Risk Analysis for Asset in Para-virtualized environment with relation to Probability of Threats and Attacks

[1]Ketan Parmar, [2]Ms. Aspriha Das
[1]IT System & Network Security
[1]Gujarat Technological University, Ahmedabad, India

***Abstract* - Virtualization has become the new buzz in any industry, especially with the increased acceptance of storage networks. Virtualization has the main advantages such as secure logging and terra architecture which enhances overall performance of the server and effectively reduces the cost. Although virtualization is not a new paradigm, the way in which it is used in modern system architectures provides a powerful platform for system building. Para-Virtualized system is a category under the virtualization which modifies the guest operating system to execute operations directly on the hypervisor so that no performance loss is observed during the emulation of the complete hardware. Since the Para-Virtualization is a technology that was initiated by an open-source community, security concerns with this technology are of prime concern. Therefore, understanding the threats faced by this technology and providing adequate mitigations against these threats is essential. This paper addresses the growing security concerns associated in a Para-virtualized environment. Some of the most common threats are Denial of Resource Attack, Sniffing Attack, and Authentication and Authorization issues. This paper provides the readers an insight to modeling threats, analyzing threat parameters, deriving risk equations, and validating the results in Para-virtualized environment.**

***Index Terms* - Para-Virtualization, Risk assessment, VM, Threat**

I. INTRODUCTION

In today's s environment of IT organizations, threats and worms against data and infrastructure continuously evolving. This paper represents an insight to modeling threats and analysing threat parameters for securing data in para virtual environment. With the current trend of outsourcing data, cloud computing, and distributed interconnected networks, which results in increases exposure of organization and its computation system at risk. One solution cannot alone provide all the security to data. Moreover threats are being advanced and sophisticated in nature. It is very difficult to predict the nature of future threats and make a relation with risk parameters. So it is required to understand different aspects of threats as soon as possible before they harm enterprise or individual beyond repair.

II. VIRTUALIZATION

Virtualization broadly describes the separation of a resource or request for a service from the underlying physical delivery of that service.

A key benefit of virtualization is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources known as partitioning. This software-based partitioning approach is implemented through hypervisor architectures. which is describe in figure 1. A hypervisor architecture is the first layer of software installed on a clean x86-based system also referred to as a bare metal approach [1]. Since it has direct access to the hardware resources, a hypervisor is more efficient than hosted architectures, enabling greater scalability, robustness and performance.

II.I HYPERVISOR

The hypervisor is a piece of software written to separate and make the resources of the physical machine available to the logical machine. Traditionally, hypervisors were referred to as "Virtual Machine Monitors" or VMM (Cleeff, Pieters & Wieringa, 2009). Typically, there are two types of hypervisors (Figure1): baremetal hypervisors and hosted ones [4].Virtualization can be broadly classified into 2 types: Full Virtualization and Para-Virtualization.

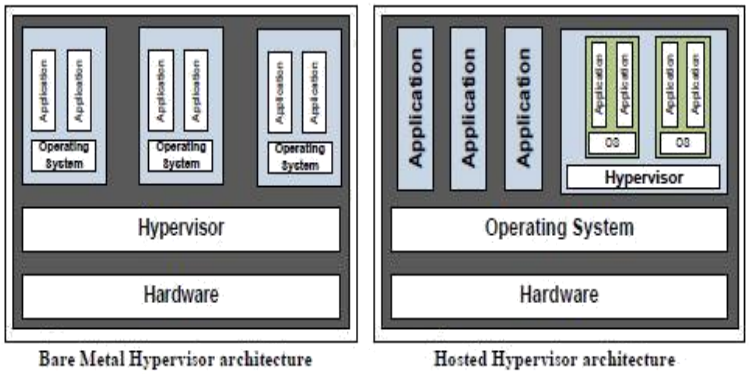

Figure 1: Logical architecture of bare-metal and hosted hypervisor [1]

II.I.1 FULL VIRTUALIZATION

The hypervisor provides a full simulation of the underlying hardware. Therefore, the guest operating system is unaware of the virtual environment around it. All applications that are compatible with the operating system would run as though they are the raw hardware of the physical machine[14]. The major advantage of this type of virtualization is that it provides complete isolation between the hypervisor and the guest Virtual Machine.

II.I.2 PARA VIRTUALIZATION

A virtual machine created with a para-virtualized hypervisor uses the techniques of resource sharing, where the kernel is modified to represent the required device of the physical machine to the VM [4]. The hypervisor in para-virtualization operates within the operating system that is modified to work in a virtual machine. The device drivers in para-virtualization are installed parallel to the hypervisor, so the virtual machine can directly talk to the physical resources, implementing resource sharing (VMware, 2007).

