A surface study on cloud infrastructure and categorization of cloud threats

Mohammad-Reza Memarian

September 2014

1 Introduction

Most of the issues which are accused to be threats against cloud computing are not new security issues toward computing world. They existed before creation of cloud computing concept too. The impact of those threats may vary in cloud context and out of cloud context. Various researchers have categorized cloud threats with different approaches. In section 2 of this material, cloud threats have been categorized based on other articles and author's analysis of the matter. In section 3, a generic discussion of cloud platform key components has been done. In section 4, notable related works in addition to some explanation out findings has been discussed.

2 Cloud threats categorization

It is not possible to sketch a clear line between cloud specific threats and other type of threats. Although cloud related threats were a danger to the security of computing beforehand too, but some of them get more bold when performing in cloud context. Indeed some specifications in the nature of cloud computing are sources of cloud related threats. According to [1], cloud related threats are either prevalent in one of the cloud computing core technologies, or one of the five cloud essential specifications is the source of their cause. Other reason would be that they are existing because of the lack of controls which existence of cloud computing causes that, or they are prevalent in the state-of-the-art cloud offering. The core cloud technologies are virtulization, web services/applications and cryptography. According to [2], five essential cloud characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services.
Virtualization plays a vital role in the heart of the cloud infrastructure. It is deployed because of economy of scale but on the other hand it attracts various risks to the security of the cloud. Although IaaS model is mostly integrated with Virtualization, but SaaS and PaaS are also affected by vulnerabilities in virtualization as they are built on top of IaaS model. Various security problems

which are related to secure consumer's data storage on and transfer to cloud can be partially solved by cryptography. On the other hand breach in the crptographic algorithms may cause various harms to the cloud confidentiality. In the case of web applications, as an instance it is very prevalence that users are just authenticated through a simple user name and password for using from a web service that this matter affects cloud authentication and authorization issue. In a material prepared by NIST, another approach has been used toward cloud threats identification. In [3], there are nine top level threats which are cloud threats and are specially related to shared and on-demand nature of the cloud. These threats in order of importance are Data breach, Data loss, Account hijacking, Insecure APIs, Denial of services, Malicious insiders, Abuse of cloud services, Insufficient due diligence and Shared technology issues.
So generally as mentioned earlier, as cloud is constructed based on several technologies, it is vulnerable to the same threats that it's core technologies are vulnerable to. According to [4], notable security issues related to cloud infrastructure are Abuse use of cloud, Insecure interfaces and APIs, sharing technical flaws, cloud security mis-configuration, service disruption, multi-tenancy, side channel attacks, data security and loss and leakage. The mentioned categorizations have been analyzed. The result is a new cloud threat categorization table with focus on cloud infrastructure. Because of the size limitation, it is provided in an pdf file outside of this material. There exist standards from well-known and globally accepted agencies which have defined in each of the areas of concern various standards to be used as best practices to handle the situations. In a document created By NIST in [5], eight areas of concern are mentioned and the maturity status is sketched in tabular format. It is a very rich and complete technical material that can be used as a reference toward assessing various cloud components.

3 Cloud Infrastructure architecture

In this section a very generic description of cloud platform components is discussed. There are various open source platforms which make service providers capable of offering IaaS. Although architecture of the software and hardware used to deliver cloud services can be different among cloud service providers for different service models, but generally the platforms used by them have same core components and modules.
In IaaS, Client has total control over Software stack and provider has admin control over hypervisour and total control over hardware. Customers will be able to configure their virtual networking features through interfaces that are provided to them through hypervisour by the provider. Cloud components communicate with each other through application programming interfaces. According to [6], three vital components of cloud infrastructure platforms are Cloud manager, Cluster manager and Computer manager. These terms have are referred as other names in different platform. In Eucalyptus deployment these components are called cloud controller, Cluster controller and node controller respectively.

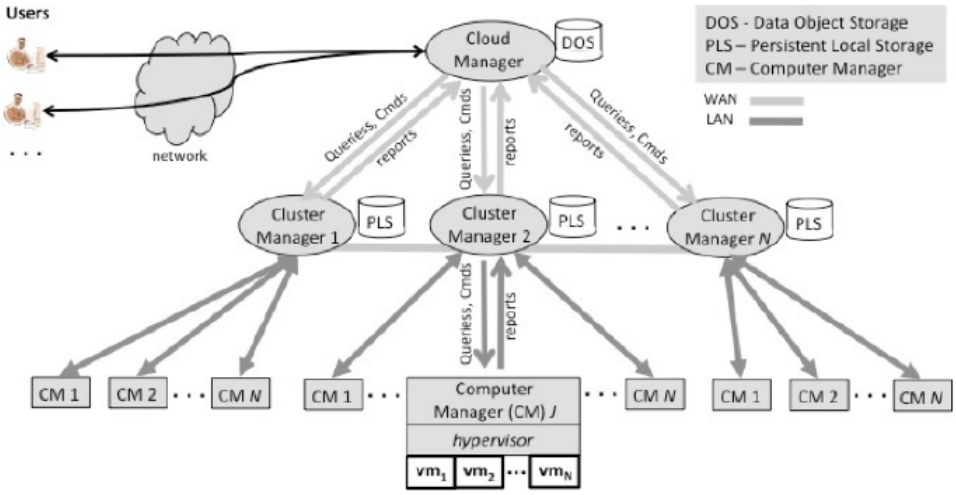

Figure 1: Figure 1: Logical IaaS infrastructure

A very short description of each component is given below.

