Enterprise to Cloud Security Assessment
A Method using OSSTMM 3.0 Concepts

Ronivon Costa[1] and Carlos Serrão[2]
[1]VANTIS, R. Rui Teles Palhinha, 6 - 3ºG, 2740-278, Porto Salvo, Portugal
[2]ISCTE-IUL, Av. das Forças Armadas, 1649-026, Lisboa, Portugal

Keywords: Cloud Security, Security Assessment, OSSTMM 3.

Abstract: Much has been talked about security, and with the wide spread and adoption of Cloud computing, the talk has followed the buzz and put Cloud Security in the spotlights. Security guides for the Cloud has been published, but we understand that is still missing a practical assessment methodology that would allow organizations to quick understand how the security of their assets are impacted when it is farmed out to Public Clouds. Our contribution to address this problem is a method to isolate the organization's assets from the environment it is hosted, and compare metrics from the environment only. This method provides the important benefit of allowing the organization to determine how security will be impacted without having to actually migrate its resources.

1 INTRODUCTION

The difficult in evaluating security of complex systems has been an obstacle in the adoption of Cloud by large organizations, since the security properties of such services is dependent of several factors, most of them out of the customer's control. One valid approach for an enterprise to verify how a Cloud provider would satisfy its own security requirements can be based on actual tests of that Cloud, but considering that every company wanting to adopt services from a specific Cloud provider would have to run its own tests in the process of evaluation, we can foresee a huge expenditure in terms of time and cost during the process just to verify viability. And this expenditure would increase even more if the process had to be performed for different projects in the same enterprise. The US Government has launched the FedRAMP project in 2012 to overcome this issue, and will allow participating agencies to jump in into Amazon Cloud services with its projects without requiring a new evaluation for every project (Reuters, 2013).

Not every Cloud provider will be willing to allow prospectors testing its resources against vulnerabilities, since some types of active tests will trigger security alarms that will be difficult to differentiate from legitimate, actual threats. One way to overcome this difficulty is the Provider itself run the security assessment and to publish the test results available to all prospectors. Using methodic process and well accepted metrics, this assessment can be instrumental in helping a company in the decision of migrating resources to a Cloud. On such method that fulfills this requirement is the Open Source Security Testing Methodology Manual (OSSTMM) and its rav concept (Herzog, 2010).

Using the rav, it is possible to make sense of the actual security of a system related to an optimal state, which can also be compared to other system. In other terms, one can verify the security of the enterprise systems when all resources are hosted in the internal network, and then compare with the security of the same enterprise with some of its resources in a Cloud. Although the systems are different, the rav will provide a metric that can be related in these very different situations.

In this paper, we explore this characteristic of the OSSTMM methodology and propose an even more direct approach to verify how security is affected when the Cloud is a variable to take into consideration.

2 PROBLEM

The decision to adopt the Cloud must consider

Costa R. and Serrão C. (2013).
Enterprise to Cloud Security Assessment - A Method using OSSTMM 3.0 Concepts.
In *Proceedings of the International Conference on Knowledge Discovery and Information Retrieval and the International Conference on Knowledge Management and Information Sharing*, pages 571-578
DOI: 10.5220/0004666005710578

several factors besides the financial direct benefits. Cloud adoption can have different effects in the global security of an enterprise network, and some of these changes will happen due to the movement of assets from one site to another and a corresponding risk transfer (ENISA, 2009).

The above concept can be generally expressed by the following metaphor: There are three safes, each one protecting valuable assets: Gold, Silver and Bronze. There is not enough space in the owner's own property to store all three safes, so the owner will have to rent space somewhere to store one of them. The decision about which safe will be stored in the rented space must be based on:

a) the importance of the safe contents (assets);

b) how well protected the safe is now;

c) how well protected will it be in the new place.

The knowledge of a safe existence and place of storage is a risk factor, and therefore should be avoided. For example, if it is brought to a thief knowledge about the existence of a safe full of valuable assets made of bronze stored in a given place, all of the other two safes will also be at risk of being stolen since it is all stored in the same physical location. If the safe with bronze assets is stored in a different location, and someone tries to steal its contents, the other two safes will not be at risk.

