ISSN:0975-9646

Meeting the challenge of Virtualization impact on Cloud services

N.L.Udaya Kumar[1], Dr.M.Siddappa[2]
[1]Research Scholar, Jain University, Bengaluru
[2]Professor and Head, Dept of CSE, SSIT, Tumkur

Abstract *:* Cloud computing is defined as collection of virtualized computing resources, Cloud security is one of the buzz words in Cloud computing. Since Virtualization is the fundamental of Cloud computing, it is necessary to have more knowledge to avoid attacks, intrusions and system failures. The purpose of virtual computing environment is to improve resource utilization by providing a unified integrated operating platform for users and applications based on aggregation of heterogeneous and autonomous resources. In this paper we focus on challenges of virtualization security, vulnerabilities, impact of virtualization on cloud services and propose some approaches to overcome these problems.

Key words: component; cloud computing; virtualization; security; vulnerability;

INTRODUCTION

Considering the reduction in Global warming Cloud computing is moving towards the platform of virtualization[1]. Under this technique hardware or software resources such as memory, CPU, storage, network are logically partitioned and provided to multiple tenants. However virtualization is complex and has a considerable attack surface. It is prone to bugs and vulnerabilities[2].

Generally, a cloud is discussed in terms of services. The menu of services is being enriched as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) have been invented as part of XaaS. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. By combining a set of existing and emerging techniques from research areas such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. As promising as it is, cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These Virtualization enables the organization to attain significant gains in efficiency and cost-effectiveness, along with the additional benefits of greener consolidated data center, increased scalability and improved time to resource fulfilment. Unfortunately, the advantages of virtualization are balanced by increased risk exposure as virtual systems in data center face many of the same security challenges, in addition to a number of unique challenges in protecting these IT resources. The organization needs to be consider which security mechanisms can best protect both physical and virtual servers, particularly as a virtualized architecture fundamentally affects how mission-critical applications are designed, deployed and managed.

Virtualization provides on-demand resource provisioning and multitenancy. However, current virtualization security mechanisms might not work in cloud computing. For example, traditional virtualization security solutions assume that a guest OS inside a virtual machine (VM) is known in advance. In Cloud computing, the guest OS running in a VM is controlled by a user, and a prior knowledge of the guest OS is unavailable. In this paper we focus on challenges of virtualization security, vulnerabilities, impact of virtualization on cloud services and propose some approaches to overcome these problems.

VIRTUALIZATION COMPONENTS

Virtualization is one of the most important elements that makes Cloud computing. It is a technology that help IT organizations optimize their application performance in a cost-effective manner, but it can also present its share of application delivery challenges that cause some security difficulties. Most of the current interest in virtualization resolves around virtual servers in part because virtualizing servers can result in significant cost savings. The phrase virtual machine refers to a software computer that, like a physical computer, runs an operating system and applications. An OS on a virtual machine is called a guest operating system. In addition, there is a management layer called Virtual Machine Monitor (VMM) or Hypervisor that creates and controls all virtual machines in virtual environment.

A Hypervisor is one, which is responsible for creating virtual machines out of available physical machine and sharing the available resources across created virtual machines. It is so named because it is conceptually one level higher than a supervisor. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest OS. Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisor is installed on server hardware whose only task is to run guest operating system.

Challenges Of Cloud Virtualization Security

Malware: A virtualized system uses the same operating system - and enterprise and web applications – as a physical system. The primary threat to these virtualized systems is the capacitry of malware to remotely exploit vulnerabilities in these systems and applications, although there are also vulnerabilities that can be exploited in the system's hypervisor [see figure].

