THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Reviewing Threats Prevalent To Hypervisor

Madhuri
Asstt. Prof.
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India

Harjeet Kaur
Asstt. Prof.
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India

Gunseerat Kaur
Asstt. Prof.
School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India

Abstract
Cloud computing is the at the business epitome of the computational paradigm that has innovated for major gains being achieved by apparently anybody who makes use of its services. The security problems seem to persist at every hierarchy in this model supporting. This paper presents a brief study on the issues and challenges faced in cloud computing in case the foremost layer, Hypervisor is compromised. Initially, we identify the evasive reasons under which a hypervisor or virtual machine monitor can be compromised. A long term significance regarding protection of the core and other documented problems are enlisted, finally analyzing the taxonomy of the security issues pertaining to hypervisors and their exhibited weaknesses.
Keywords: Cloud computing, hypervisor, security, virtualization, attacks, NIST.

I. INTRODUCTION

Cloud computing has revolutionizedthe upcoming widely dispersed computer system generation that offer services as per usage, the agility is that the computing systems and resources are distributed and compute to the needs of the users. According to NIST cloud computing paradigm can be definedas appropriate, access to a centralized set of various resources (for example servers, services, storage , applications and network bandwidth) provisioning and management is done by cloud service providers. Elasticity, Pay-as-you-use, On-demand access and multi tenant environment are the main features that enable the cloud to share the same service instances and resources of the cloud model[1]. Scaling the resource up and down, focusing on resource utilization and hosting a diverse array of programs available from highly intense computational applications reduced to low weight utilities. These characteristics work together to focus on improving user experience and service availability. This model doesn't only accommodate the requirements of high end businesses but also cater to the requirements of small and medium scale upfront investments. According to a Gartner survey[2]on cloud computing earnings, worth USD 58.6B in 2009[3] was cloud market revenue , which would be expected to USD 68B in 2010 and would attain to USD

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

148B by 2014[4]. These profits implied that cloud computing is a rising platform. The attackers threat expanded and they are trying to find vulnerabilities in the existing models, therefore revenue gained still has some issues that affect the credibility and persuasiveness of that system.

Securing the cloud models is the major requirement of an organization that obstruct adaption to this model:

- Outsourcing functionalities to third party sources can cause loss of data (control loss)
- Coexistence of different users on same resource can cause irrationality of space and user access controls.
- SLAs signed between cloud consumers and cloud providers does not guaranteed for security.
- Offering these confidential and valuable data publicly increases the possibility of more attacks.

II. CLOUD COMPUTING SECURITY ISSUES

Data security is the major concern in cloud community, especially when it comes to public clouds where the data processing and storing cannot be under control, there are issues which govern major lack of control over the infrastructure managing the cloud, thereof making it vulnerable to the following security issues.

- *Data breach*: Integrity deals with-protection of data from unauthorized manipulation and fabrication whilst confidentiality governs to only authorized personnel being able to access the protected data. The data breach can be experienced from any end can be from risk of breach from internal employees. SaaS service providers should prevent data leaks and zone out various vulnerabilities preventing data breaches in order to protect user and organization's data[5]. Amongst the biggest concern to maintain integrity and confidentiality is to employ efficient public key encryption algorithms like RSA, DES, AES to enhance the perimeter of security. Apparently, the fact that these practices also are not completely free from vulnerabilities. One cannot rule out the possibility of side-channel attacks and other means of data thefts. Fine grained access control and modular security can be provided with combination of other apparent techniques like attribute based encryption and proxy encryption.
- *Data lock-in:* The customer from one cloud organization is withheld from migrating to another or such migration might take place that may lose some users data or is prevented from adopting in newer environment. [6]Coghead enlists one such examples where the customers were left looking for options such as to re-write their code in order to run their applications on other server platforms. The suggestive solution is to provide standardized cloud Application Programming Interface (API), for instance GoGrid API [7]
- *Data remanence:* Another means of achieving data for exploits is to take data from remains in various forms of storage. As a common practice the deletion of header and not the internal content falsifies that the data remains even after deletion. This serves as a channel for malicious entities to capture snippets and threaten the security. Major concerns of this kind of breach are public clouds, Storage network industry association has provided a solution to data remanence problem by encrypting and shredding the key, providing no means to retrieve back data and leaving only option of rewriting the source.
- *Data recovery:* Cloud computing works with backups very often, keeping data in a single place is not amongst the best practices. However, this practice is also an invite