The metaphor presented illustrates three characteristics of the concept used in this work which are:

- Risk transfer;
- Improved security by limiting the number of visible targets;
- Influence of the surrounding environment over the asset's security.

The schematics in figure 1 illustrates some possible attack vectors to four targets in a (simplified view) of a network (left). If the attacker succeeds using any of the vectors, the compromised internal target can be used to attack more important targets in the same network (in the right diagram).

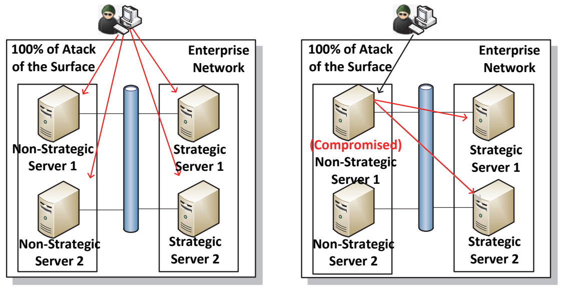

Figure 1: Global attack surface.

Moving some targets to a separate environment will have two effects, which is the change in the exposure level of the moving targets, and the change in the exposure level of the remaining targets. This change can be for good or for bad, and it will depend on the targets moved, its importance, and how it interacts with other enterprise components.

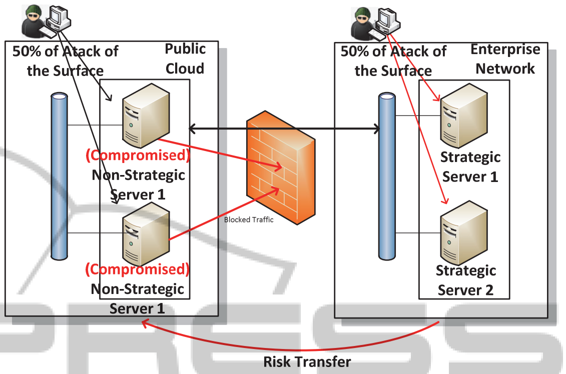
50% of Atack of the Surface
Public Cloud
(Compromised) Non-Strategic Server 1
(Compromised) Non-Strategic Server 1
Blocked Traffic
50% of Atack of the Surface
Enterprise Network
Strategic Server 1
Strategic Server 2
Risk Transfer

Figure 2: Split attack surface.

Every component in a given scope will contribute to the overall security property of that environment (Yildiz et al, 2009), and that is the reason why every target must be included in a security assessment. However, the surrounding environment will have an even stronger influence. Verifying the security of the surrounding environment using OSSTMM methodology concepts will allow the comparison of security in absolute values for both environments by using a metric called *rav* (Herzog, 2010).

3 RELATED WORK

There are several evaluation, risk and assessment methodologies available, as well as guidance to improve systems security including the cloud (CSA, NIST, OWASP and etc.). While a few published guidelines has targeted the Cloud (CSA, 2009)(US CIO, 2010), most of them are a general framework or methodology designed as a checklist or a process to run networking and systems testing.

The process of evaluating Cloud adoption involves more variables than the security properties of the systems and environment. We start from the point where all administrative and political decisions has already been dismissed as not blocking for the cloud adoption, and so comes the time to define which resources are more appropriate to move. The technical decisions about what can be moved out can be evaluated against security metrics previously obtained from tests performed on predefined models. The specifics of the tests will not be covered, however, some guidelines should be followed to assure that Cloud specific issues are addressed, such as what to what to test, the approach, and how to evaluate the results.

OWASP (2012) has started a new chapter denominated "Cloud-10 Project" to approach Cloud security risks. OWASP top ten lists are important because it helps the enterprises to focus on the most serious threats to web applications, and the Cloud-10 projects is a work in project (Pre-Alpha) to address this new paradigm in enterprise computing. OWASP top ten lists are maintained by a community of users and experts in every domain, and are ranked by criteria such as (OWASP, 2012):

- Easily Executable
- Most Damaging
- Incidence Frequency (Known)

The OWASP Cloud-10 project defines the criteria that can guide the security tests, but an appropriate testing methodology is required. The Open Source Security Testing Methodology or OSSTMM has its focus on operational effectiveness, that is, how it works (Herzog, 2011). OSSTMM3 is an evolution from a penetration testing methodology which evolved to more than a best practices framework by 2005 (Herzog, 2010) and finally into a more contemporary security assessment methodology that prioritizes tests (avoiding guesses), concentrates on the interactions and its required protections, and balance between security and operations (Herzog, 2011).