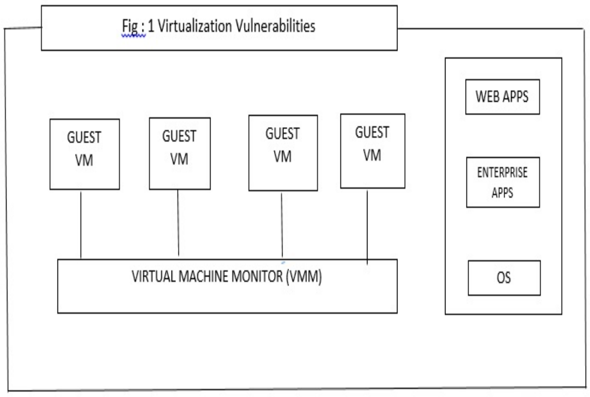


Fig : 1 Virtualization Vulnerabilities

Confidentiality: A user can access Saas offerings via a web browser over the internet. The user's network traffic and data should remain confidential in transit – that is, protected from unauthorised access. Adopting HTTPS mitigates confidentiality risks. Additionally, because a user can upload data to a cloud when using the Saas offering, the cloud should also prevent unauthorised users from reading the stored data. A Paas provider offers a development environment to establish web services or applications and thus has similar confidentiality concerns. In Iaas, multiple users can rent computing resources from a single physical infrastructure. Thus, confidentiality in this case requires isolating resource usage among the multiple users – that is, one user should not be able to view another user's memory status or resource use. Furthermore, because Paas is based on Iaas virtualization, protecting the status of resource use is also a security challenge in Paas.

Integrity: Integrity is damaged if an illicit user executes, modifies, suspends, copies, replays or delays data, messages or assets. Attackers are often interested in different targets, such as network traffic or virtual disks, so the integrity mentioned here varies based on the attack and service model. Similar to the discussion about confidentiality in Saas, we need to protect data in transit, stored data and network traffic. In Paas and Iaas, the integrity of the platform settings and configuration files is especially important, because if someone maliciously modifies such settings or files, it would affect not only the Paas and Iaas offerings but also the services deployed through those offerings, such as Saas applications. The business scenarios for cloud computing, to some extent, magnify the security challenges.

Availability: Availability is endangered if the service or server is spoofed, penetrated or suspended and can't operate as expected. Since broad network access is essential to cloud computing, the internet-facing resources, such as the Domain Name System(DNS) are one of the main targets of attacks on availability. DNS attacks are not new in the IT security realm. However, the attacks are still problematic in cloud computing owing to its characteristic broad network access. A user can't access the service offering over the internet without reliable DNS. In addition to the internet-facing resources, the service offering itself should be secure in terms of availability.

Security Management: To accommodate on-demand self-service and rapid elasticity, security management in cloud computing must be able to immediately address and reflect the changing requests. Additionally, the scope of cloud computing could increase the load and complexity of security management, leading to another security challenge.

VM Hopping: With VM Hopping, an attacker on one VM gains access to another victim VM [6] [7]. The attacker can monitor the victim VM's resource usage, modify its configurations, and delete stored data, endangering that VM's confidentiality, integrity and availability. A prerequisite for this attack is that the two VMs must be running on the same host, and the attacker must know the victim VM's IP address. Although Paas and Iaas users have only limited authority. Thomas Ristenpart and his colleagues have shown that an attacker can obtain or determine the IP address using standard customer capabilities [5]. We thus infer that VM hopping is a reasonable threat in cloud computing. Furthermore, multitenancy makes the impact of a VM hopping attack potentially larger than in a conventional IT environment. Because several VMs can run simultaneously on the same host, all of them could become victim VMs. VM hopping is thus a crucial vulnerability for Paas and Iaas infrastructures. It could also indirectly affect Saas, because Paas and Iaas offerings are often the foundation of Saas. To develop and deliver Saas offerings, Saas providers rent or purchase computing capabilities from Paas and Iaas providers. Saas offerings deployed on victim VMs would also be vulnerable to VM hopping, affecting availability. It could also endanger Saas confidentiality and integrity if the users data is falsified when the attacker gains access to the target VM.

VM Mobility: The contents of VM virtual disks are stored as files such that VMs can be moved or copied from one host to another over the network or via portable storage devices without physically stealing a hard drive [6] VM mobility provides quick deployment but could lead to security problems, such as the quick spread of vulnerable configurations, which an attacker could exploit to jeopardize the security of a new host. Several types of attacks exploit vulnerabilities in VM mobility – including man-in-the-middle attacks [7]. Attack severity ranges from leaking sensitive information to completely compromising the guest operating system. Also, because VM mobility offers increased flexibility, it similarly increases the complexity of security management. In the Iaas model, a provider offers underlying hardware and resources as a service, and a user can create his or her own computing platform by importing a customized VM image into the infrastructure service. The large scale of Iaas makes VM mobility's impact on confidentiality and integrity in the cloud potentially larger than in a conventional IT environment. On the other hand, SLAs could reduce the complexities raised by VM mobility if they clearly stated the shared obligations of service providers and users for security management. A Paas provider offers a provider-designated computing platform and solution stacks to service users. The users exploit the libraries and API to develop their own applications on a mixed computing platform with importing their own VM images. Although Paas depends on virtualization as a key implementation technology, it does not support VM mobility, so this service model doesn't have the same security challenges as a conventional IT environment. Nevertheless, SaaS AND Paas confidentiality, integrity, and availability are still exposed to the threats raised from Iaas.

