Journal of Theoretical and Applied Information Technology
20th August 2013. Vol. 54 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY OF CLOUD COMPUTING SECURITY OVERVIEW OF ATTACK VECTORS AND DEFENSE MECHANISMS

[1] M. LEMOUDDEN, N. BEN BOUAZZA, B. EL OUAHIDI, [2] D. BOURGET

[1] Mohamed-V University-Agdal Rabat, Faculty of Sciences, L.R.I. B.O. 1014 Rabat Morocco
[2] Institut Mines Telecoms, Telecom Bretagne,Technopôle de Brest IROISE, 29238 Brest Cedex, France
E-mail: [1]{mouad.lemoudden,ben.bouazza.naoufal, bouabid.ouahidi}@gmail.com, [2] daniel.bourget@telecom-bretagne.eu

ABSTRACT

Enterprises are more and more moving to the cloud to take advantages of its economic and technological model. However, Privacy and Security issues are often cited as the main obstacle to the adoption of cloud computing for enterprises; hence we need to have a clear understanding of security needs in the cloud in order to achieve solutions. The aim of this paper is twofold: firstly, to distinguish general security issues from cloud-related, and secondly, to provide an overview of attack vectors and defense strategies.

Keywords: *Cloud Computing, Security, Vulnerability, Threat, Attack, Defense.*

1. INTRODUCTION

In a network diagram, the Internet portion is represented by cloud graphic, which typically represents the part of the system solution that is owned by someone else. But it's not simple to equate cloud computing to the Internet. Business may choose to access applications that reside in the cloud; this would eliminate the need to install applications locally in every computer in the company, and make updates/upgrades easier since someone else is hosting and it's completed by them. Moreover, one of the biggest advantages to the cloud is the ability to access your applications and data from anywhere on any device that connects to the Internet. With cloud computing a business can cut operation costs, while allowing IT department to concentrate on strategy as opposed to maintaining the data center on premises. Cloud computing is indeed gaining traction with businesses all over the world and the benefits seem overwhelming, but one of the biggest obstacles for the adaption of cloud computing is security.

Numerous factors are pointed to be an obstacle to the adoption of cloud computing [1]: processing of sensitive data outside the enterprise, shared data, ineffectiveness of encryption, among others.

Before we dive into cloud privacy and security issues, we'll give an overview of cloud computing definition and architecture. As a broad of definitions have been given to explain cloud computing, we adopt the definition of cloud computing provided by The National Institute of Standards and Technology (NIST), since it covers, all the essential aspects of cloud computing [3]:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is composed of five essential characteristics, three service models, and four deployment models.

• Essential Characteristics: (On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service)

• Service Models: (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS))

• Deployment Models: (Private cloud, Community cloud, Public cloud, Hybrid cloud)

This paper is a survey on state of the art of cloud computing security. First, we'll explore exactly what are the security principles and terms, because one of the most confusing things about security is security terms, and in some cases those are used interchangeably. We'll then discuss traditional security and cloud-specific security. From there, we'll go hands-on as we examine some common attack vectors in the cloud. Finally, we'll tackle some defense strategies for cloud computing.

Journal of Theoretical and Applied Information Technology
20th August 2013. Vol. 54 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. VULNERABILITIES, THREATS AND RISKS IN THE CLOUD

2.1 Vulnerabilities

According to the Open Group's risk taxonomy [2], Vulnerability is "the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force. ". In this sense, vulnerability is described in terms of resistance to a certain type of attack. Cloud computing could change the probability of a harmful event's occurrence, causing significant changes in the vulnerability factor. In this section, we differentiate between two types of vulnerabilities:

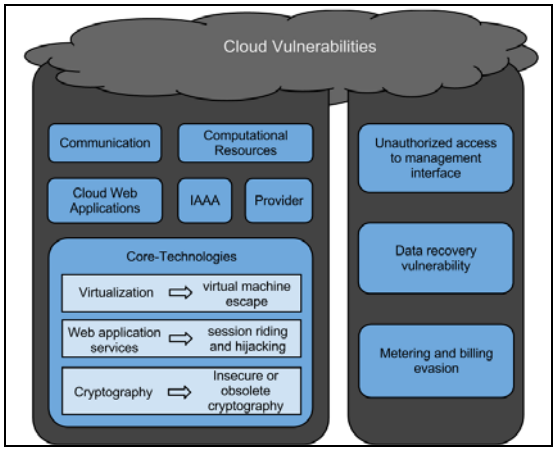

Figure 1: Two types of Cloud related Vulnerabilities

- Cloud-Related Vulnerabilities:

Computational resources are a highly relevant set of vulnerabilities that concern how virtual machine images are managed. Because cryptography is frequently used to overcome storage-related vulnerabilities, this core technology's vulnerabilities play a special role.

Resource pooling is one of the main characteristics in the cloud, and because of that, several customers are likely to share certain network infrastructure components which links to vulnerabilities of shared communication.

Vulnerabilities associated with the IAAA (Identity, Authentication, Authorization, and Auditing) elements must be regarded as cloud-related because they're prevalent in state-of-the-art cloud offerings. Of these IAAA vulnerabilities, authentication-related ones primarily put user data at risk.

Vulnerabilities that are relevant in the cloud typically concern the provider; among them are insufficient security audit options, lack of standard security controls regarding audit and logging [15], certification, and continuous security monitoring.

To meet its characteristics, the cloud relies heavily on capabilities available through several other core technologies, namely web applications and services, virtualization (IaaS offerings), and cryptography. Each of these technologies has vulnerabilities that are either intrinsic or prevalent in its state-of-the-art implementations.

Vulnerabilities in standard security controls must be considered cloud related if the cloud innovations directly cause difficulties in implementing the controls. Such vulnerabilities are also known as control challenges.

- Essential Characteristic Vulnerabilities:

As noted earlier, NIST describes five essential cloud characteristics. However, in some of these characteristics, there may underlie a basis for a vulnerability; for example, Unauthorized access to management interface which is caused by cloud characteristic on-demand self-service, Data recovery vulnerability which is a result of cloud characteristics elasticity and resource pooling (there is the possibility of recovering data written by previous user), and Metering and billing evasion is finally a resulting vulnerability of the measured service characteristic; the data able to achieve this characteristic can be manipulated.

2.2 Threats

According to the Open Group's risk taxonomy [2], a threat is "Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures." A threat can be either intentional or accidental, and is a possible danger the can exploit a vulnerability with the potential to adversely impact systematic operations.

Essential to cloud adoption risk management, the first step for organizations is to identify precisely where the greatest cloud threats lie. For the reasons of providing a needed context, we have identified top threats that can result in harm, ranked in terms of severity, based on a Cloud Security Alliance (CSA) study [4]:

Journal of Theoretical and Applied Information Technology
20th August 2013. Vol. 54 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 2: Top Cloud Threat in terms of relevance

Data Breaches: to illustrate the potential magnitude of this threat, a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server; allowing an attacker to get at not just that client's data, but every other clients' data as well. The challenge is that the measures put in place to mitigate one of the threats can exacerbate another. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data.

Data Loss: with the possibility of causing devastating impact, a loss can considerably introduce financial implications, legal ramifications, influence on trust between different actors related to a business and damage to reputation. Data Loss can occur due to malicious intent, accidental deletion by provider, or worse, a physical catastrophe leading to permanent loss.

Account/Service and Traffic Hijacking: this type of threat typically has to do with credential theft, which leads to compromises on confidentiality, integrity and availability of deployed cloud services. Cloud service providers should be aware of these practices as well as possess a defense strategy that prohibits the sharing of account credentials between users and services.

Insecure APIs: usage of weak APIs exposes organizations to issues such as malicious or unidentified access. APIs play an integral part in management of a cloud environment; their security is synonymous with that of the cloud.

