Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Security Assessment for Cloud Applications

Stefano M P C Souza, Ricardo S Puttini
Universidade de Brasília
Brasília, Brazil

***Abstract*—This work presents a comprehensive view of technologies and techniques presented in recent literature in response to specific security issues in each service layer of a common cloud computing deployment architecture. First, we present the common cloud architecture, with the typical service layers and a list of threats and concerns resulting from that architecture. Then, we propose a simple and straightforward procedure for assessing risks and selecting the adequate mitigation mechanisms for such risks. We also list some of the most important standards and technologies for cloud security.**

Keywords—Cloud Computing; Security; Risk Assessment; Standards

I. INTRODUCTION

Cloud computing is a business model by which pooled computational resources are provisioned, on demand and with rapid elasticity, through a broadband network, in the form of a metered service [1]. The main economic appeal of this new service paradigm is that consumers are able to turn capital into operational costs, pushing concerns with ownership and maintenance of the underlying infrastructure supporting their computer and communication systems to the service provider [2].

In this market, different actors have different and specific economic interests, which result in specific security needs. Security in any business is the overall effort to ensure continuity, protecting values (e.g. facilities, products, services, knowledge, and public image) by identifying, assessing and mitigating all risks of loss or disruption [3]. Thus, security in cloud computing, in a broader sense, can be seen as a series of functional requirements that need to be implemented at every layer of technology and for every usage, maintenance or auditing interaction (e.g. interfaces, APIs, processes, configuration) simply that every actor may continue to efficiently perform his role in the market [4].

Cloud services providers basically need to be able to bill the use of their resources and services. For that same purpose, they need a trusted and stable service that consumers would be willing to pay for. CSPs need to keep compliance to a series of auditing and certification standards, as they are subject to legal and regulatory constraints on the territories where they operate. Security and assurance of business continuity are the main aspects of most of those standards.

Consumers, on the other hand, need to keep governance over their assets and values, despite of the technological apparatus supporting their operation. They depend on the CSP's ability to deliver the promised services at the agreed levels. Since they consume cloud services though the Internet, they also need to be assured that no unavailability on the network carrier (or internet service provider) will affect their businesses. Notwithstanding the fact that they share control over their systems with the CSPs, cloud consumers are ultimately held responsible for the protection of their end-user's personal, private and personally identifiable data.

Governments carry out macroeconomic stabilization and resource allocation adjustment functions. They need to promote markets' growth, safety and stability, in order to foster economic development and social welfare. Also, they are huge consumers of computational resources and holders of the most sensitive data concerning individuals, enterprises and matters of national security. Therefore, they need sound and well tested security technologies and procedures that enable the existence of dependable players in the market, so that they can consume cloud services themselves.

Cloud brokers may combine services from different cloud providers or simply add value to the services of a single provider. In both cases, compliance to Service Levels Agreements (SLA), as well as security procedures and standards are an essential part of the brokers' core business. Auditors, in turn, derive their entire participation in this market from standards and certifications applicable to cloud services and agents.

Security for such a broad market is not achieved with the mere aggregation of mechanisms. There are no physical perimeters or network zones that would allow the idea of a single security layer, or checkpoint. Cloud actors face a complex environment, with software components, storage and database services each running on different virtual machines, in different servers, different data centers, sometimes even in different countries.

Therefore, security must be comprehensively examined from each stakeholder's point of view. Each actor needs to build a solid understanding of the relationship between assets, threats, and likelihood (or frequency) of attacks. And, then, respond appropriately, mitigating any relevant risks [3].

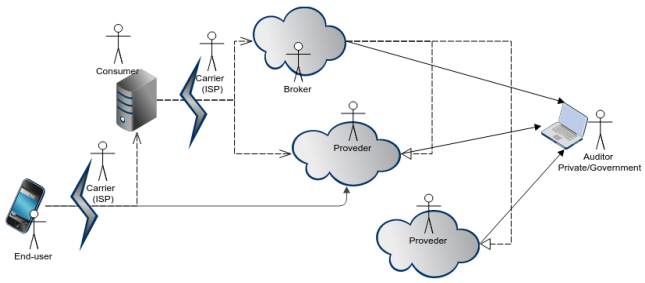

Fig. 1. Cloud actors

Most texts in the area are focused in specific attacks against consumers, especially those related to data breaches. There are several attacks against cryptographic primitives that use information leaked by the underpinning software and hardware stack to break the confidentiality of information stored or processed on the cloud (e.g. timing attacks and memory padding attacks) [5, 6].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Proposed solutions range from techniques aimed at improving a provider's ability to protect its infrastructure from external attackers and from malicious tenants, to solutions focused on the end-user, such as universal client-side encryption [7]. This last kind of solution is usually based on the assumption that the cloud environment will always be untrusted, so the consumer or even the end-users must encrypt data prior to sending to the cloud in order to assured data access control policies are enforced.