VM Diversity: Virtualization lets a user efficiently create many VMs, but securing and maintaining the VMs is difficult owing to the wide range of Oss that can be deployed in seconds. VM diversity makes VM security management a challenge, but SLA constraints could help address this issue. In Iaas, a service provider must ensure security and robustness of the services and hypervisor, while the user must properly configure their VM image and secure the service offerings. In other words, the user should share the responsibility of keeping the guest OS patched and updated. Because Iaas scatters the responsibilities of a central service provider, it's resistant to the security management issues raised by VM diversity. Similarly, Paas is robust against VM diversity compared with conventional IT environment. If the obligations of both the provider and user are explicitly described in SLAs.

VM Denial of Service: Virtualization lets multiple VMs share physical resources, such as CPU, memory, Disk and network bandwidth. A Denial-of-service (DoS) attack in virtualization occurs when one VM occupies all the available physical resources such that the hypervisor can't support more VMs, and availability is imperilled. The best approach to preventing a DoS attack is to limit resource allocation using proper configurations. In Cloud computing, DoS attacks could still occur, but having service providers set adequate configurations to restrict the resources allocated to the VMs reduces their probability. In addition, it's beneficial to configuration management to have the SLA clearly define service provider and user responsibilities.

PROPOSED SOLUTIONS

We are proposing four different approaches – one is to apply a virtual security appliance within the virtualized computing environment, to monitor the traffic flow between VMM and one or more guests [fig 2]

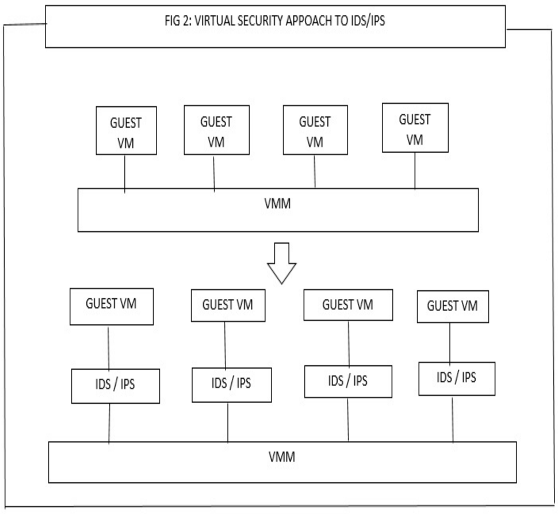


FIG 2: VIRTUAL SECURITY APPOACH TO IDS/IPS

Although a virtual-security-appliance solution provides IDS/IPS protection from attacks originating on the network, there are significant limitations to this option:

Inter VM-traffic: Virtual security appliance must be placed between VM and VMM, which cannot prevent attacks between VMs.

Mobility: If controls are used to transfer a VM from one physical server to another, the security context is lost. It is necessary to configure the clustering of virtual security appliances for every potential destination to which a VM could be relocated, resulting in a corresponding negative impact on performance.

Performance bottlenecks: The virtual security appliance must process all traffic between VMs and the network, which can result in a performance bottleneck.

In the second approach, the same IDS/IPS functionality can be applied to each virtual machine [fig 3].