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

to the failure of backups[8]. On the occasion of server breakdown the main concern is to recover data for the users but also to ensure that the vulnerable server is not affected by any breaches in the meanwhile. Some organizations provide for a backup of user services and ensure data mirroring to prevent and secure against such breakdowns.

- *Data locality:* SaaS model doesn't show the locality of data to the user, avoiding leakage of potential data and privacy governed by laws in many countries. Hence it is very important to decide the locality of the data along with its jurisdiction.

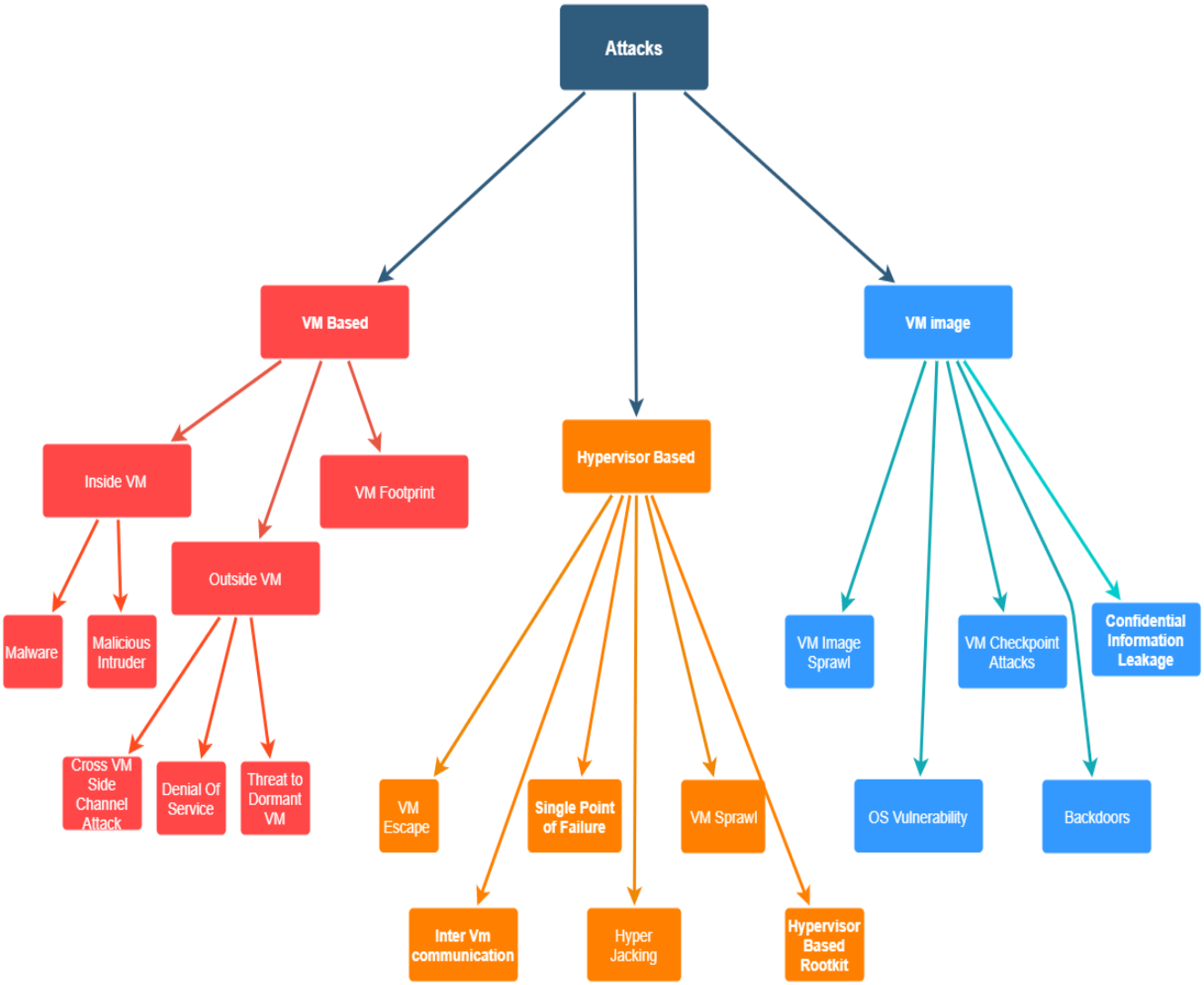

Fig 1 Chronology of various threats on Cloud computing

III. RELATED WORK

ENISA investigated some of the different security paradigms, relating to adoption of cloud based security and customer vulnerabilities and relevant challenges. The likelihood of the risks that can impact exposure in cloud computing and that might continue to affected assets and threats in related projections have been discussed by [9]. [6] discusses the security issues with Service Level Agreement's specifications which are related to data position, division and restoration of data. [10]discussed higher level of issues such as leakage of data, data breach,competence, remittance, and confidentiality of data. Kretschamann acknowledged Open Virtualization Format (OVF) and its issues with portability of malicious code as well. [11]analysed thescientifical safety related threats generating from migrating to the cloud

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

computing paradigm like XML-attacks, invasion of privacy through Web Browser. The authors represented the possible security loopholes into different categories such as technological, cloud characteristics based, security controls. [12]discussed in their paper about the privacy obstacles of the cloud service delivery paradigm, especially in the case of SaaS model. CSA [2] discussed the key issues of cloud computing. They offer a set of proven methodology for the cloud provider, cloud consumers and cloud security vendors to follow in each domain. CSA published a set of brief reports in which they put detail about some of these domains. In [5] the cloud paradigm to investigate the main reason and major indicators with security issues/problems and prevalent work. It will provide great understanding to the major issue and delivering such options.

IV. SECURITY FLAWS IN VIRTUALIZATION

Major security flaws are identified with the similarity to the physical systems that we use everyday. The following are the enlisted issues:

1. *Communication issues between VMs and Hosts*

Primal benefit of Virtualization of hypervisor is to provide independent host and guest VMs but eventually this has drawn out to be a threat as a vulnerable host can lead to complications with the isolation between the guest VM data[13].To make sure that the different programs running in any particular VM does not have permission to access another executing VM, isolation should be carefully equipped and maintained in a virtual environment. Another concern is that the host machine cannot be allowed to transfer data between the layers without permit in the same environment[14]. In VM shared clipboard is a productive feature for transferring information between host and virtual machine. Although this distinctive characteristic can also be treated as a entry point for transmission of data between cooperating suspicious program in VMs.

In certain technologies the virtual layer is also found to be listening to the keystrokes over the different virtual terminals, another association with privacy theft, these listeners were embedded over the layer and were given necessary amount of kernel privileges whilst installation, causing opportunity of breach[15]. The captured logs of the host and guest systems show how vulnerabilities were nabbed in the crux of adverse permissions[5]. Therefore some applications avoided isolation and supported portability over different platforms, exploiting the security paradigms.

2. *Virtual machine malignant escape*

The solution to the isolation issue, sharing of data over different guest and host virtual machine is to program in such a way that the virtual machine monitor doesn't allow monitoring of one from another. In other words, the host or other virtual machine cannot interact with the virtual machines because of its design method. But the companies are simply misusing the isolation[1]. To fulfil their organizational needs, they work on implementation of the dynamic isolation which damage the security of the system. Altercation to this solution is Virtual machine escape, worst case of the paradigm in which the program running in between the host and guest machine. The introduction of new software bugs has shown compromising the isolation, bypassing the virtual layer's code and hence having privilege to access the native machine. The program that gets permissions to use the native machine, as it is considered as a root, also gains the root privileges that essentially escape the virtual machine access. This leads to a total collapse of the environmental security paradigm [12]The solution is to configure each detail between the integration.