The important observation here is that each stakeholder, with corresponding needs, must be taken into consideration. There will be significant trade-offs between security needs and other business requirements, markedly concerning the costs of implementing the appropriate security measures. There will also be trade-offs between the security needs of one stakeholder and businesses conditions of other agents in the market. For example, a secure administration interface, with very limited or restricted features, certainly improves security form the CSPs perspective. But it also lowers the flexibility and quality of the service when considering the consumers perspective.

Therefore, we argue that each stakeholder, especially the consumer, should perform a security assessment of their assets on the cloud and take the appropriate measures, according with their level of control over the operation of the cloud service. We present a general procedure for security assessment that can be used by any actors is the cloud market.

The following section introduces a simple cloud anatomy, with the most distinguishing characteristics of cloud environments. In the third section, we present the main security concerns that affect cloud consumers. It includes a list of the top threats to cloud resources, as well as discussion on how security issues effectively alter the economics of cloud computing. The fourth presents the risk assessment procedures, with a list of some of the standards that are commonly used by cloud service providers (CSPs), cloud developers and other stakeholders.

II. A Typical Cloud

To understand the various types of assets that can be hosted in the cloud and the different vulnerabilities and attacks to which they are subject, it is necessary to know the most common service models. It is necessary to understand how each stakeholder, including end-users and external agents can interact with the elements of each service model. The forms of interaction and their control levels determine the degree of participation of the various actors in the security their assets in the cloud.

Figure 2 shows, concisely, what would be the typical architecture of a cloud, pointing out its essential characteristics, as well as the most common service layers. At the top, the deployment models: public, community, hybrid and private. In the bottom frame immediately, the service features that define cloud computing: large stock of computer resources; served on demand; with rapid elasticity; in the form of a metered service; through a broad band network.

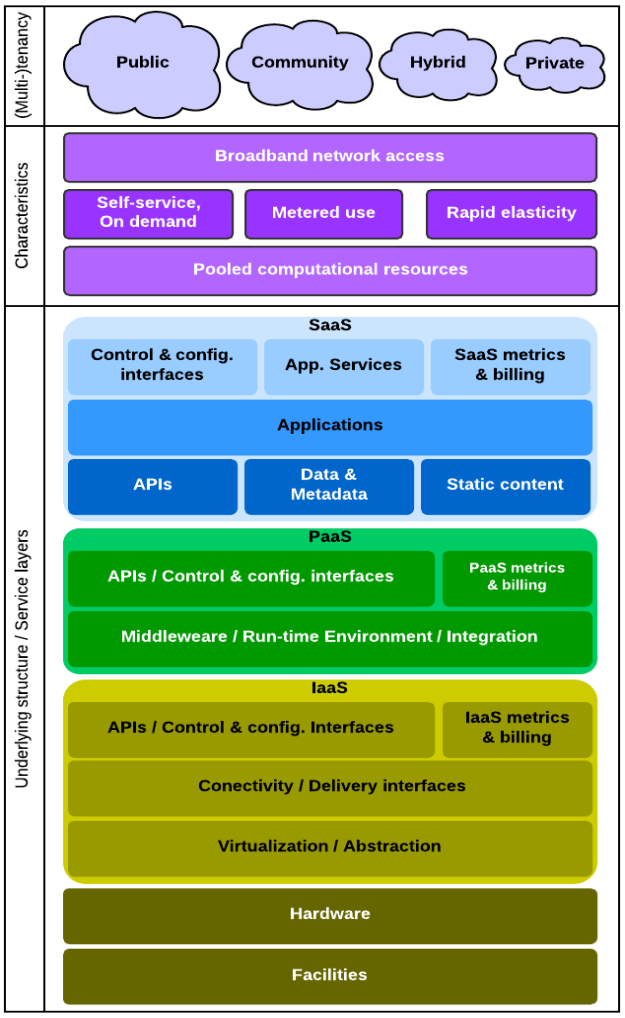

Fig. 2. A typical cloud architecture

At the top, we find the deployment or tenancy models: in public clouds, an organization offers computational capacity on the open market. In community clouds, a group of organizations share the costs and administration, and consume the resources in the form of metered services. Private clouds are run by very large organizations, which supply their subsidiaries with computing power. Hybrid deployments are any combinations of such models [8].