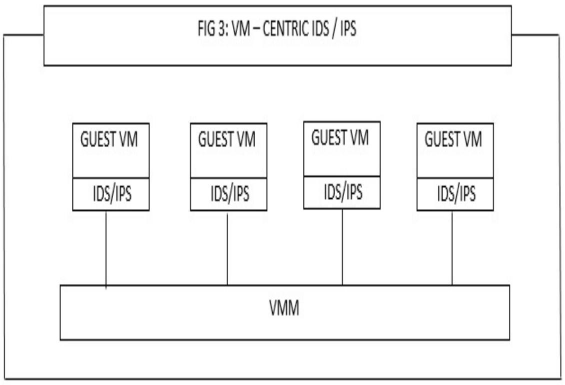
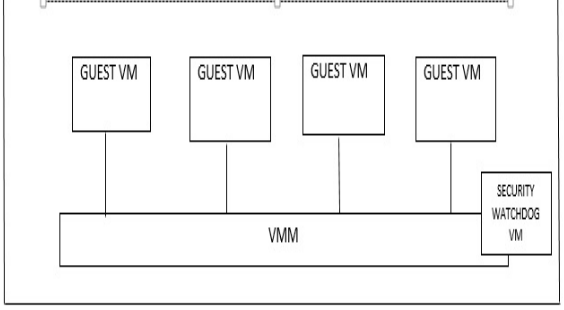


FIG 3: VM – CENTRIC IDS / IPS

Unlike the virtual-security-appliance method, the VM-centric approach avoids the limitations of inter VM traffic, mobility and lack of visibility. Although the VM-centric option also has a performance impact on the system, it is distributed across the VMs in the IT infrastructure. However, a VM-centric architecture still faces the challenge of deploying an IDS/IPS security agent on each VM.

The third approach is to introduce new means of security control, ie., Security Watchdog for Virtual Machine Monitor (VMM) itself. Security Watchdog functions utilize introspection APIs to access privileged state information about each VM, including their memory, state and network traffic. This removes the Inter-VM and non transparency limitations of the virtual-security-appliance approach for IDS/IPS filtering, because all network traffic within the server is visible without changing the virtual network configuration. However, mobility and performance impacts must still be considered when performing IDS/IPS filtering in security Watchdog.

FIG 4: SECURITY WATCHDOG VM



A wide range of security functions – including antivirus, encryption, firewall, IDS/IPS and system integrity all potentially can be applied in security watchdog VMs. Virtual security appliances are being repurposed to use these APIs, and VM-centric agent technologies also will be redesigned to execute in security watchdog VMs. However, flexibility still will be required to deploy some functionality within a security watchdog VM and within some VMs using VM-centric agents, because:

• Certain security functionality only can be achieved by VM-centric agents – for example, dealing with encrypted traffic or accessing certain real-time state information.

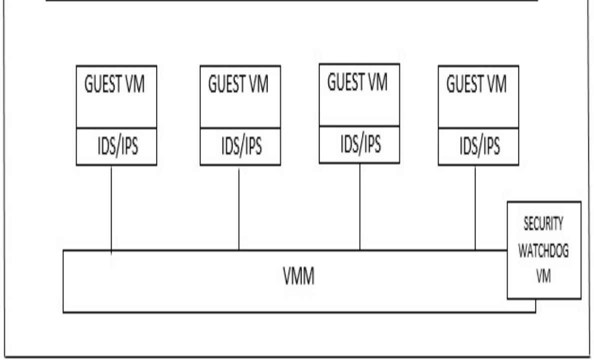
• Performance tradeoffs exist between implementing a solution via security watchdog VM versus deploying a VM-centric agent.

• Necessary introspection APIs are being developed and released in stages, you need mechanisms to deliver security during the transition as security watchdog VM functionality emerges.

As a result, a combined approach is needed – one providing both the benefits of a VM-centric approach and the advantages offered by introspection APIs, to provide intelligent options that minimize performance bottlenecks and redundant controls while cost-effectively reducing security risks.

The fourth is combined security approach to protect both VMM and Virtual machines. It consists of a VM-centric agent that can be deployed on individual virtual machine, as well as a security Watchdog for Virtual Machine Monitor and multiple virtual machines. This architecture can avoid the problems of Virtual machines and Virtual Machine Monitor.

FIG 5: COMBINED IDS / IPS APPROACH



CONCLUSION

In this paper, we discussed security vulnerabilities in cloud virtualization. Then we propose different approaches to overcome the vulnerabilities of VMs and VMM. While a virtualized IT infrastructure shares many of the same security challenges faced by physical server environments, we can leverage our investment in multiprocessor, multi-core architectures and virtualization software to provide the security mechanisms required to protect them. Adopting the combined approach with security software enables optimized protection, immediate solution deployment and ensures a baseline of security for all virtual machines without introducing bottlenecks or redundant controls.