OSSTMM has redirected its focus in the earlier releases from testing physical resources such as firewalls and routers to verifying operational security and its related channels, such as Human, Physical, Wireless, Telecommunications, and Data Networks (Herzog, 2010) in the latest versions of the methodology. OSSTMM also introduces its own measurement metrics called ravs, which provides graphical representation of system's states and system state changes over time, and are suitable to be used in operational monitoring consoles.

The Cloud Security Alliance (CSA) is a non-profit organization engaged in providing security awareness and tools to adopters. CSA has a specific publication providing guidance to Cloud security, "Security Guidance for Critical Areas of Focus in Cloud Computing" (CSA, 2009), which is structured around thirteen domains covering several aspects of Cloud security, including Identity and Access Management. CSA has also started the "Consensus Assessments Initiative" to provide means of documenting existing controls for Cloud services, This initiative is based on a questionnaire available at CSA web site, which can be downloaded, have the questions answered and then submitted to the repository of respondents where it can be consulted by customers.

Guidance is also provided by the US Government, and targeted to U.S. Federal Agencies but publicly available. The "Proposed Security Assessment and Authorization for U.S. Government Cloud Computing" has a strong focus on authorization, defines a baseline of security controls and a monitoring process, and also proposes a framework to assess cloud security during vetting of Cloud Service Providers (U.S CIO, 2010).

4 BACKGROUND CONCEPTS

The Figure 3 presents our base line model. Everything inside the enterprise can be seen as a controlled environment, while everything in the outside is beyond its control (Grobauer et al, 2011) (Hiroyuki et al, 2011), and therefore, must not be trusted. That is not to say that an intranet is a safe place to run business without protection, which it is not. According to the "2011 Cyber Security Watch Survey - How Bad Is the Insider Threat?" (CERT 2011) carried out by the Carnegie Mellon University over a population of 607 companies, 27% of all security incidents were caused by insiders in 2010, at the same time that 46% of all respondents affirm that the internal incidents had caused more damage than the outside attacks.

In the Figure 4 we have extended some services from the internal enterprise network to a Public Cloud, while in Figure 5 it was extended further to provide employee's access to the organization's resources in the Cloud.

Almost any enterprise application can be configured to work in a Public Cloud. However, two important factors must be considered:

- The Cloud is not under the Enterprise's control - therefore, it can be considered an uncontrolled environment (Hiroyuki et al, 2011).
- To work with the applications in the Public Cloud, it is necessary to cross a potential insecure channel: the Internet.

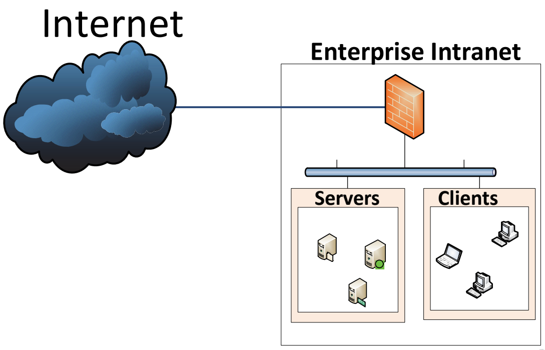

Figure 3: Base line.

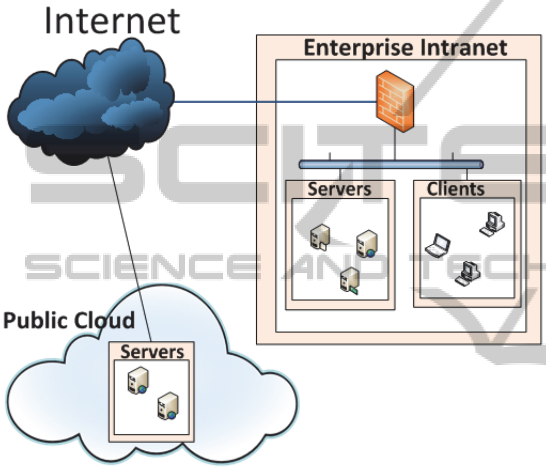

Figure 4: Enterprise to Cloud Use Case 1.

