International Journal of Reliable Information and Assurance
Vol.7, No.2 (2019), pp.1-6
http://dx.doi.org/10.21742/ijria.2019.7.2.01

A Methodology for Assessing Security Vulnerability of Cloud Services

Kwang-Kyu Seo

Dept. of Management Engineering, Sangmyung University, Korea
kwangkyu@smu.ac.kr

Abstract

Cloud services continue to change the business paradigm to use computing resources such as infrastructure, platform and application using the network access. They have created new security threats and challenges. When large amounts of data are saved in the cloud, the cloud is naturally exposed to attack. In cloud services, analysis and evaluation of security vulnerability should be made with protection plans that provide the objective data and information necessary to establish measures for information protection for each business of firms and take into account the impact on their respective responsibilities. This paper presents a framework to evaluate security vulnerability that reflects the business impacts. Through this framework, it is possible to evaluate vulnerability items of cloud services. Eventually, the proposed methodology will help establish security policies for both cloud service providers and users.

Keywords: *Evaluation framework, Vulnerability, Security, Threat, Cloud service*

1. Introduction

Cloud services continue to change the business paradigm to use computing resources such as infrastructure, platform and application using the network access. However, they are encountering security problems. The importance of cloud security is much more growing, and it is very necessary to assess the importance of security threats.

In order to prevent security vulnerabilities, researches to accumulate and effectively provide information about security weaknesses is actively carried out [1][2]. Typical examples are "Common Weakness Enumeration (CWE) [3], Common Vulnerability Enumeration (CVE) [4], and National Vulnerability Database (NVD) [5]". In addition, "CWE/SANS Top 25 and OWASP Top 10" are being announced in order to select and respond to important security weaknesses among various security weaknesses [6][7]. In Korea, security weakness criteria for information software development security policy are proposed by the Korean government and the Korea Internet Development Agency (KISA) has launched a new vulnerability discovery prize system from 2012 to promptly respond to new security vulnerabilities [8].

It is important to determine the severity of security weaknesses or resulting security weaknesses found in the information system development and operation, and to carry out a priority response to critical and weak points. To do this, evaluation scales are needed to evaluate security weaknesses and security vulnerabilities. Common examples are "Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS)" [9].

Article history:
Received (May 17, 2019), Review Result (June 13, 2019), Accepted (July 8, 2019)

Print ISSN: 2288-8950, eISSN: 2207-5143 IJRIA
Copyright ⓒ 2019 GV Press

While software vulnerability analysis, cloud service vulnerability analysis and software security vulnerability quantification studies have been carried out, but the research on security vulnerability quantification studies of cloud services has not been done.

The impact and severity of security vulnerabilities in cloud services are affected not only by their inherent characteristics, but also by the nature of their environment, application areas, and information system environment. Therefore, a new security vulnerability assessment method considering the characteristics of cloud services is needed. It is necessary to establish and utilize a quantitative evaluation framework to determine the importance of cloud security vulnerabilities. This study explores a quantitative methodology to assess the importance of security vulnerabilities of cloud services and it can calculate the weakness scores of vulnerabilities of them.

2. Background

Currently, CWSS and CVSS are the most typical security vulnerability and vulnerability assessment systems. In this section, CWSS and CVSS are explained as a basic research background. In addition, the risk assessment method of “the Open Web Application Security Project (OWASP) “is also described briefly.

CWSS is a system for assessing the importance of security weaknesses and has been promoted as part of the CWE project to build overall software security weakness specification data. The characteristics of CWE and CWSS are that it is a community-type collaboration that is made up of governments, academia, and industries that are responsible for the development and security of secure software. The CWSS provides quantitative criteria that can prioritize elimination of various weaknesses commonly encountered in software.

CVSS provides a general framework for assessing security vulnerabilities as a result of evaluating the importance of actual security vulnerabilities from security weaknesses. CVSS differs from CWSS in that it targets real security vulnerabilities that can be exploited by attackers in real-world software.

OWASP deals with the security of web applications as an online community where methodologies, documents and tools are freely available. OWASP Top 10 presents the most critical threats and risks to firms and businesses.

3. A methodology for assessing security vulnerability of cloud services

According to the "Critical Analysis Criteria for Vulnerable Information and Communication Infrastructure" published by the Korean government, the main checkpoints are divided into management, physical and technical. Administrative analysis and evaluation are confirmed by document confirmation and interviews with information security officers, and physical analysis and evaluation are confirmed and evaluated through actual inspection of controlled areas. Technical checkpoints are evaluated through inspection tools or mock hacks.