III. PROTECTION RINGS

Protection rings architecture is a formal mechanism to segregate the trusted operating system from the untrusted user programs [3]. These rings allow various levels of isolation and abstraction of privilege within the architecture of a computer system. Ring-0 is the most privileged ring that interacts directly with the physical hardware resources [14]. These restrictions are set on the outer rings to protect data and functionality from faults, misuse of resource, and malicious behavior.

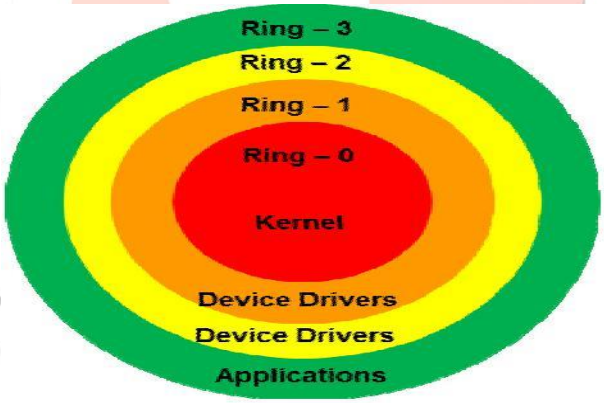

Figure 2: Protection rings in x86 CPU architecture[4]

Ring-0 is the kernel mode and Ring-3 is the user mode. The kernel mode is where the code is executed without any restriction access to the underlying hardware resources. Any CPU instruction can be executed and any memory address can be referenced in this mode.In the user mode, the code is executed with no ability to directly access the underlying hardware resources or reference any memory address.

In a virtualized environment the hypervisor is said to run in the kernel mode, because, it is the responsibility of the hypervisor to assign the hardware resources and allocate memory address to the guest VMs. Henceforth, the kernel of the guest VMs runs in a less privileged ring than Ring-0. Therefore, the kernel of the guest VMs has less privilege to access resources or reference memory address without the consent of the hypervisor [2].

IV. RISK EQUATIONS

To mitigate any possible attacks, it is important to understand the risks involved while implementing a new technology so that adequate security measures can be taken effectively. Hence, it is also necessary to formulate these risks, to properly plan out the security implementations on the network. Mathematically risk equation can be written as [5][10].

Risk = Threat * Vulnerability * Impact

Threats for Para-Virtualized Environments can be classified into three main categories:

1. Authentication Level Attack
2. Hypervisor Level Attack
3. Kernel and Disk level Attack

IV.I Authentication Level Attack

This is the most basic form of attack. This attack is carried out in order to gain control of the Virtual Machine [13]. The attacker tries to break into the VM by compromising the security features incorporated in VM. The different authentication methods are:

1. Encrypted Password
2. Active Directory
3. Secure Login

Thus the risk equation for an authentication can be written as:

$$P(AU) = \sum_{x=0}^{n} x\,[P(F) * [P(i) + P(e)]]$$

Where, P(AU)=Probability of authentication level attack, P(F)=Probability of attack due to failure in authentication, P(i)=Probability of attack due to internal user, P(e)=Probability of attack due to external user, x=Number of users trying to attack the network.Total risk equation of an authentication level attack can be expressed as,

$$Risk = \sum_{x=0}^{n} x\,[P(F) * [P(i) + P(e)]] * \left|\sum_{i=0}^{n} E_i * \sum_{j=0}^{n} R_j\right| * \left|\sum_{i=0}^{n} D_i * \sum_{j=0}^{n} U_j\right|$$

Where, Di = Estimated value of damage on impact, Uj = Estimated value of users affected by attack and Ei = Estimated Exploitability value, Rj = Estimated Reproducibility value.

The impact for such an attack is low since the number of users affected is few in number. The damage caused by a simple attack is restricted to that particular VM and hence the impact is very low as compared to higher level of attacks. These levels of attacks become effective when it is combined with a higher level of attack. The risk equation for this attack can be derived as the product of probability of an authentication level attack, vulnerability caused due to the threat, and the impact of the attack

IV.II Hypervisor Level Attack

The hypervisor is merely an operating system designed with the purpose of abstracting hardware from one or more Virtual Machines running above it. The hypervisors use hypercalls to communicate between VMs and the host OS. Under hypervisor level attacks, the attacker can either be a malicious user on the guest Virtual Machine (VM) or a malicious user who has gained access to the host VM through a sniffing attack or man-in-the-middle attack [6].