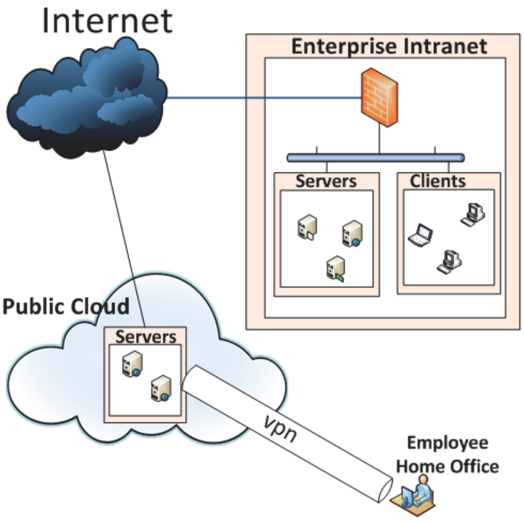

Figure 5: Enterprise to Cloud Use Case 2.

The subtle change in the level of trust in the surrounding environment is more than enough to make it unviable to apply an unprotected authentication protocol for services in a Public Cloud, so there must be a VPN connecting both separate environments. The risk of exchanging private, important data over the internet in the scenario above is a showstopper for most of the companies. The communication between the clients on the company's Intranet and the server in the Public Cloud can be intercepted in a number of ways, including by the man-in-the-middle attack and the eavesdropping technique, to intercept and decode authentication information and application data.

Several factors that must be considered to choose the resources to be migrated to the Cloud and not all of them are related with security, such as the following provided by (Krutz and Vines, 2010):

- The criticality level of the application
- The sensitivity of the data
- Functionality over VPNs
- Performance
- Cost to move to another provider
- Bandwidth utilization

Since there is not a specific methodology or framework to assess Cloud security, we have chosen a generic, more contemporary methodology, OSSTMM, as a basis for our security assessment. The OSSTMM proposes a methodology to verify and test the Operational Security (OpSec) of systems (Herzog, 2010).

Assessing Cloud security is not a trivial activity, For the Cloud, some parts of the OpSec procedures such as physical security and the internal operational processes can only be assumed to be compliant with the enterprise's policies by means of terms of contracts and SLAs (Hiroyuki et al, 2011) from the perspective of the customer. Other technical security properties can be tested, but the lack of Cloud specific metrics (Grobauer et al, 2011) implies that we have to propose a method to quantify security for these use cases, which we do by using the rav concept, from the OSSTMM (Herzog, 2010).

A security assessment following the OSSTMM will result in a numeric value representing the level of security of the assessed system – the *rav*. When there are several targets in the scope for a security assessment, the values obtained for all individual targets can be combined to produce a final *rav*, representing the actual security for the whole system. The *rav* calculation can be simplified as (Herzog, 2010):

$$\text{Rav} = \text{Controls} - (\text{Porosity} + \text{Limitations})$$

Where:

- Porosity: The number of visible holes in the scope, which means that only what can be detected during the tests is accounted for the rav.

- Controls: The controls in place to protect the targets.
- Limitations: also known as "vulnerabilities", are derived from the porosity and the controls. The higher the porosity, higher will be the limitations. The less controls found, the higher will be the limitations.

The porosity can be determined by a set of security tests in the system, which may be comprised of several individual components. In a security test, every component in the system will be a target. There are several tools available to test systems from several attack vectors and documented in several literatures as for example by (Wilhem, 2010) and (McClure at al, 1999). To assess the models in this work, we have used the OpenVAS, an open source security vulnerability scanner software.

The OSSTMM is not a methodology to test Cloud specifically, but a generic methodology to test many types of IT and non IT systems. The difficulty to standardize Cloud security assessment and evaluations is already subject of concerns in the professional sector (Grobauer et al, 2011). Several organizations have been making different contributions, and using different approaches (NIST 2011)(CSA 2009)(OWASP 2012)(USCIO 2010).