In the lower box of Figure 1, we see the common layers of the underlying infrastructure supporting cloud services. The services offered in lower layer are commonly classified as Infrastructure-as-a-Service (IaaS) and generally represent the most basic resources, direct representations of physical devices, such as processing time, disk space and network traffic. These products are managed using a specific interface created by the provider. This interface should offer features such as creation, destruction, ligament, shutdown, copy and configuration of virtual machines.

In the top layer, finally, we see services with the highest level of complexity, classified as Software-as-a-Service (SaaS). In this service model, the consumer interacts directly with applications developed by the CSP, paying for specific features and usage limits.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

This stack of cloud services shows that the greater the complexity of services, the lower the level of control is left to the consumer. When pushing costs and other business concerns over its operations to the CSP, the consumer also relinquishes control over the security. This does not mean the consumer will be more exposed, since the provider will probably have greater investment capacity and highly trained personnel. The CSP has greater chances of understanding and responding appropriately to the various threats.

III. TOP THREATS

Since 2010, the Cloud Security Alliance's Top Threats Working Group (TTWG) keeps track of the threats, both perceived and reported, that have greater impact on the cloud computing market. These threats alter the landscape in many ways, adding costs and complexity and even preventing enterprises and individuals from entering the market as consumers or providers [9].

A. *The Treacherous 12*

The latest report from the TTWG, entitled "The Treacherous 12", was published in early 2016 and highlights the following threats:

1) Data Breaches: Data leakage by accidental or unauthorized access, or any other way, is the main concern and also the most common security breach on cloud services. It has been the main point of tension for most CIO's and decision making bodies when deciding whether or not move for cloud solutions.

2) Weak Identity, Credential and Access Management: Weak passwords, the repeated use of the same password along different web applications, the lack of use stronger authentication protocols, all of these make it very difficult for cloud consumers and providers to effectively enforce access control to resources in the cloud.

3) Insecure APIs: Especially in configuration, provisioning, orchestration and monitoring interfaces. Some SDK's and API's offer too much power over the consumer's account (as to scaling out or in, creating or disposing of instances, etc.) but have not been built with security as a main architectural aspect. Consumers must be especially aware of such risks when using some dynamic programming languages - such as PHP and JavaScript (ECMAScript) – that have a history of serious security issues.

4) System and Applications Vulnerabilities: Both providers and consumers (especially in IaaS models) may be responsible for unpatched or poorly managed software with bugs and vulnerabilities that attackers can use to affect the system or the service operation, steal information or even take control of the system.

5) Account Hijacking: Web based administrative interfaces are prone to suffer XSS, CSRF and XML signature wrapping attacks. Many attacks on Amazon AWS administration console were reported, both on the HTML and the web services versions, amounting to several hijacked accounts. There is one extreme case where information posted by the consumer on a support forum was enough for an successful attack [10].

6) Malicious Insiders: Researchers at Carnegie Mellon University have built up a good definition of this threat: "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems". [11]

7) Advanced Persistent Threats: These refer to attacks with a large time span. The attacker infiltrates the system compromising one device and gathers information on network topology and other aspects of the system before striking his target. The best mitigation efforts against these 'stealthy' attacks are a serious culture on security and user engagement. Users must be aware of 'social engineering', Trojan horses and other common attacks.

8) Data Loss: While storage costs may have lowered at a polynomial rate, transfer tariffs only shrunk at a linear rate in past decades. This means that the consumer is dependent on an effective governance and SLA compliance by the provider to ensure the safety of the data on the cloud, as the costs of a backup policy - transferring huge amounts of data out of the providers cloud - are usually not feasible.

9) Insufficient Due Diligence: Consumers trying to push management costs to the provider do not always fulfill their part in preparation for incident response, encryption and other measures that they would normally take when managing on premise resources. A known example of insufficient attention to the security are the too wide and too weak configuration usually assigned to security groups in AWS EC2 instances [10].

10) Abuse and Nefarious use of Cloud Services: Spammers may cause blacklisting of an entire range of IPs, affecting other tenants. Also, an attacker can use a massive amount of resources in a cloud to quickly carry out DDoS attacks or crack encryption keys

11) Denial of Service: DoS and DDoS attacks are most likely used to prevent the consumer from reaching his resources at the provider's network. Even though a CSP's infrastructure may not go down so easily, some DoS attacks can also take advantage of poorly configured HTTP servers, databases and other web application components on the consumers VMs to bring down an entire service layer with a very small payload.