The vulnerability assessment process shows the risk level for the vulnerability check item. The risk level is shown in three levels of high, medium, and lower. The improvement direction should be established by early improvement at high level and medium and low levels should be established with middle or long-term improvements. However, in order to perform effective vulnerability analysis and evaluation, it is necessary to analyze the potential risks of each vulnerability.

In this paper, we analyze the potential risks of cloud services and then quantify them using CWSS, a security vulnerability quantification methodology. However, there is a disadvantage of the quantitative methodology of CWSS. Because CWSS evaluates vulnerabilities and quantifies vulnerabilities in terms of attack technology, there is no way to quantify vulnerabilities to cloud services provided by a company or organization and to determine services that need priority. In the case of a company or an organization suffering from an attack using vulnerability discovered in a cloud service, it is needed to assess the vulnerability and quantify it. To deal with these problems, we suggest a quantitative evaluation framework for cloud service vulnerability evaluation items using OWASP, an application risk assessment methodology.

3.1. Criteria for selection of evaluation scale

CWSS (Common Weakness Scoring System) is divided into 3 groups and 16 factors. Details are shown in the following [Table 1].

Table 1. CWSS scale

Group	Name
Base Finding	“Technical Impact (TI)”
	“Acquired Privilege (AP) ”
	“Acquired Privilege Layer (AL) ”
	“Internal Control Effectiveness (IC) ”
	“Finding Confidence (FC) ”
Attack Surface	“Required Privilege (RP) ”
	“Required Privilege Layer (RL) ”
	“Access Vector (AV) ”
	“Authentication Strength (AS) ”
	“Level of Interaction (IN) ”
	“Deployment Scope (DS) ”
Environmental	“Business Impact (BI) ”
	“Likelihood of Discovery (DI) ”
	“Likelihood of Exploit (EX) ”
	“External Control Effectiveness (EC) ”
	“Prevalence (P)”

Of the 16 factors, five factors were selected based on the OWASP risk assessment methodology for quantitative assessment. Eleven items were excluded because they were not suitable for evaluation as a general characteristic of the security weakness itself, or were dependent on the environment or dependent on the characteristics of the operating system and the software were considered to be inappropriate for the evaluation items.

Technical Impact (TI) as an example of five factors is as follows. Evaluate the technical impact of a successful attack if the attack is compromised by the vulnerability. The evaluation method refers to documents such as OWASP, and the items that are not applicable are given the default rating. The evaluation scale is as follows.

Table 2. Rating scale of technical impact (TI)

Value	Code	Weight	Description
Critical	C	1.0	the impact of data loss and destruction is significant
High	H	0.9	the impact of data loss and destruction is high
Medium	M	0.6	the impact of data loss and destruction is moderate
Low	L	0.3	the impact of data loss and destruction is low
None	N	0.0	the impact of data loss and destruction is none
Default	D	0.6	default

Copyright © 2019 GV Press

Unknown	UK	0.5	not enough information about the security vulnerability
Not Applicable	NA	1.0	not applicable
Quantified	Q		quantify with users weights

3.2. Evaluation of vulnerability of the cloud service

AS mentioned before, the CWSS methodology combined with OWASP risk assessment methodology is used for quantitative evaluation. The score of CWSS has a range from 0 to 100. The formula used is as follows.

$Score = Base\ Finding\ Point * Attack\ Surface\ Point * Environment\ Point$

It consists of the product of each group formula. Details are as follows.

① Base Finding Point

It has a range from 0 to 100 and the formula used is as follows.

$Base\ Finding\ Point = [(10 * TI + 5 * (AP + AL) + 5 * FC) * f(TI) * IC] * 4.0$

$f(TI) = 0, if\ TI = 0;$

$f(TI) = 1, otherwise.$

② Attack Surface Point

It has a range from 0 to 1 and the formula used is as follows.

$Attack\ Surface\ Point = [20 * (RP + RL + AV) + 20 * DS + 15 * IN + 5 * AS] /100.0$

③ Environment Point

It has a range from 0 to 1 and the formula used is as follows.