In this paper, this difficulty is recognized, but it is out of scope to develop a specific Cloud security assessment framework of methodology to evaluate the results of our study. Instead, the security assessment was based on the shortcut proposed in the OSSTMM methodology, which consist of taking into consideration only the Porosity and Limitations found, assigning default controls for discovered services and accepting an uncertain but perhaps small error margin (Herzog, 2010).

Using the *rav* metric proposed in the OSSTMM will make it possible to find a security value for the baseline relative to the scope, and later compare with the values obtained from the assessment of the Cloud model. This comparison between different systems is supported by the methodology by using the concept of "Actual Security", which gives the actual security of any system in terms of rav (that can also be seen as a percentage). Using the rav, we can compare the security of two different systems and actually understand from each one, how much it is prepared for the threats against its attack surface (Herzog, 2010).

In order to focus on specific Cloud security issues, it was used the concepts presented by (Grobauer et al, 2011), who proposes that vulnerabilities are Cloud specific when it:

- is intrinsic to or prevalent in a core cloud computing technology,
- has its root cause in one of NIST's essential cloud characteristics,
- is caused when cloud innovations make tried-and-tested security controls difficult or impossible to implement, or
- is prevalent in established state-of-the-art cloud offerings.

From the above Cloud specific vulnerabilities, we defined a testing process to include:

- Assessment of the Cloud Web Management interface (dashboard);
- Assessment for systems from inside the Cloud;
- Assessment from the system from inside the Cloud using a separate, hostile Tenant;
- Testing all know targets for open TCP/UDP ports;
- Testing of all knows targets for known Common Vulnerabilities and Exposures (cve.mitre.org);

5 THE METHOD

The method proposed in this paper follows the OSSTMM for assessing security, but the main contribution from that methodology is the metric called rav. But instead of using the raw value of the rav that is obtained from the security assessments, we propose using a delta obtained from the comparison with a base line model. Using the actual values calculated for every model will give a perception of the security for that specific scenario, when composed by those specific assets with that specific configuration. On the other hand, using a delta will make it possible to have an exact perception of the difference of security derived from that environment's influence. The method used in this work will result in a percentage value, which will be the final metric to ultimately take the conclusions about how security is affected after migrating services to the Cloud. This percentage can therefore, be applied by different enterprises, or by the same enterprises in different projects when evaluating viability of moving resources to that Cloud. The metric is valid only for that Cloud, but different assessments can be performed for other Cloud infrastructures for comparison.

A security assessment using this methodology should always begin by defining a base line model that will be used as a reference for later comparison with other models. For a corporate scenario, the base line should always be the actual organization private network.

The steps to apply the methodology are:

1. Identify political and administrative issues. Any identified blocking issue should stop the process and no further (operational) tests have to be done. The resource should not be migrated to the Cloud;
2. Define a security test guideline that can be applied to both the enterprise and to the Cloud. This test must include:
   - Scope for the enterprise tests. Must include an external security test (from the Internet). The internal test must be also part of the scope, although it may be defined around only those components that interact with the relevant targets.
   - Scope for the Cloud tests. Must include an external security test (from the Internet) and one test from inside the Cloud from a separate (hostile) tenant. A test from inside the tenant itself is optional, and depends on if the systems in the Cloud will have users other than the administrators.
   - Tools to use, including operating system and version where the tools will run, testing tools including version and knowledge base information;
3. Perform the Cloud security test – or request the security assessment report from the Cloud provider; the report must contain metrics according to the OSSTMM, and provide a final Actual Security value.
4. Perform the Enterprise security test and generate a report;

It is recommended to use the rav spreadsheet calculator: (http://www.isecom.org/research/ravs.html). In this method, the spreadsheet should be filled with the values obtained in the security tests, but the controls should have assigned default values taken from the field “Total” in the “Porosity” (visibility + access + trust).

The results can be analyzed in two ways:

a) Compare the Actual Security for the two tests;
b) Calculate the percentage variation for the Actual Security between the Enterprise security assessment and the Cloud security assessment.