12) Shared Technology Issues: Using a more complex technique, an attacker may use side channel timing information to extract private keys been used in other VMs on the same server. Also, bugs in large-scale shared software platform are very difficult to identify and correct. An error in software may affect the availability of a CSP's services for hours, even days.

B. *Economic impact of cloud (in)security*

Along with these threats there are other concerns, maybe on a less technical point of view, that bring significant impact on the overall efficiency of the cloud market. Daryl Plummer, Gartner's vice president, points out some problems that CEO's face on their attempt to use cloud services [2]:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

1) Lack of a mature certification and audition system – The use of established audition and certification standards designed for on premise solutions may not tackle the main and most important aspects of security in the cloud;

2) Specific insurance contracts, practices and processes are yet to be developed – Economic agents are more exposed to moral hazard and other asymmetry of information negative externalities. Therefore, insuring solutions dependent on cloud computing services can be prohibitively expensive;

3) The desired level of transparency is not clear – On the one hand, consumers desire a transparent description of service and a clear SLA from the provider, in order to fully understand all the risks taken. On the other hand, avoiding the hassle of specifying and dealing with the details of the implementation of IT solutions is one of the top advantages of cloud computing, and the essential element of its economic appeal.

IV. A Security Assessment procedure

As previously discussed, there is no simple way to approach security in cloud environments. It becomes even harder when dealing with applications that suffer specific and strict legal restrictions: such as health information and financial or tax reporting.

A. The general procedure

Nonetheless, we can present the following steps as the minimum practical measures for the security of assets in the cloud computing environment:

1) Inventory: The organization needs a list of assets that are generated, processed, stored or simply transported by the cloud;

2) Analysis: For each asset, or each kind of asset, there must be a list of all vulnerabilities and correlated attacks. That is an understanding of all the characteristics of the asset or the technology used to access and manipulate the asset, that can be used by a third party to gain unauthorized access, or cause disruption and losses.

3) Classification: The next step is to classify the attacks by likelihood of occurrence and economic impact. This likelihood can be measured in terms of number of vulnerabilities it exploits, the complexity and cost of implementing the attack and the probable economic outcome for the attacker.

4) Mitigation: Risk mitigation should start by addressing the vulnerabilities that give way for the attacks classified in the higher impact and likelihood groups.

B. Available standards and mechanisms

The procedure described above can be used before moving to a cloud service, as a step in the design of the cloud application or as a way to assess the security of applications already deployed. One can check the security mechanisms and processes that are in place against the list created while performing the assessment procedure.

Now, rolling out your own security solution may result even more hazardous than doing nothing. Particularly when resorting to cryptographic protocols and primitives, one should be aware that poor implementations completely defeat the purpose of the security mechanism. Those must not be implemented by professionals without sound background in mathematics and extensive programming experience. The most recommended strategy is to use well established and tested libraries, such as OpenSSL and BouncyCastle.

Another difficulty that may arise in this process is that sometimes it easier to spot vulnerabilities then to decide what the most adequate solution is. Consumers may have a hard time determining what kind of security measures to look for in order to manage the security of its applications. We have listed a few standards and technologies that may be used to respond to most of the threats in cloud environments.

Table I displays general purpose standards, that can be used to determine whether a cloud provider maintains good management practices and, therefore, could be expected to have a good security policy in place. Note that some of these standards, such as SOC 3 or SSAE 16, were not tailored for the technology market, so they only indirectly indicate the existence of good information security practices.

Table 2 brigs a list of standards that are directly related to security in cloud environments. Cloud consumers are strongly advised to learn the contents of these standards and contract cloud services from providers that are compliant to those standards that better respond to the security requirements of their applications and end-users.

TABLE I. General Purpose Standards

Standards	Purpose
ISO/IEC 27001:2005	Information Security Management Systems
ISO/IEC 19770-1:2012	Software Assets Management
PCI DSS	Certification for credit card information processing systems
HIPAA	Health Insurance Portability and Accountability Act
SSAE 16/ISAE 3204	Auditing/Certification standard for enterprises dealing with financial information. Focuses in privacy and security of information
SAS 70	Auditing standard for data center controls and management
SOC 1	Service Organization Control, auditing reports on the effectiveness of controls over financing reports
SOC 2 & SOC 3	Provide stricter audit requirements then SOC 1, and benchmarks that enable comparisons between audited organizations.