3.1 Cloud manager

Cloud manager is the public access point to the cloud in case of public cloud where users sign up for using the services. it's main responsibility is to manage the resources that consumers rent from the provider, user authentication, generation and validation of credentials and top level resource allocation. In the case that consumer send a request to employee some resources, the cloud manager determines availability of the resources in one of the clusters. Cloud manager tightly cooperates with cluster manager as well as Data object storage repository. As clusters may be located in different geographical locations, normally the network connection of cloud manager and cluster managers are through WAN and high speed networks.

3.2 Cluster manager

Cluster manager is responsible for number of computer systems (may be as large as hundreds of systems)which host several virtual machines. cluster manager receives resource request commands from cloud managers and calculates what portion of the request can be satisfied by computer systems in that cluster. Cluster managers are connected to nodes via LAN connections and they are connected to Persistent Local Storage.

3.3 Computer manager

Computer manager cooperates with the hypervisour running on each node of a cluster. Computer manager sends status messages on possibility of starting new virtual machines in response to resource requests from cluster managers. As virtual machines running on a node may be allocated to various users, computer manager is responsible for preparation of isolated environments by using facilities of its hypervisour.

3.4 Hyprvisour and virtual elements as Attack surfaces

Based on [7], There exist various attack surfaces which gives opportunity to attackers for accomplishing their malicious activities in the cloud. Hyperviosur is one of those elements which causes widening of attack surface through channels and APIs. In virtualization, there are security concerns about virtual network protection and virtual machine images. Of course the security of a computer system depends on the quality of the underlying software kernel that controls the execution of the processes. As a result, if Hypervisor and underlying virtual infrastructure are compromised, the whole virtual client virtual machines on that system are taken. Different attacks toward virtualization are mentioned in our excel threat excel table.

4 Discussion and related work

According to my own findings, I would like to discuss some interesting topics here.
a) Cloud infrastructure architecture is very complex and advanced. So assessing all the components with regard to some standards may not be practical and still is too general. If we consider openStack as a case study, the following pieces of components operate in it: openStack Compute(Nova), OpenStack object storage(swift), OpenStack image service (Glance), dashboard (horizon), Identity management (keystone), Networking (Quantom) and many more. Meanwhile I have to mention that cloud manager plays a vital role in the overall IaaS architecture. If our desire is to do assessment, I think it is better to focus on the cloud manager component (other components can be nominated too), choose a platform as a case study and get it under assessment. For an instance, cloud manager APIs can be assessed for possible vulnerabilities. In general, some of the notable comparison papers can be found in [8], [9].

b) During my readings, I noticed a problem in Image repository system of the cloud which of course is not a new problem but is important. There are some very notable works which been done on this matter. The problem is lack of proper and secure management of VM images in image repositories of cloud systems. Users when using from the cloud services are able to either publish an image or retrieve an image. For an instance a developer can publish a preconfigured image with necessary software and configurations for certain group of users. There are some risks for publishers as either their private data may be

published or unauthorized entities may get access to the image. On the other hand retrievers may be at risk of using images with malwares being embedded in them. With the consideration that large providers have image repositories of thousands VM images, scanning these images and detecting malicious activities among them is a time-consuming, energy-consuming and unreliable work. Service providers normally do not have proper and secure handling about this matter as in Amazon website it has been stated that the third party images are used based on consumer risk. So service providers mostly act as image storage entities. The first secure VM management has been designed in [10] in 2009(Based on author's declaration). In [11], model introduced in [10] and other existing methods by 2012 plus each one's pros and cons have been discussed. VM image security is an important matter as VM security is the primary stage in the cloud security.

References

[1] E. S. Bernd Grobauer, Tobias Walloscek, "Understanding cloud computing vulnerabilities," Siemens, Tech. Rep., 2011.

[2] T. G. Peter Mell, "The nist defenition of cloud computing," National Institute of Standard and Technology, U.S. Department of Commerce, Tech. Rep., 2011.

[3] , "The notorious nine cloud computing top threats in 2013," Cloud security alliance, Tech. Rep., 2013.

[4] S. B. A. A. Issa M. Khalil, Abdullah Khreishah, "Security concerns in cloud computing," in .

[5] , "Nist cloud computing standards roadmap," National Institute of Standard and Technology, U.S. Department of Commerce, Tech. Rep., 2013.

[6] R. P.-C. J. V. Lee Badger, Tim grance, "Cloud computing synopsis and recommendations," National Institute of Standard and Technology, U.S. Department of Commerce, Tech. Rep., 2012.

[7] T. G. wayne Jansen, "Guidelines on security and privacy in public cloud computing," National Institute of Standard and Technology, U.S. Department of Commerce, Tech. Rep., 2011.

[8] N. J.-R. P. Oliver Popovic, Zoran Jovanovic, "A comparison and security analysis of the cloud computing software platforms," *TELSIKS*, 2011.

[9] F. W. G. C. F. Gregor von Laszewski, Javier Diaz, "Comparison of multiple cloud frameworks," in .

[10] G. A. V. B. P. N. Jinpeng Wei, Xiaolan Zhang, "Managing security of virtual machine images in a cloud environment," in .

[11] K. K. K. S. K. Gundeep Singh Bindra, Prashant Kumar Singh, "Cloud security: Analysis and risk management of vm imahes," in .