The method in “a” is perfectly allowed by the OSSTMM methodology and give non related metrics (Herzog, 2010) which can be used to have an overall perception of the security provided by the system.

The method in “b” provides a better perception of the “gain” or “loss” when comparing two systems. This method is our proposed methodology to evaluate the security impact of migrating resources to a Cloud when we have a previous reference. Both methods provide valuable decision information, but the method in “b” will provide a better understanding of how much security will influence future use cases.

6 CASE STUDY

This case study was developed for an MSc thesis, where the authors have setup labs to apply the method described in this paper. The base line model in figure 3 was composed of one Windows Domain Controller, one internal Windows Web server, one Windows user workstation, one Linux box configured as both a default router and VPN for the entire network, and another Linux box running the public Internet Web Portal. The Internet Web Portal provided an internet presence as found in most enterprises, while the internal Web server is for private, internal use only by the enterprise’s employees.

Regarding the physical architecture of the Use Cases, the Base Line model was fully implemented in a VirtualBox virtualization environment, while the Enterprise to Cloud Use Cases were implemented using also an OpenStack IaaS Cloud. The Cloud was implemented in a single box, and made accessible from the Internet to allow the management of the services as required by a Public Cloud.

In figure 4 and figure 5, the Internet Web portal and the private internal Web server has been migrated from the organization’s internal network to the Public Cloud.

The security assessment of the case study models were based in the shortcut proposed in the OSSTMM methodology, which consist of taking into consideration only the Porosity and Limitations found, assigning default controls for discovered services and accepting an uncertain but perhaps small error margin (Herzog, 2010). Base on that principle, the results presented below were obtained filling the *rav* calculator spreadsheet with the porosity and limitations detected by OpenVAS (tables 1, 2, 3 below). Default values were assigned to the controls, what makes it possible to compare different infrastructures using different controls, which is the most probable scenario when comparing an organization's infrastructure with a Cloud infrastructure. After running the security assessment using OpenVAS and transporting the metrics to the *rav* calculator, we could compare the results from the Base Line with results from two models (Use Case 1 and Use Case 2), and came to a conclusion that the security is not heavily impacted in the Cloud use cases, with a loss of 2,4601% in the Use Case 1 and 2.8272% in the Use Case 2 relative to the Base line model (table 1).

Table 1: Case study results.

	Base Line	Use Case 1	Use Case 2
Actual Security (rav)	77.5333	75,6259	75.3413
Variance	N/A	-2,4601%	-2.8272%

The above results were obtained from the vulnerability assessment which produced the following data:

Table 2: Porosity.

	Base Line	Use Case 1	Use Case 2
Visibility	101	148	159
Access	2	4	5
Trust	3	3	4

Table 3: Limitations.

	Base Line	Use Case 1	Use Case 2
Vulnerabilities	13	24	24
Weaknesses	28	32	32
Concerns	53	76	86
Exposures	15	328	341
Anomalies	0	0	0

The mapping between the Security Assessment and the inputs to the rav calculator is as follows:

Item	How to get
visibility	Number of servers in the use case + number of unique open ports for all servers
Access	Interactions points between the servers and the outside world
Trust	Interactions that do not require authentication

The *Limitations* in the *rav* calculator were mapped directly from the OpenVAS Results as seen on the next table.

OSSTMM	OpenVAS
Vulnerability	High Severity
Weaknesses	Medium Severity
Concerns	Low Severity
Exposures	Log
Anomalies	False Positives

Applying the concepts proposed in our method, the variance obtained can be used as a reference value when the enterprise will require the evaluation other migrations of resources to the same Cloud, thus eliminating the necessity of running further security assessment to determine viability. This process can be used repeatedly by the enterprise which will consequently provide several benefits such as short project life cycles, cost reduction,

7 CONCLUSIONS AND FUTURE WORK

Using the method proposed by this paper will make it possible to have a practical and objective view of the security provided by a specific Cloud provider. Using the metrics from a security assessment over that Cloud, one can estimate how much the security of its assets will be influenced even before migrating them to that Cloud. Although there will be considerable resistance from the Cloud provider to allow for any customer to perform a security testing, the barrier can be overcome by standardizing the tests and defining criteria to allow the Cloud provider to perform them and making the results publicly available.