Denial of Service: DoS has always been an Internet threat, but it resurging in frequency and sophistication in the cloud. DoS outages prove to be costly for customers, which may have a direct impact on quality of service (QoS) that a cloud service provider promises to a cloud client over a Service Level Agreement (SLA) that can lead to penalty in this case.

Malicious Insiders: considering the level of access, malicious insiders can break the trust of different parties, cause financial impact, brand damage and productivity. This kind of human element threat is present in all types of service models, so it's critical that the cloud service provider possesses a defense process to contain damages.

Abuse of Cloud Computing: an example might be a malicious hacker using cloud servers to break an encryption key too difficult to crack on a single computer, launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes to identify it.

Insufficient Due Diligence: this threat has to do with organizations embracing the cloud without fully understanding the cloud environment and associated risks, giving rise to operational and architectural issues, or contractual issues over liability and transparency.

Shared Technology Vulnerabilities: this type of threat targets the shared technology inside the cloud environment: disk partitions, CPU caches and other shared elements. A defense in depth strategy is recommended, and should include storage, and network security enforcement and monitoring.

2.3 Risks

According to ISO 27005, Information Security Risk Management guideline, risk is "the potential that a given threat will exploit Vulnerability of an asset or group of assets and thereby cause harm to the organization [7]." Risk is the probable frequency and probable magnitude of future loss.

So how do we quantify risk? In essence, we say that risk is a function of threats as they seek to exploit vulnerabilities, and in light of the countermeasures, we apply to protect our assets. However, this is difficult because it requires that we determine tangible values for somewhat intangible assets; meaning that we need to quantify risk at an appropriate order of magnitude. This is the risk formula used in information security [5]:

$$\text{Risk} = \left(\frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Countermeasures}}\right) \times (\text{Asset value})$$

It is envisioned that more and more businesses will adopt cloud services and subsequently own no IT assets. Figure 3 shows a list of Cloud Computing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and SaaS Models top 10 security risks, as compiled by OWASP [6].

Figure 3: Top 10 Cloud Security Risks

3. CLOUD COMPUTING VECTOR ATTACKS

An attack vector is a path by which a cyber criminal can pick up access to a network server or a computer in order to deliver a malicious effect.

In an information security context, one can achieve deception by exploiting stereotypical thinking, processing ability, inexperience, truth bias and other semantic attack vectors [8].

With the advent of cloud computing and the shared usage of resources, large volumes of data is being stored and the number of users has increased heavily. In the wrong hands, these volumes of data can lead to severe situations. To some degree, firewalls (set of programs that protect the resources of a private network from users from other networks) and IDS (Intrusion Detection Systems) can block attack vectors. But no protection method is totally efficient; a defense method can be effective today but may not remain so for long, because cyber criminals are continually updating attack vectors, and seeking new ones.

Some of the potential attack vectors hackers may attempt include:

Denial of Service (DoS) Attacks: A denial-of-service (DoS) attack involves a disruption to the normal functioning of a website or web service. Because it's shared by definition, DoS attacks are thought to be much more damaging in the cloud. In a DoS attack, an attacker attempts to prevent legitimate users from accessing privileged information or services by targeting the computers and the network of the victim or the end points he's trying to use. Typically, the attacker will overload a site's server with requests for access above its capacity. In the Cloud environment, when the operating system notices high workload on the flooded service, it will provide more computational power (virtual machines, service instances) to cope with the additional workload. Thus, rendering the hardware workload process do ineffective. In reality the cloud is enabling the attacker with computational power, from a single flooding attack entry point, to perform a loss of availability on the intended service [9], or to reach a complicated, resourcefully demanding premeditated goal. In a distributed denial of service attack, the attacker uses several host computers to attack another computer or network.

