Analysing Security Threats and Solutions during Transition to Cloud Environment

Amit Wadhwa
Assistant Professor
Amity University Haryana

Ruchi Kamra
Assistant Professor
Amity University Haryana

ABSTRACT

Cloud computing as one and all know is a computing area which has evolved from grid, utility computing, virtualization and SOA. As per the knowledge a cloud based infrastructure is based on certain elements like extended elasticity, [3]metered service, on demand service availability[3], clustered resources and large network access. For providing these services or features it follows certain cloud service adoption models. All these models face some security concerns or the others. In the past many security models[1] are presented by many researchers for resolving them and giving out a better known solution to IT industry adopting cloud. This paper aims at analyzing issues involved with virtualized architecture incurred while cloud migration, figuring out various security measures from varying risk levels and present a refined or distinguished security model or solution based on all those issues discussed throughout the study. Main focus of the analysis carried here is on issues involved while adopting virtualization based infrastructure for moving in cloud, authentication based risks, risks incurred while data migration, attack on VM's, issues while adopting virtualization, risk generated from malicious insiders are few to be discussed here.

General Terms

Cloud Computing, Virtualization, Security Threats

Keywords

Cloud Security Threats, Virtualization, VM (Virtual machine), CSP (Cloud service provider), Hypervisor, Virtual machine manager (VMM), VDC (Virtualized data center).

1. INTRODUCTION

Cloud computing, as defined by NIST [4], is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". For using the cloud based services, every user subscribes them by registering with a CSP based on a well defined and restricted service-level agreement (SLA). Generally computing resources are provided to users or cloud adopters as virtual machines (VM). In order to accomplish the above said processes one requires a cloud interface with which users can submit a request to access the virtual machine available with a host. These front-end interfaces and connected resource hosts are managed by a central server whose task is to provision these resources.

The all above core components like server, [2] host machine and users are normally authenticated using certain [2] cryptography based protocols.

Now a days, organizations or businesses choose the cloud as a solution based on certain considerations like, as generally business owners do not know the deep insights about the technology emerging today. So, it becomes much convenient to have experts working in a system to look after all IT aspects like managing licences, software related update and architecture based on network to name a few. Secondly, a business or organisation getting started during the setup time just requires some initial investments in field of IT infrastructure. By using the pay-per-use service of a cloud service provider (CSP) one needed to pay only for the resources it works with. Another main and important advantage of the cloud is that it is flexible, scalable and extensible enough to meet the increasing IT needs. [2]The three advantages mentioned above and many more that invite many companies to move into the cloud architecture from their traditional non virtualized architectures, provided and making security of system at stake [2].

Cloud based architectures introduced by cloud service providers offer users with three different and inherent levels of services namely Infrastructure as a Service (IaaS), [1],[3]Platform as a Service (PaaS), or Software as a Service (SaaS)[1]. Clients who want to use IaaS service will have access to hardware components like servers, host/compute etc. and software components like OS, [4]virtual machine manager (VMM) and applications etc. For using it they require [2]dummy machines to experiment or even smart devices like smart phones, PDA's and tablets etc, for making them able to access the different services offered by the CSP. [2]The other service level is PaaS which offers the client software packages that allow software development and running. [2]Ultimately software as service allows users to have access to a set of applications provided by CSP managing them over the network.

2. TRANSITION AND OTHER ISSUES ADOPTING AND IMPLEMENTING CLOUD

Here in this paper, various security issues and concerns will be analysed and classified, these were extracted from the literature representing various dimensions to risks involved in this architecture.

2.1 Steps with Issues Adopting Virtualized Infrastructure

Virtualization is basically about abstracting physical resources from users view level and providing them as their virtualized instances. It allows users to use those resources in a virtualized manner then allocating them dedicatedly. While building cloud infrastructure a layer cloud service management is required over a VDC. And for having a VDC in architecture all the resources of a data center need to be virtualized. It can be visualized as shown here in Figure 1.