Regarding to the method presented in this paper, we understand that some gaps must be addressed, such as the depth of the security assessment. In our case study, the tests was performed using the OpenVAS security vulnerability scanner software (www.openvas.org), which does not verify some Cloud specific issues such as VM isolation, memory sharing, storage sharing and reuse, etc. Therefore, a more in depth assessment should include a set of tools tests to verify virtualization robustness and isolation effectiveness.

Another improvement can be done in the verification of the Security Controls. In our study case, we have used default controls for all the interaction points and vulnerabilities as supported by the OSSTMM methodology. The Cloud providers can add much more value to their security assessment reports if they decide to actually verify and report all the controls implemented, thus reducing the error margin in the results. These controls may come from an existing source such as from the "Consensus Assessments Initiative" questionnaire (CSA, 2011).

REFERENCES

Reuters, 2013, “Amazon wins key cloud security clearance from government”, available online: http://www.reuters.com/article/2013/05/21/us-amazon-cloud-idUSBRE94K06S20130521.

European Network and Information Security Agency (ENISA), (2009), “Cloud: Benefits, risks and recommendations for information security”, http://www.enisa.europa.eu/.

Yildiz, M., Abawajy, J., Ercan, T., Bernoth, A., 2009, “A Layered Security Approach for Cloud Computing Infrastructure”, 2009. *10th International Symposium on Pervasive Systems Algorithms, and Networks,* IEEE 978-0-7695-3908-9/09, p.763-767.

Herzog, Pete, 2010, “OSSTMM 3 – The Open Source Security Testing Methodology Manual – Contemporary Security Test and Analysis”, Institute for Security and Open Methodologies (ISECOM), (Online). Available at: http://www.isecom.org/mirror/OSSTMM.3.pdf.

Herzog, Pete, 2011, “Analyzing the Biggest Bank Robbery in History: Lessons in OSSTMM Analysis”, Online Banking Magazine, 2/2011, (Onine). Available at: http://hakin9.org/analyzing-the-biggest-bank-robbery-in-history-lessons-in-osstmm-analysis/.

Cloud Security Alliance, 2009, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, (Online). Available at: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

Cloud Security Alliance, 2011, “Consensus Assessments Initiative”, (Online). Available at: https://cloudsecurityalliance.org/research/cai.

U.S. Chief Information Officer, 2010, “Proposed Security Assessment and Authorization for U.S. Government Cloud Computing”, (Online). Available at: http://educationnewyork.com/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf.

OWASP, 2012, “Cloud Top 10 Security Risks”, (Online). Available at: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project.

Grobauer, B., Walloschek, T., Stöcker, E., 2011. "Understanding Cloud Computing Vulnerabilities". In IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011, doi:10.1109/MSP.2010.115, (Online). Available at: *http://www.computer.org/csdl/mags/sp/2011/02/msp2011020050-abs.html.*

Hiroyuki, S., Shigeaki, T., Atsushi, K., 2011, “Building a Security Aware Cloud by Extending Internal Control to Cloud”, 2011 *Tenth International Symposium on Autonomous Decentralized Systems*, IEEE 978-0-7695-4349-9/11, p. 323-326.

CERT, 2011, “2011 CyberSecurityWatch Survey - How Bad Is the Insider Threat?”, Carnegie Mellon University, (Online). Available at: http://www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf.

Cloud Computing Use Cases Group, 2010, “Cloud Computing Use Cases Version 4.0” (Online). Available at: http://cloudusecases.org.

Krutz, R., Vines, R., 2010, Cloud Security: A Comphrehensive Guide to Secure Cloud Computing, Wiley Publishing, Indianápolis.

NIST, 2011, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology – U.S Department of Commerce, NIST Special Publication 800-145 (Online). Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Wilhelm, T., 2010, Professional Penetration Testing, Elsevier Inc, Burlington.

McClure, S., Scambray, J., Kurtz, G., 1999, Hacking Exposed: Network Security Secrets and Solutions, Oxborne, California.