Cloud Malware Injection Attack: In a malware injection attack, a malicious attacker attempts to inject malicious services or virtual machines into the cloud, which appears to be a valid instance service executed in the cloud and be treated as such. If successful, the cloud service will be exposed to spying activity and blockings. This can be accomplished by subtle data modifications, which forces a lawful user to wait until the completion of a malicious service which he wasn't responsible for generating. The attacker usually starts by creating his own malicious service implementation module in a way that it will run in Iaas, PaaS or SaaS of the cloud servers. This type of attack is also known as a meta-data spoofing attack. A hopeful countermeasure approach is to perform a service instance integrity check prior to usage for incoming requests. The main idea of this attack is that a manipulated copy of a victim's service instance is uploaded to be subsequently processed within that malicious instance. In terms of classification, this attack is the major representative of exploiting the service-to-cloud attack surface [10].

Cross-VM Side Channel Attack: a Side Channel attack involves a compromise to the cloud by placing a malicious virtual machine (VM) in close proximity to a target cloud server. Recently, a group of researchers has developed a side-channel attack targeting VMs that could pose a threat to cloud computing environments [11]. The attack allows a malicious virtual machine to extract a private ElGamal decryption key from a co-resident virtual machine [11]. This elaborate attack, able to extract a complete cryptographic key, is said to be the first solid confirmation of a long hypothesized attack vector concluding that highly sensitive workloads should not be placed in a public cloud. What makes this attack stand out is that the adversary doesn't need to compromise his VM (or any software) to mount the attack; the hardest part is getting the malicious VM to sit on the same host as the victim.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Authentication Attack: Authentication is considered a weak point in virtualization technology and is frequently targeted; especially the mechanisms used to secure the process of authentication [12]. Currently, regarding the service, only IaaS is offering information protection and data encryption based on what a person knows, has, or is. Most user-visible services today still use simple username and password type of knowledge-based authentication, with the exception of certain financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc).

Man-In-The-Middle Cryptographic Attacks: this attack is one in which the attacker places himself between two users and intercepts messages and then retransmits them, substituting the public key, so that the two users still appear to be communicating with each other. The intruder usually uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to acquire access to the message, or enable the attacker to modify the message before retransmitting it.

4. CLOUD DEFENSE OVERVIEW

As it's well known, a threat is blocked by control of vulnerability, in this section we'll provide an overview of some common strategies to secure the cloud environment from different vulnerabilities that were mentioned earlier.

4.1 Strategies

In this section, we're going to study two practical types of defence strategies in the cloud that we deem to be notable. They form a set of best practice approaches that rely on intelligent applications of existing techniques and technologies.

- *Defense in-depth*: this strategy is based on the idea that individual security controls are typically incomplete or otherwise not sufficient, and that multiple reinforcing mechanisms or controls will compose a more complete and robust security solution [16]. The strategy basically consists of exploiting several techniques (a layered approach) to reduce the risk when particular component security is compromised or faulty. For example, a sandbox mechanism adds a layer of security between the applications running within a guest virtual machine and the hypervisor. The use of encryption for VM network traffic can result in effective network isolation between adjacent VMs that reside on a shared physical machine, which ensures security.

- *Honey Pot*: the idea behind a honey pot is to setup a "decoy" system that appears to have several vulnerabilities for easy access to its resources. The decoy system should be set up in a similar manner to those of the production servers in the corporation and should be loaded with numerous fake files, directories, and other information that may look real. By making the honey pot appear to be legitimate, it leads the hacker to believe that they have gained access to important information. The intruder may stay around in an attempt to collect data while the honey pot collects information about the intruder and the source of the attack. The idea is not to capture the bad guy but to monitor and learn from their moves, find how they monitor and exploit the system, figure out how those exploitations can be prevented in legitimate systems and doing this without detection from the hacker [14].

Honey pot can be used by cloud service providers, one Honey pot VM for each hardware server, which can serve as a form of intrusion detection at the hypervisor [13].

4.2 Countermeasures

DoS and DDoS are known to exhaust as much as all network resources when at full strength, but still, we expect that extensive and cautious monitoring of both network and available resources with anticipatory measures can significantly give us a step ahead to control this type of attacks.