These hypercalls can be modified on either end of the VM to initiate and terminate connections. Unlike an authentication level attack, hypervisor level attacks cause a much more severe impact on the network.

In case of hypervisor level attacks, the attacker tries to modify the existing code or exploit the defects in the existing code used to communicate between VMs and gain control over the communication. Therefore, the attacker can get more resources from the host VM than the allocated amount of resources. Thus the vulnerability to such an attack is lesser than that of the authentication level attacks since the attacker first has to gain control over the VM to perform any modifications. This type arises a potential threat for the virtualized environment. Thus hypervisor level attack can be represented as,

$$P(HU) = \sum_{x=0}^{n} x\,[P(C) * (P(H,G))]$$

Where, P(HU) = Probability of successful hypervisor level attack, P(C) = Probability of successful attack on the communication channel of the hypervisor, P(H,G)=Probability of attack being carried out on either host VM or guest VM or both, x= Number of users successful in trying to attack the communication channel of the hypervisor.

Risk equation for a hypervisor level attack can be derived

Risk=(P(H)*V(H)*I(H))

Which can be expressed as:

$$Risk = \sum_{x=0}^{n} x\,[P(C) * (P(H,G))] * \left|\sum_{i=0}^{n} E_i * \sum_{j=0}^{n} R_j\right| * \left|\sum_{i=0}^{n} D_i * \sum_{j=0}^{n} U_j\right|$$

This type of attack has a higher impact since the number of users affected will be higher. When there is a modification of source

code involved, then the damage to the asset increases. This is because, it requires more time to identify the fault and debug the fault to eliminate the threat.

IV.III kernel level attacks

By compromising the security of the entire network the attacker gains access to the host VM, through which kernel level attack can be carried. Severity of kernel level attack is much higher and thus proper measures have to be taken to mitigate such attacks. In this level of attack, attacker gains control of the host VM by either performing an authentication level attack or a combination of authentication level attack and a hypervisor level attack on the host VM [14].

Once the attacker gains access to the host VM, rootkits are installed on the kernel of the host VM. The rootkits record values of all the data, such as data communication parameters, of VM's, buffer levels, registry values, and relay the data acquired to the attacker. The rootkits are similar to worms or viruses which are short programs that work in the background away from the administrator's domain.

The attacker, with this knowledge, can launch an attack from the remote machine and thus affect the entire communication channel of the environment. These attacks are much harder to identify since the rootkits act at the root-level or kernel level.

In the driver level of the attack, the attacker uses the information obtained by the help of rootkits to identify the location of arrays. During the data transfer between the VM's and the driver, the attacker can intercept and modify the existing data. However, the vulnerability of such an attack is much less in value since this attack can be carried only from the host operating system environment. Thus, the probability of a kernel and disk level attack can be written as,

$$P(KU) = \sum_{x=1}^{n} x\,[P(R) + P(D)]$$

Where, P(KU) = Probability of attack on the host VM kernel and disk array attached to machine, P(R)=Probability of successful installation of rootkits on the host VM kernel, P(D)=Probability of attack on the disk array during data transference and data storage.

Risk equation for a Kernel level attack can be derived as,

Risk = [P(KU) * V(KU) * I(KU)]

$$Risk = \sum_{x=1}^{n} x\,[[[P(A)||P(A)\&\&P(C)] + P(D_h) + \sum_{i=1}^{n}[P(f_i) + P(r_i)]]] * \left|\sum_{i=0}^{n} E_i * \sum_{j=0}^{n} R_j\right| * \left|\sum_{i=0}^{n} D_i * \sum_{j=0}^{n} U_j\right|$$

These types of attacks are very slow in nature and thus require a lot of time to detect. This type of attack has a higher impact since the number of users getting affected will most times be 100%. Such type of attacks cannot be eliminated completely, however, only measures can be taken to reduce the probability of such attacks occurring.

V. SIMULATION RESULTS

The risk equations can be validated theoretically using a simulation tool such as MATLAB. The MATLAB code was written to understand the behaviour of the attack by considering a normally distributed random value set. These random values can be seeded as per the user and network requirements with an upper limit and a lower limit thus providing a complete range of all possible values.

V.I Analysis of Authentication Level Attack

The authentication level attack mainly considers the type of attack and point of attack. As mentioned earlier the risk equation considers the probability of the attack, vulnerability to the threat, and the impact of such an attack on the physical machine. The total risk equation for the authentication level attack is expressed earlier in equation 2.