3. *Hypervisor or VMM host:*

Host machine is also termed as an access point in the virtual environment and there are ramifications that allow the host to track and interact with the updated VM programs. Therefore, the strict protection of the host machines is more necessary than the protection of

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

individual VMs. Distinctive methods provide indication for the native machine to effect the guest virtual machines. Multiple ways are available to effect the guest virtual machine running on the host, powering off or restarting of the virtual machines. Monitoring, manipulating and modifying the resources available for virtual machines done by host machine. The host machine be able to view, copy and modify applications between the data stored[5]. The host hence should be assigned separate spaces between virtual disks and separate traffic for VMs to pass through the hosts enabling the VM environment with enough isolation avoiding any gateway damage to virtual machines. Another, vulnerability is ARP poisoning attack due to which a secant hub/switch can be compromised at host level and hence guest machines can be under the same radar of packet sniffing and data breach. Due to this ,the guest machines detect the data packets in the network system or much worse case is that ARP poisoning could be used by the guest machine to divert packets to and from another guest[16]. The problem could be solved by authenticating the network traffic.

4. *Denial of Service*

A common security breach since the early stages, compromise the host and all the resources to the guests will be under influence, hence denial of service to the guest. Sharing the same underlying resources creates this problem and The system therefore denies the service to other guests requesting resources; which is in return because there is no resource accessible to other guests [17].Latest updation in the technologies provides various methods to scale down the resources provided to an individual guest machine and the proper implementation of it will ultimately reduce the ratio of DOS attack.

5. *Guest-to-Guest attack*

As previously discussed in order to secure the host machine from affecting the individual VMs. An intruder gaining the root access of the hardware primarily breaking into virtual machines and calling for guest machine to guest machine attack due to an ability to control one of the likely vulnerable machines, and its security framework being already broken[18].

6. *External Modification of a VM*

Multiple applications are available which totally rely on the hardware resource of virtualized environment. So these applicationsrxecuting on VM needs liable environment to execute that programs. If a virtual machine may be scaled due to some reason , the application could be in running stage on that VM but the reliability issues. There should be the digital signature approval before executing such sensitive applications or programs.

7. Modification of the hypervisor:

Hypervisor is the backbone of the guest machines' support and responsible of providing all the isolation and independence to the guest machines. A hypervisor with vulnerable codes will lead to the break in security design of the system and several options exist for recommended solution to secure hypervisor from any surpassing modifications or validations.

#	**Type of Attack**	**Vulnerability**	**Tools/ Causes for attacks**
1.	VM Escape	It is a vulnerability method in which an attacker attacks a host VM through a guest VM and can have access to the host operating system and all other guest operating system.	Cloudburst by Immunity canvas[5].

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

2.	Single Point of Failure	It is a risk that will have the major impact on the hypervisor which will drastically affects the virtualized environment as the VM's will become unavailable.	Pitfall in the design and implementation of the hypervisor[15].
3.	VM Sprawl	It is a phenomenon that occurs when the network's number of virtual machine reaches a level where it can no longer be handled efficiently by the system administrator	Crashme, IOfuzz
4.	Hyper Jacking	This method includes the installation of fraudulent hypervisor which will have full authorization of the server. The OS is unaware about the fact that it is being compromised as the rogue hypervisor works beneath the machine.	VENOM
5.	Inter VM communication	Inter-VM attacks refer to attacks initiated directly from one virtual machine to another, typically evading the hypervisor	ZIVM,FIDO,Xen Store[19]
6.	Hypervisor Based Rootkit	A rootkit behaves as a trojan in which the intruder can have the administration level privileges to the system. After installation, it will completely deactivate the anti malware from the infected system.	BluePill by Rutkowska