REFERENCES

[1] Yamini B & selvi D V, 2010, "Cloud virtualization: A potential way to reduce global warming", *In recent advances in space Technology services and Climate change* (RSTSCC), 2010.pp.55-57

[2] Szefer, J., et al. 2011, "Eliminating the hypervisor attack surface for a more secure cloud", *Proceedings of the 18th ACM conference on computer and communication security, Chicago, Illinois, USA*, ACM:401-412.

[3] K.Owens, "Securing virtual computer infrastructure in the cloud", *white paper, savvis communications corp.*, 2009.

[4] A.Jasti et al., "Security in Multi-tenancy cloud", *proc. IEEE Int Carnahan Conf. security technology (ICCST 10)*, IEEE Press, 2010.

[5] T.Ristenpart et al., "Hey you Get off my cloud: Exploring information leakage in third-party compute cloud", *proc 16th ACM conf. computer and communication security* (CCM 09).

[6] T.Garfinkel and M Rosenblum, "When virtual is harder than Real: security challenges in Virtual machine based computing environments", *proc. 10th workshop on hot topics in Operating systems*.

[7] J.Oberheide, E. Cooke, and F.Jahanian, "Empirical exploitation of live virtual machine migration", *proc. Black Hat DC 2008 convention, 2011*; *www.net-security.org/dl/articles/migration.pdf.*

[8] Salesforce.com, Force.com, http://www.salesforce.com/platform/

[9] https://apps.gov/cloud/advantage/main/start page.do

[10] CloudSecurityAlliance,http://www.cloudsecurityalliance.org/

[11] G. J. Popek and R. P. Goldberg, "Formal requirements for virtualizable third generation architectures," *Comm. ACM,* vol. 17, no. 7, pp. 412– 421.

[12] Hassan Takabi, James B.D. Joshi, Gail-Joon AHN, "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Security & Privacy, 2010*, 10(6): 24-31.

[13] Siani Pearson, Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", *Proceedings of IEEE*

International Conference on Cloud Computing Technology and Science, 2010, 693-702.

[14] Prasad Saripalli, Ben Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", *Proceedings of IEEE 3rd International Conference on Cloud Computing (ICCC)*, 2013, 280-288.

[15] Gunnar Peterson, "A Security Architecture Stack for the Cloud", *IEEE Security & Privacy*, 2010, 10(5): 83-86.

N L Udayakumar received B.E degree in Computer Science & Engineering from University of Bangalore, Karnataka, India in 1993 and M.Tech degree in Computer science and engg from VTU, Belgaum, Karnataka in 2007. He has teaching experience of 16 years. He published 03 Technical Papers in National, International Conference and Journals.. He is a Life member of ISTE. He is working in the field of Cloud computing, Virtualization, Storage area networks and Computer networks. He is working as Assistant Professor in Department of Computer Science & Engineering from 2004 in Sri Siddhartha Institute of Technology, Tumkur.

M.Siddappa received B.E and M.Tech degree in Computer Science & Engineering from University of Mysore, Karnataka, India in 1989 and 1993 respectively. He has completed doctoral degree from Dr.MGR Educational Research Institute Chennai under supervision of Dr.A.S.Manjunatha, CEO, Manvish e-Tech Pvt. Ltd., Bangalore in 2010. He worked as project associate in IISc, Bangalore under Dr.M.P Srinivasan and Dr. V.Rajaraman from 1993 – 1995. He has teaching experience of 26 years and research of 10 years. He published 52 Technical Papers in National, International Conference and Journals. He has citation index of 129 till 2015 and h-index of 5 and i10-index of 2 to his credit. He is a member of IEEE and Life member of ISTE. He is working in the field of data structure and algorithms, Artificial Intelligence, Image processing and Computer networking. He worked as Assistant Professor in Department of Computer Science & Engineering from 1996 to 2003 in Sri Siddhartha Institute of Technology, Tumkur. Presently, he is working as Professor and Head, Department of Computer Science & Engineering from 1999 in Sri Siddhartha Institute of Technology, Tumkur. He has visited Louisiana University Baton rouge, California University and Wuhan University Chaina.