The simulation for this type of attack is considered by assigning a random variable list for all the three types of probabilities. The probability of an authentication level attack involves the parameters of failure of authentication method, probability of attack due to an internal user and probability of attack due to an external user.

V.I.1 Risk of an Authentication Level Attack

The risk is generally calculated as the product of threat, vulnerability and impact of an attack. All the three components are measured individually by considering the parameters that affect them and the corresponding values of these parameters are substituted in the equation to obtain the total risk value. Figure 3 shows the risk equation due to authentication level attack. The probability of risk is considered by increasing the value of number of users linearly. The risk of an authentication level attack being carried out is comparatively on the higher side due to the fact that the machine has a vulnerability value for these forms of attack. Although they are more prone to these forms of attacks, the impact of this attack would be much less and thus would not be a major factor during the risk assessment process. However, it is necessary to assess the risk of such attacks because of the fact that these forms of attack can be used to launch more impactful attacks, such as the hypervisor level attack.

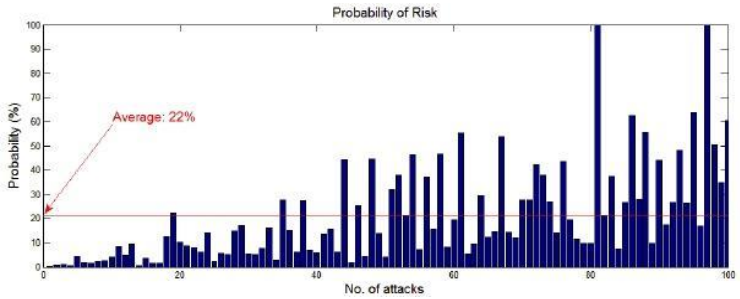

Figure 3: Risk due to an Authentication Level Attack

V.II Analysis of Hypervisor Level Attack

The hypervisor level attack can be defined as an attack made to gain control over the hypervisor in a virtual environment. Once, the attacker gains control, attacks such as spoofing and denial of resources can be carried out and degrade the performance of the Virtual Machine. Therefore, it is necessary to understand and assess the risk involved in such attacks. Results has been taken by considering the number of attack attempts made on the x-axis to its corresponding value on the y-axis.

V.II.1 Risk of a Hypervisor Level Attack

The Figure 4 depicts the average risk assessed for a hypervisor level attack. The average risk level of a hypervisor level attack is around 25%. The impact of such an attack is much higher and thus could lead to a major security flaw if overlooked.

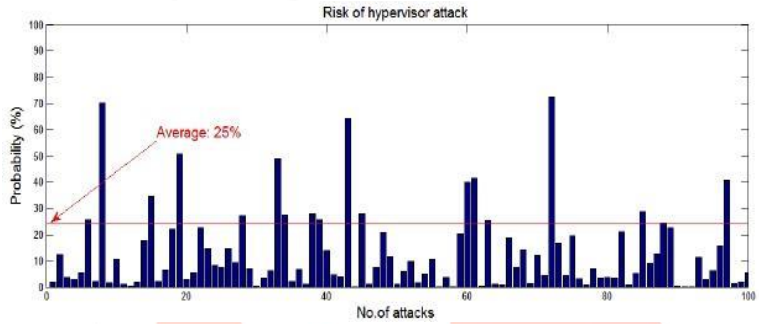

Figure 4: Risk due to a Hypervisor Level Attack

V.III Analysis of Kernel and Disk Level Attack

The kernel level attacks are carried out basically on the kernel of the host operating systems from the host Virtual Machine. The attacker gains control of the host Virtual Machine and installs a small program which gains information from the host machine kernel and relays that information to the remote attacker. The users on the host machine are unaware of this program that runs on the kernel, and with this information that is relayed, the attacker launches the attacks from the outside along with that, the attacker will also be able to identify the locations of the disks on the network and would be able to access them, thereby enabling the attacker to modify or destroy data.

V.III.1 Risk due to Kernel and Disk Level Attack

The probability of risk is relatively less as compared to other forms due to the fact that this attack is not very simple to carry out. The success rate of carrying out such an attack is much less and requires a very long time to carry out such an attack. However, once an attack is successful it is very hard to find out the source of the attack and it has a very great impact on the virtual environment. Figure 5 shows the graph for the probability of risk due to a kernel and disk level attack.