V. CONCLUSION

In conclusion the virtualization technology is to run two or more operating systems on potential costing hardware. The evident mark is the ultimate protection of the hypervisor, this paper presents the vulnerable points of hypervisor and its associated threats. The security flaws enlisted are a threat to cloud as well as the user, thus prevention and solutions have to be implemented properly. As per the discussion in this paper, analysis has been done specifically for the hypervisor-based attacks along with the tools/causes for its generation. Some attacks such as Single Point of Failure, VM Sprawl and Inter-VM communication requires some modification at the design and architectural level. On the other hand , there are some threats which can be generated with the help of various tools and different solutions exist to detect or eliminate the risk involved in these types of attacks . For exampleRedpill developed by Rutkowska is used to detect the hypervisor based rootkit attack. Similarly for the detection of VM Escape attack multiple intrusion detection systems are available , Collabra: A xen hypervisor based IDS is an example of it. To conclude,It is often an ignorance on the part of the clients to not start at the bottom level to implement varied set of security measures.

REFERENCES

[1] J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: A survey on concepts, taxonomy

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

and associated security issues," in *2nd International Conference on Computer and Network Technology, ICCNT 2010*, 2010, pp. 222–226.

[2] H. Zhou and Q. Wen, "A new solution of data security accessing for Hadoop based on CP-ABE," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, pp. 525–528, 2014.

[3] M. RezaeiJam, L. M. Khanli, M. S. Javan, and M. K. Akbari, "A survey on security of Hadoop," *Proc. 4th Int. Conf. Comput. Knowl. Eng. ICCKE 2014*, pp. 716–721, 2014.

[4] P. You, Y. Peng, W. Liu, and S. Xue, "Security Issues and Solutions in Cloud Computing," in *2012 32nd International Conference on Distributed Computing Systems Workshops*, 2012, pp. 573–577.

[5] R. Patil and C. Modi, "An exhaustive survey on security concerns and solutions at different components of virtualization," *ACM Comput. Surv.*, vol. 52, no. 1, 2019.

[6] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2012.

[7] D. J. Wu, C. H. Mao, T. E. Wei, H. M. Lee, and K. P. Wu, "DroidMat: Android malware detection through manifest and API calls tracing," in *Proceedings of the 2012 7th Asia Joint Conference on Information Security, AsiaJCIS 2012*, 2012, pp. 62–69.

[8] G. Kaur and S. Singh, "Comparison of Machine learning algorithms in Anomaly detection.," *Int. J. Adv. Res. …*, vol. 8, no. 5, pp. 2241–2247, 2017.

[9] P. Adluru, S. S. Datla, and X. Zhang, "Hadoop eco system for big data security and privacy," *2015 Long Isl. Syst. Appl. Technol.*, pp. 1–6, 2015.

[10] A. R. Riddle and S. M. Chung, "A survey on the security of hypervisors in cloud computing," *Proc. - 2015 IEEE 35th Int. Conf. Distrib. Comput. Syst. Work. ICDCSW 2015*, pp. 100–104, 2015.

[11] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[12] M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust.*, no. December, p. 7, 2010.

[13] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, 2017.

[14] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013.

[15] G. C. Obasuyi and A. Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment," *Int. J. Commun. Netw. Syst. Sci.*, vol. 08, no. 07, pp. 260–273, 2015.

[16] F. A. H. Jing, S. B. L. Renfa, and T. C. T. Zhuo, "The research of the data security for cloud disk based on the Hadoop framework," *Proc. 2013 Int. Conf. Intell. Control Inf. Process. ICICIP 2013*, pp. 293–298, 2013.

[17] K. Labib and V. R. Vemuri, "Detecting Denial-of-Service And Network Probe Attacks Using Principal Component Analysis," 1998.

[18] P. Barthakur, M. Dahal, and M. K. Ghose, "A Framework for P2P Botnet Detection Using SVM," *2012 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, pp. 195–200, 2012.

[19] M. A. Ferrag and A. Ahmim, *Security solutions and applied cryptography in smart grid communications*. .