\sum_{i=1}^{3} Vm_i = [A_1 - (A_{11} \vee A_{12} \vee A_{13})] + [A_2 - (A_{21} \vee A_{22} \vee A_{23})] + [A_3 - (A_{31} \vee A_{32} \vee A_{33})]$$

We assume that,

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Here,

$A_{12}, A_{22}, A_{31}, A_{32}, A_{33}$are marked as zero because service is not available.

In Application $[A_{12}, A_{22}, A_{31}] = [1, 0, 1]$

$$\sum_{i=1}^{3} Vm_3 = [1 - (1 \vee 0 \vee 1)] + [0 - (1 \vee 0 \vee 1)] + [1 - (0 \vee 0 \vee 0)]$$

$$= [(1 - (1)) + (0 - (1)) + (1 - (0))]$$

Apply to $A - B = A \cap B^c$

$$= (1 \cap 0) + (0 \cap 0) + (1 \cap 1)$$

$$= 0 + 0 + 1 = 1.$$

If any one of the application fails, it does not collapse the overall system. Hence the system is said to be more robust.

Vulnerability Assessment model:

In a paper Martin Barrere *et al*, has used the 'flattern method' to identify the set of vulnerabilities by using the formula

$$vflattern(PM) = (\sum_{i=1}^{m} a_{i1}, \sum_{i=1}^{m} a_{i2}, ..., \sum_{i=1}^{m} a_{in})$$

The vflattern operation aggregates the number of times that each property occurs within the whole set of known vulnerabilities. The resulting vector provides an indicator that helps to identify most common properties involved in vulnerabilities.

$$hflattern(PM) = (\sum_{j=1}^{n} a_{1j}, \sum_{j=1}^{n} a_{2j}, ..., \sum_{j=1}^{n} a_{mj})^T$$

Other useful metric can be extracted from the pattern matrix when the aggregation operation is performed horizontally, as indicated by hflattern.

Vulnerability assessment process over a given system is defined by the following equation:

$$w = hflattern(PM) - [PM * s^T]$$

$$w = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} \\ \sum_{j=1}^{n} a_{2j} \\ . \\ . \\ . \\ \sum_{j=1}^{n} a_{mj} \end{pmatrix} - \left[\begin{pmatrix} a_{1,1} & a_{1,2} & ..... & a_{1,n} \\ a_{2,1} & a_{2,2} & ..... & a_{2,n} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ a_{m,1} & a_{m,2} & ..... & a_{m,n} \end{pmatrix} * \begin{pmatrix} s_1 \\ s_2 \\ . \\ . \\ . \\ s_n \end{pmatrix} \right]$$

$$w = \{w_1, \quad w_2, \quad .... \quad w_m\}$$

The resulting assessment vector de-notes the status of each vulnerability v_i in the target system

$$w = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}_{\rightarrow}$$

But in this paper, we have developed a method which can detect and also recover vulnerability. The mathematical model is given by

$$PM = \begin{matrix} v_1 \\ v_2 \\ . \\ . \\ . \\ v_m \end{matrix} \begin{pmatrix} p_1 & p_2 & ..... & p_n \\ a_{1,1} & a_{1,2} & ..... & a_{1,n} \\ a_{2,1} & a_{2,2} & ..... & a_{2,n} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ a_{m,1} & a_{m,2} & ..... & a_{m,n} \end{pmatrix}_{a_{i,j} \epsilon \{0,1\}}$$

Each matrix row encodes the properties of observed vulnerability $V_k$to be present. Consider the scenario having instance with three vulnerabilities V_1, V_2 and V_3. A pattern matrix can be built follows,

$$v1 = \{p1, \quad p2, \quad p4\}$$
$$v2 = \{p3\}$$
$$v3 = \{p1, \quad p2, \quad p4\}$$

$$PM_{3*4} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

The vulnerability recovery model (VRM) is given by,

$$C_i - M_{i,j} * D_i = (j-3) * S$$
$$C_i = \begin{cases} No & of & terms \\ if & D_i = (D_i)^T \end{cases}$$

$$D_i = D_i^T, D_i \leftarrow M_i$$

$$\begin{pmatrix} 4 \\ 1 \\ 4 \end{pmatrix} - \left[\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right] = (4-3) * S$$

$$\begin{pmatrix} 4 \\ 1 \\ 4 \end{pmatrix} - \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix} = S$$

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}_{\rightarrow} = S$$

Hence by applying the VRM methodology, any number of vulnerabilities can be detected and recovered.