Some consumers may have to look other certifications as well. Organizations deal with credit card payments, for instance, need to find CSPs that are PCI compliant. Those running health information systems will need to hire HIPPA compliant providers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

TABLE II. CLOUD SECURITY STANDARDS

Standard	Purpose
ISO/IEC 17826:2012	Cloud Data Management Interfaces
ISO/IEC 27017	Guidance on information security in cloud computing
ISO/IEC 27018	Control objectives, controls and guidelines for the protection of Personally Identifiable Information in the cloud
PMRM TC	OASIS Privacy Management Reference Model for Cloud Computing
TOSCA TC	OASIS Topology and Orchestration Specification for Cloud Applications

Table 3 displays a number of standards, technologies and commercial products that have become *de facto* standards in specific areas, such as authentication, authorization and identity management, - which are very sensitive for security and privacy.

There are many security technologies fit for the cloud, and even a form of SaaS sometimes called Security-as-a-Service, specialized in security. We can cite services such as AWS CloudHSM, SafeNet, CipherCloud and Gazzang. The consumer must consider all available options and pick those standards and technologies that best fit his assets and business conditions.

TABLE III. SECURITY TECHNOLOGIES

Standards/ Technologies	Purpose
SAML/XACML	Federated authentication information exchange
SCIM	Cross-domain identity management
Oauth, OASIS CloudAuthZ	Authorization protocols
OpenID, Facebook Connect	Federated authentication APIs (or SaaS services)
SRP, WebFinger, OIDC	Authentication protocols
WS-Sec/WS-Fed	Web-services security and federation
RFC 7515, RFC 7516	REST API's security (JSON encryption & signature)
FIPS 140-2	A standard for the accreditation of cryptographic libraries
PKCS Series	Public Key Cryptography Standards
RADIUS	Remote Authentication Dial In User Service

V. CONCLUSION

Cloud computing still has many open security issues and services suffer a great lack of reliability. As CSPs continue to grow and spread their data centers globally, it is becoming increasingly harder for consumers to evaluate the levels of security and what legal accountability CSPs are subject to. Therefore, security assessments must be a continuous activity.

We showed how the regular cloud architecture offers different levels of control and responsibility as one moves from simple to more complex services. And we demonstrated the need for an understanding of how the new control boundaries laid for the assets imply different levels of participation in systems security in the cloud.

Most security expertise and solutions developed for 'on premise' systems are still valid and useful, but should be carefully applied to this new context, taking in account the architectural complexity of the cloud. And this work brought to the reader's attention both general purpose and cloud specific security standards.

Finally, we presented a list of practical recommendations to ensure application security and privacy of end users in the cloud. We believe the procedure presented in this work, together with the guidance of the standards and technologies listed herein, can be of great help to the average cloud consumer when assessing the security of his assets in the cloud.

REFERENCES

[1] P. Mell, and T. Grance, The NIST Definition of Cloud Computing (SP-800-145). Gaithersburg: NIST, 2011.

[2] D. Plummer, The Business Landscape of Cloud Computing. London: Gartner/Finantial Times, 2012.

[3] M. Iorga and A. Karmel, "Managing Risk in a Cloud Ecosystem" in *IEEE Cloud Computing*, vol. 2, no. 6, pp. 51-57, Nov.-Dec. 2015.

[4] Janseen. W, Grance, Timothy, Guidelines on Security and Privacy in Cloud Computing (SP-800-144). Gaithersburg: NIST, 2011.

[5] N. J. Al Fardan and K. G. Paterson, *Lucky Thirteen: Breaking the TLS and DTLS Record Protocols*, in Security and Privacy (SP), 2013 IEEE Symposium on, Berkeley: IEEE, pp. 526-540, 2013.

[6] M.K. Reiter, *Side Channels in Multi-Tenant Environments*, in Proceedings of the 2015 ACM Workshop on Cloud Computing Security Workshop (CCSW '15). New York : ACM, 2015

[7] D.C. Wilson, and G. Ateniese, *"To share or not to share" in client-side encrypted clouds*, in Proceedings of the 17th International Conference on Information Security, Honk Kong (ISC 2014). Elsevier, LNCS, vol. 8783, pp. 401-412, 2014

[8] R.B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, *NIST Cloud Computing Reference Architecture*, in Proceedings of the 2011 IEEE World Congress on Services (SERVICES '11). Washington: IEEE Computer Society, pp. 594-596, 2011.

[9] The Treacherous 12: Cloud Computing Top Threats in 2016. Seattle: Cloud Security Alliance, 2016.

[10] J. Somorovsky, M. Heiderich, M. Jensen, et al, *All your clouds are belong to us: security analysis of cloud management interfaces*, in Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11). New York: ACM, pp. 3-14, 2011.

[11] G. Solowash, Common Sense Guide to Mitigating the insider Threat 4th Ed. Berkeley: CERT, 2012.