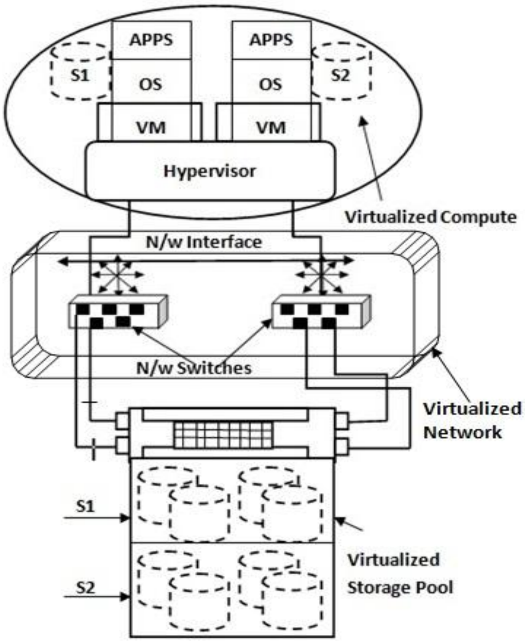

Figure 1: Virtualized Data Center in Cloud Environment

[3]Challenges faced while virtualizing a data center are discussed with following steps:

Step 1- Virtualize Compute/Host: In order to virtualize compute or host running user applications a layer of virtualization is introduced between other layers of architecture and compute. The layer has a hypervisor over which VM's work, and above VM's OS and applications work. So, in order to introduce these layers user's view is abstracted and it will increase the security breach chances as we have to provide security at VM level, hypervisor level and also OS and apps running in various VM's needed to be installed keeping the intermixing of user's data in mind. And this introduces a hell lot of complexity and risk factors in the architecture.

Step 2- Virtualize Network: Next step would be to virtualize the network level layer. For doing that one might use [3] VLAN's and VSAN's architectures. In both the architectures the networking devices used have to be configured to address multiple users request coming from above layer of compute. In order to do that these architectures of [3]VLAN and VSAN's use different techniques like NIC teaming, zoning etc to address issues raised with multi-tenancy architecture having VM's installed on same physical architecture controlled with a hypervisor.

Step 3- Virtualize Storage: In order to virtualize the storage area of a data center things like working with virtual volumes, creating logical virtual partitions of the storage area using concept of virtual storage provisioning to create [3]LUN's is needed. Finally allocating storage to the user working over the network layer at compute level is handled by allocating virtual LUN's generated from shared virtual [3]storage pool managed by special software installed over storage level.

2.2 Security Concerns Developing over Cloud

Apart from the above mentioned issues emerged while implementing virtualized architecture over a cloud there are some other security concerns which are required to be addressed. The Issues which require concern are like:

- Multi-Tenancy: As it is one of the important features of cloud, providing great benefits as multiple users can use the same hardware and work on same server simultaneously and independently. But this would also possess a great threat to the system as its harder for the CSP's to provide uniform security level to various users working in different platforms. As in it if an OS is compromised then it might impact the security of other users using same server.
- Attack Rate/Factor: As the cloud is a huge network of servers and computes connected over the network and CSP has to make them available to its users with all the features like ease of use and efficient processing requirements, in order to provide that it uses different technology options and different types of heterogeneous hardware devices. Providing security to these different types of hardware is very difficult for CSP to manage.
- Information and Data Ownership: In all information providing system authentication and authorisation of its users is major point of concern for the provider (CSP in case of cloud platform) or system manager. [3]Main focus of cloud based architecture is also on providing feature of confidentiality, proof of integrity and the major requirement of availability of data to its users.
- Privacy of Data: CSP has to make sure that data of all users working over the network or cloud architecture is safe from every perspective and in order to do that it has to decide a security policy. Private data of cloud users need to be protected from unauthorised access and disclosure which holds a major point of concern.

2.3 Key Security Threats over Virtualized Cloud Architecture

Apart from the above mentioned point/areas of concern following are the key security threats that emerge over virtualized architecture:

- VM Theft and VM Escape[3]: Theft associated with VM corresponds to the unauthorised copying of VM files stored under [3]VMFS (virtual machine file system) and VM escape corresponds to the mechanism where applications running over host would try to override OS and VM and start interacting directly with virtualization layer. Overriding process results in attacker accessing all other VM's working over that virtualization layer.
- Faulty Hypervisor: It corresponds to the phenomenon where an attacker tries to attack over install a faulty hypervisor or virtual machine manager to gain access to the underlying server without the knowledge of guest OS.
- Denial of Service[5] (DOS and Distributed DOS) Attack: In this phenomenon the actual users of an information provider system are debarred from the services and resources provided by that system. DOS attack might affect network components and other resources available on host system for legitimate users.
- Another attack would be Distributed DOS attack[6] where a rogue DDOS master program is installed over a stolen account of some user and with this the attacker

could access and attack other users working over the same network.