As a strategy taken for data storage security, organizations might require that all information stored in the cloud be encrypted because of the insufficient trust in the implemented cloud security, or they may require encrypting only some of the information in the cloud; accepting additional risk but limiting the risk of not storing all information in an unencrypted form [17]. It is also suggested to use homomorphic token with distributed verification of data security and locating the server being attacked [18].

For Trust model for interoperability and security in cross cloud, it is suggested to separate domains for providers and users, each with a special trust agent, apply different trust strategies for service providers and customers and to take time and transaction factors into account for trust assignment. [19]

Secure virtualization can be considered as a backbone to cloud security, it is suggested to implement an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

machines and monitor the behavior of cloud components by logging and periodic checking of executable system files. [20]

5. CONCLUSION

Cloud computing is constantly evolving; which means that as the technology matures, new types of security issues will arise, while some will disappear into the background. From a security point of view, cloud computing contains numerous vulnerabilities, threats and risks. In this work, using precise definitions, we have successfully identified and distinguished between traditional and cloud related security issues, gaining a generally clearer picture of cloud computing concerns that we found to be missing looking in the security discourse in the cloud. This paper presents an overview of the main attack vectors and defense strategies / countermeasures that need to be applied in order to reach a secure cloud objective.

It is our understanding that the main principle for a standard security model to be deployed in the cloud is to communicate with any type of cloud environment, deal with either predefined or customized security policies and to be implemented in all levels. We are in the process of developing a framework model that should subsequently be implemented in the cloud, dedicating a large effort to the virtualization security aspect. We hope this work can be a catalyst to an informed, continued research of interest to the cloud.

REFRENCES:

[1] Gartner, Assessing the Security Risks of Cloud Computing - Enterprise Cloud, 2008.

[2] The Open Group, “Risk taxonomy”, 2009.

[3] National Institute of Standards and Technology, Information Technology Laboratory, “The NIST Definition of Cloud Computing”, 2009.

[4] Cloud Security Alliance, Top Threats Working Group, “The notorious nine: cloud computing top threats in 2013”. February 2013.

[5] Winkler, “Securing the Cloud – Cloud computer security techniques and tactics”, chapter 1 – Introduction to cloud computing and security, Elsevier, 2011.

[6] The Open Web Application Security Project, “Category OWASP cloud - 10 project”, 2012: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

[7] ISO 27005, Information technology - Security techniques, “Information security risk management guideline”, 2011.

[8] Tiantian Qi. “An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering”. IEEE Intelligence and Security Informatics, pp. 152-159, New Brunswick, USA, May 2007.

[9] M. H. Sqalli, F. Al-Haidari, K. Salah “EDoS-shield- a two- steps mitigation technique against EDoS attacks in cloud computing”, 4th IEEE International Conference on Utility and Cloud Computing, 2011.

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On technical security issues in cloud computing”, in Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II), 2009.

[11] Y. Zhang, M. K. Reiter, T. Ristenpart, A. Juels, "Cross-VM side channels and their use to extract private keys", 2012.

[12] B.Meena, K. A. Challa “Cloud computing security issues with possible solutions”, 2012.

[13] CHAPTER 4 Securing the Cloud: Architecture

[14] SANS Institute, Global Information Assurance Certification Paper, “Honey pots and Intrusion Detection”, 2002

[15] N. Ben Bouazza, M. Lemoudden, B. El Ouahidi, D. Bourget, “UML syslog extension for cloud logs,” In press, 2013.

[16] National Security Agency (NSA), Defense in depth, A practical strategy for achieving Information Assurance in today’s highly networked environments, 20 Marsh 2013.

[17] NIST Special Publication 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations; 2012.

[18] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing,” 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

[19] S. Pal, S. Khatua, N. Chaki, S. Sanyal, “A new trusted and collaborative agent based approach for ensuring cloud security,” Hunedoara International Journal of Engineering (Archived copy), 2012. ISSN: 1584-2665.

[20] W. Jansen, T. Grance, “NIST Guidelines on Security and Privacy in Public Cloud Computing,” Draft Special Publication 800-144, 2011.