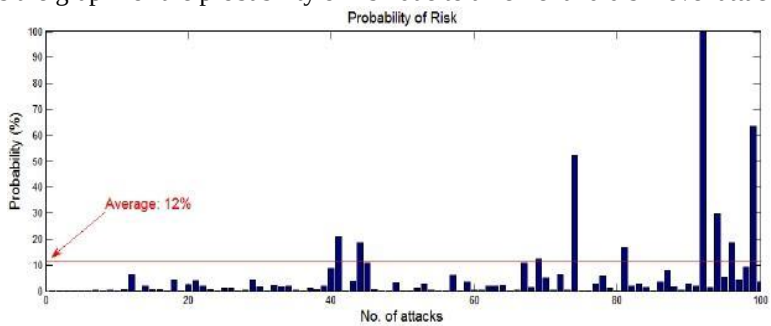

Figure 5: Risk due to a Kernel and Disk Level Attack

VI. CONCLUSION AND FUTURE WORK

This paper provides a basic structure of risk assessment of assets in a para virtualized environment. The risk assessment methodology has been studied for analysing and to developed risk equation in each level. The basic threats in this level has been studied to analyze the performance aspects such as vulnerability and impact. The results obtained clearly show that, the impact of a kernel and disk level attack is relatively higher than any forms of attack in a Virtual Machine. Thus, based on this inference the security aspects can be planned to avoid any possible threat to a para virtual environment.

This work can be extended to other form of virtualization in future. Before implementing a security feature within a network, most important aspect is to understand the risk associated with any form of threat. This paper is intended as an introduction to the security concerns, considerations, and implications arising from use of virtualized systems.

VII. REFERENCES

[1] ”Virtualization Overview” VMWare White Paper,Inc.3145 Porter Drive Palo Alto CA 94304 USA @2006.

[2] EverthingVM.com, ”History of Virtualization” http://www.everythingvm.com/content/history-virtualization.

[3] J. Hoopes, ”Virtualization for Security”, Syngress - Elsevier Inc., 2009.

[4] Fatma Bazargan, Chan Yeob Yeun, Mohamed Jamal Zemerly,”State-of-the-Art of Virtualization, its Security Threats and Deployment Models” International Journal for Information Security Research (IJISR), Volume 2, Issues 3/4, Septem-ber/December 2012 Copyright 2012, Infonomics Society International Journal for Information Security Research (IJISR), Volume 2, Issues 3/4, September

[5] Dr G. Kbar, ”Security Risk Analysis for Asset in relation to Vulnerability, Probability of Threats and Attacks”, Proc. Innova-tions in Information Technology, 2008. IIT 2008. International Conference, Dec.2008, pp 668-672, doi: 10.1109/INNOVA-TIONS.2008.4781631.

[6] Z.Wang, X.Jiang, ’HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity,’ Security and Privacy (SP), 2010 IEEE Symposium, July 2010, pg 380-395, DOI: 10.1109/SP.2010.30

[7] Michale Pearce, ”Virtualization: Issues, Security Threats, and Solutions”, ACM Computing Surveys, Vol. 45, No. 2, Article 17, Publication date: February 2013.

[8] A. Asosheh, B. Dehmoubed, A.Khani, ”A new quantitative approach for information Security risk assessment”, Computer Sci-ence and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, pg 222-227, DOI: 10.1109/ICC-SIT.2009.5234391.

[9] C. P. Sapuntzakis, R. Chandra, B. Pfaff, J. Chow, M. S. Lam, and Rosenblum, ”Optimizing the Migration of Virtual Computers. In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI 2002)”, ACM Operating Systems Review, Winter 2002 Special Issue, Boston, MA, USA, Dec. 2002.

[10] G. W. Dunlap, S. T. King, S. Cinar, M. Basrai, and P. M. Chen. ReVirt, ”Enabling Intrusion Analysis through Virtual-Machine Logging and Replay”, In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI 2002), ACM Operating Systems Review, Winter 2002 Special Issue, Boston, MA, USA, Dec. 2002.

[11] A. Householder, A. Manion, L. Pesante, G. Weaver ”Managing the threat of Denial-of-Service Attacks”, Published by CERT coordination Center, October 2001.

[12] C. Gebhardt, C. Dallon, and A. Tomlinson, ”Seperating Hypervisor Trusted Computing Base Supported by Hardware”, Proc. 5th ACM Workshop on Scalable Trusted Computing, STC?10, Octboer 4, 2010, Chicage, Illinois, USA, pp. 79-84.

[13] J.D. Hietala, ”Top Virtualization Security Mistakes (and How to avoid them)”, A SANS Whitepaper, sponsored by Catbird and McAfee, August 2009

[14] N. Liao, F. Li and Y. Song ”Research on real-time network security risk assessment and forecast”, Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference, July 2010, pp 84-87, doi: 10.1109/ICICTA.2010.273