- Leakage of Data: Basically in this the attacker is the one which is working with a [5]VM on a server and he might attack on the preceding VMs running over the same server, thereby generating unauthorised access to the confidential data of the users working with the attacked VM. It poses a great threat to the temporary or cached file stored on the attacked VM's.

3. SOLUTIONS TO CLOUD SECURITY THREATS

As discussed above there are various points of concern and threats from which cloud users are required to be protected and CSP has the responsibility of providing perspective security levels in order to allow users to work freely without worrying about the underlying threats in the architecture[6]. So here an insight onto some thefts and their proposed solutions to be employed by CSP in order to gain and maintain trust among his customers will be put forward.

- Protection against threats imposed by multi-tenancy, VM Theft and escape: In order to provide protection at compute level holding VM's with OS and apps, [5]CSP should keep track on the unused components like NIC's, HBA's and disk drives employed in the architecture. As all these impose and act as an open point of attack and result into vulnerable contact points to attackers. For providing security against VM theft and escape one would restrict to limit the movement of VM's working over a server and access to [3]VMFS must be protected with some security algorithms. One would implement technique of VM isolation and changing the default configuration of servers in order to prevent compromised guest OS affecting other VM's on the server. Another solution to protect VM's is to take backups of VM's from time to time and isolate the VM under attack automatically.

- Protecting Hypervisor: Hypervisors act as single point of failures as attack on them would make all VM's working over it vulnerable to attack. If a hypervisor is not in use then it should be blocked for any time of access in that configuration which would bring down the surface of attack.

- Protection against Data Leakage: A firewall can be used dedicatedly for providing security to hypervisors and VM's running over it thereby restricting access to all admin interfaces by that firewall. Another use of that firewall if to monitor VM to VM traffic making it works as a virtual firewall implemented over the network level.

- Protection against DDOS attack: Protection against such type of attacks is necessary as they consume too many resources of the server over which it happens. So in order to prevent those attacks security policies implemented over VM's must be hardened and restricted access to VM's must be provided, thereby limiting the attack surface and it might be blocked in case the limit of access has been reached.

4. CONCLUSION

Here in this paper, the process of transition from a classical to virtualized environment is discussed, thereby presenting steps involved while moving to cloud based architecture. Secondly some security concerns emerging over cloud based virtualized environment like employing multi-tenancy, ownership of data and information and other privacy related issues of data placed over a cloud environment are also put stress upon. Then various emerging upcoming threats faced in a cloud environment like VM theft and escape, security of hypervisors and DDOS attacks are elaborated in a proper way. In the end some solutions to the above discussed security concerns and threats emerging in coming cloud based models implemented by most of the IT organisations or businesses are presented.

5. REFERENCES

[1] Amit Wadhwa and Dr. V. K. Gupta, "Framework for User Authenticity and Access Control Security over Cloud". International Journal on Computer Science and Engineering (IJCSE), Vol 06, No. 04, April, 2014

[2] Mhammed Chraibi, Hamid Harroud and Abdel. Maach, "Classification of Security Issues and Solutions in Cloud Environments", International conference based on Ad-hoc generalized Wireless Sensor and networks, by ACM, at Vienna, Austria, Dec, 2013

[3] Gnanasundaram, somasundaram, and Shrivastava, Alok. *Information Storage and Management.*. USA: Wiley, 2013. Print

[4] Mell, P. and Grance, T. "The NIST definition of cloud computing". publishd inNIST Special Publication, 2011

[5] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur : "Security Issues in Cloud Computing" (Book review): Springer-Verlag Berlin Heidelberg, pg. 36–45, 2011

[6] NIST, Guidelines on Security and Privacy in Public Cloud Computing, presented in 2011

[7] J. Ru and J. Keung. "An empirical investigation on the simulation of priority and shortest-job-first scheduling for cloud-based software systems" In Software Engineering Conference (ASWEC), 2013 22nd Australian, pages 78–87. IEEE, 2013.

[8] (2010). Security Management in the Cloud. Available http://mscerts.net/programming/Security%20Management%20in%20t he%20Cloud.aspx

[9] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009

[10] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009

[11] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons et.al., "Managing Security of Virtual Machine Images in a Cloud Environment", ACM Cloud Computing Security Workshop (CCSW'09)

[12] Meiko Jensen, Jörg Schwenk and Nils Gruschka, "Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, Bangalore, India 9/2009