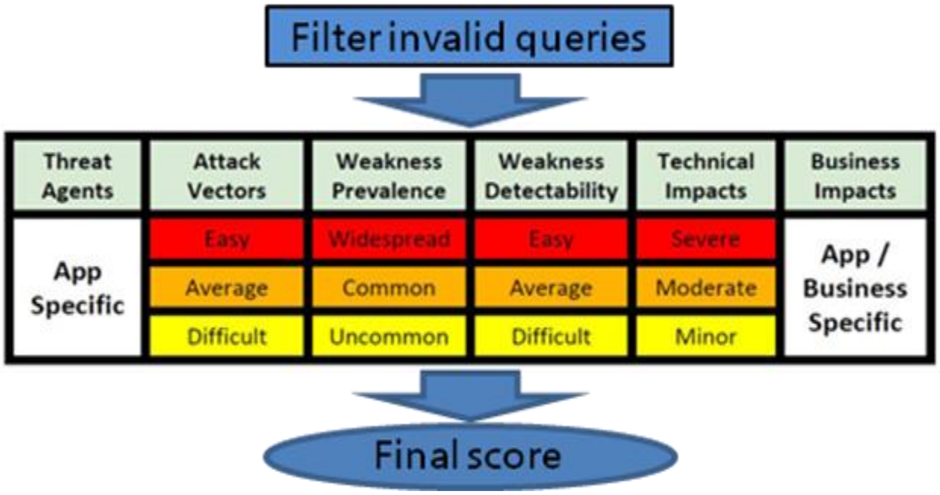
$Environment\ Point = [(10 * BI + 3 * DI + 4 * EX) + 3 * P) * f(BI) * EC] /20.0$

$f(BI) = 0, if\ BI = 0;$

$f(BI) = 1, otherwise$

4. Case study

The Korea Internet Development Agency (KISA) presented 9 vulnerability items of IaaS and 26 vulnerability items of SaaS for security vulnerability check of the cloud service [9]. The checklist consists of 9 vulnerability items of IaaS and the importance of all items gives ‘High’ level. In this case study, we only calculate the quantitative score of security vulnerability of IaaS in cloud services.



Threat Agents	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	Easy	Widespread	Easy	Severe	App / Business Specific
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

Figure 1. Vulnerability calculation process

The process of vulnerability identification is as follows. For example, a vulnerability item called 'Filter invalid queries' is assigned a risk rating for the probability of attack, frequency of occurrence, likelihood of detection, and technical impact. The weight value for the risk grade is substituted into the formula to calculate the final score. The details are shown in [Figure 1].

The vulnerability check item of IaaS was quantified as shown in [Table 3]. [Table 3] shows some top score of vulnerability items for IaaS.

Table 3. Final score of vulnerability items for the cloud service (IaaS)

Rank	Checklist	Importance	Score
1	External / internal transfer status	High	93.1
2	Filter invalid queries	High	92.5
3	Critical data access authorization	High	89.5
4	Malicious code detection scheme	High	84.5
5	Important data	High	81.5
......	......	......	......

5. Conclusion

Cloud services continue to change the business paradigm to use computing resources such as infrastructure, platform and application using the network access. However, they are encountering security problems. The importance of cloud security is much more growing, and it is very necessary to assess the importance of security threats.

This paper presented the quantitative methodology to assess the importance of security vulnerabilities and it can calculate the weakness scores of vulnerabilities of cloud services. It also reflects the influence of each institution or company. Through this, we transformed the horizontal structure of vulnerability check items of the cloud service, which had the importance of the item as a whole, to the vertical structure through the quantification. Vulnerability scores calculated using modified CWSS quantitative evaluation methodology are also meaningful, and re-measured evaluation values reflecting the impact of work have been proposed to reflect the characteristics of each company or institution.

References

[1] C. K. Park, H. S. Kim, T. J. Lee, and J. C. Ryou, “Function partitioning methods for malware variant similarity comparison,” J. of The Korea Institute of information Security & Cryptology, vol.25, no.2, pp.321-330, **(2015)**

[2] J. Park, H. Kang, and S. Kim, “How to combine secure software development lifecycle into common criteria,” J. of The Korea Institute of information Security & Cryptology, vol.24, no.1, pp.171-182, **(2014)**

[3] Common Weakness Enumeration (CWE), http://cwe.mitre.org/, **(2018)**

[4] Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org, **(2019)**

[5] National Vulnerability Database (NVD), http://nvd.nist.gov, **(2019)**

[6] 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/, **(2011)**

[7] OWASP, Top 10 - 2017, “The ten most critical web application security risks,” https://www.owasp.org, **(2017)**

[8] Korea Internet & Security Agency Korea Internet Security Center (KISC), “Bounty program for new SW vulnerabilities,” https://www.krcert.or.kr/kor/consult/consult_04.jsp

[9] KISA, “Domestic cloud service security vulnerability check,” Seoul, **(2012)**

This page is empty by intention.