This mathematical virtualization model is that, it can be useful for checking the vulnerability of the applications is streaming across the cloud. The exposure of the virtual application can be automatically recovered. This way, the vulnerability is checked over and is recovered back, without the data being viewed by the unauthorized people. The mathematical model finds the formulae for the recovery of vulnerability of the application and hence the application data can stream fromacross the virtual environment. Which follows the mathematical modeling process, there is a '0' to indicate the systems which are out of use and cannot be connected virtually because of security reasons. There is a '1' to indicate that the systems can stream application within each other securely using the virtualization technique.

Conclusion:

The result of this mathematical virtualization model is that, it can be useful for checking the vulnerability of the virtual application. The exposure of the vulnerable virtual application is automatically recovered using this mathematical model. This vulnerability application reduce the vulnerability improve the security in the virtual environment. There is a '0' to indicate the systems which are out of use and cannot be connected virtually because of security reasons. There is a '1' to indicate that the systems can transfer data within each other securely using the virtualization, and the fact that they are made secure using the mathematical modeling.

REFERENCES

Anand, R., G.A. Kumar, S. Murthy, 2012. "Mitter-Bitter monitoring system using Android smartphone's," *Computing, Communication and*

Applications (ICCCA), 2012 International Conference on , pp: 1-4.

Anand, R., S. Sarswathi, R. Regan, 2012. "Security issues in virtualization environment," *Radar, Communication and Computing (ICRCC), 2012 International Conference on*, pp: 254-256.

Anand, R., S. Saraswathi, V.R. Sindu, B. Sandhya, 2012. "Design of Secure Communication Model for Virtual Environment"Communications in Computer and Information Science, 269: 277-283.

Barrere, M., G. Hurel, R. Badonnel, O. Festor, 2013. "Ovaldroid: An OVAL-based vulnerability assessment framework for Android," *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, pp: 1074-1075.

Chen, Zhen, Han, Fuye, Cao, Junwei, Jiang, Xin, Chen, Shuo, 2013. "Cloud computing-based forensic analysis for collaborative network security management system," *Tsinghua Science and Technology*, 18(1): 40-50

Hsin-Yi Tsai, M. Siebenhaar, A. Miede, Yu-Lun Huang, R. Steinmetz, 2012. "Threat as a Service?: Virtualization's Impact on Cloud Security," *IT Professional*, 14(1): 32-37 doi: 10.1109/MITP.2011.117.

Jingzheng Wu, Yanjun Wu, Mutian Yang, Zhifei Wu, Yongji Wang, 2013. "Vulnerability Detection of Android System in Fuzzing Cloud," *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*, pp: 954-955.

Kun Huang, Ming Xian, Shaojing Fu, Jian Liu, 2014. "Securing the cloud storage audit service: defending against frame and collude attacks of third party auditor," *Communications, IET*, 8(12): 2106-2113.

Papagianni, C., A. Leivadeas, S. Papavassiliou, V. Maglaris, C. Cervello-Pastor, A. Monje, 2013. "On the optimal allocation of virtual resources in cloud computing networks," *Computers, IEEE Transactions on*, 62(6): 1060-1071.

Soares Boaventura, R., K. Yamanaka, G. Prado Oliveira, 2014. "Performance Analysis of Algorithms for Virtualized Environments on Cloud Computing," *Latin America Transactions, IEEE (Revista IEEE America Latina)*, 12(4): 792-797.