The Design of Vulnerability Management System

GeonLyang Kim, JinTae Oh, DongIl Seo, JeongNyeo Kim,

ETRI, Republic of Korea

Summary
As the number of users using the internet has increased, recently the internet services have been growing rapidly. And the number of attacks for the internet services has been growing rapidly because of software flaw vulnerabilities in recent years. The software assets composed of the internet service have lots of vulnerabilities, the system administrator don't know the response method for them in confusion. But the security organizations in Korea aren't in cooperation with other countries and organizations to collect, analyze and respond vulnerabilities and don't have the integrated database and the organized management system for the vulnerabilities.
This paper introduces the method constructing and managing the vulnerability database, the system managing the software flaw vulnerabilities and calculating the relative severity of software flaw vulnerabilities within information technology systems by referring to National Vulnerability Database(NVD) as the public vulnerability database which is being operated in USA.

Key words:
Vulnerability Assessment, Vulnerability Management.

1. Introduction

As the number of users using the internet has increased, recently the internet services have been growing rapidly. And the number of attacks for the internet services has been growing rapidly because of software flaw vulnerabilities in recent years. The software assets composed of the internet service have lots of vulnerabilities, the system administrator don't know the response method for them in confusion. So, the necessity of vulnerability management system that manage lots of vulnerabilities efficiently, select the priority vulnerabilities from lots of vulnerabilities, provide the system administrator with the relative severity of software flaw vulnerabilities has increased.

Other major countries such as USA, Japan have already realized the need of the systematic management of vulnerabilities since the 1990s or 2000s and have constructed the vulnerability management system through policy and law. They have developed it through the consistent research. And they have constructed and managed their vulnerability databases in cooperation with other countries and organizations to collect, analyze, and respond vulnerabilities rapidly.

NVD is the U.S. government repository of standards-based vulnerability management reference data. NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol(SCAP). NIST has developed the SCAP to provide the standardized technical mechanisms to share information between systems. SCAP is a multipurpose protocol that supports automated vulnerability checking, technical control compliance activities, and security measurement. SCAP consists of 11 component specifications as described in Section 2.1. The Common Vulnerability Scoring System(CVSS) is an industry standard that enables the security community to calculate the relative severity of software flaw vulnerabilities within information technology systems through sets of security metrics and formulas. During the past year, NIST security staff continued to provide technical leadership in determining how CVSS could be adapted for use with other types of vulnerabilities besides software flaws.

By the way, the security organizations in Korea aren't in cooperation with other countries and organizations to collect, analyze and respond vulnerabilities and don't have the integrated vulnerability database and the organized management system for vulnerabilities. Korea has never had any management systems for software flaw vulnerabilities

This paper introduces the method constructing the vulnerability database including the public vulnerability database and the private vulnerability database, the system managing lots of vulnerabilities, selecting the priority vulnerabilities from lots of vulnerabilities and assessing the relative severity of internet service that consists of several products having a lot of vulnerabilities

The Vulnerability Management System of this paper allows us know lots of vulnerabilities about software and application programs within information technology systems, the priority vulnerabilities, and the relative severity score representing how this internet service is vulnerable. So it has the merit that we can plan countermeasures for lots of software flaw vulnerabilities according to the relative severity score in advance.

Manuscript received April 5, 2013
Manuscript revised April 20, 2013

2. Related Works

2.1 SCAP

To support the overarching security automation vision, it is necessary to have both trusted information and a standardized means to store and share it. Through close work with its government and industry partners, NIST has developed the SCAP to provide the standardized technical mechanisms to share information between systems. Through the NVD and the National Checklist Program(NCP), NIST is providing relevant and important information in the areas of vulnerability and configuration management. Combined, SCAP and the programs that leverage it are moving the information assurance industry towards being able to standardize communications, collect and store relevant data in standardized formats, and provide automated means for the assessment and remediation of systems for both vulnerabilities and configuration compliance.

SCAP is a suite of specifications that use XML to standardize the format and nomenclature by which security software products communicate information about software flaws and security configurations. SCAP includes software flaw and security configuration standard reference data, also known as SCAP content. This reference data is provided by the NVD.

SCAP is a multipurpose protocol that supports automated vulnerability checking, technical control compliance activities, and security measurement. The U.S. government, in cooperation with academia and private industry, is adopting SCAP and encourages its use in support of security automation activities and initiatives.

At the end of September 2011, draft SP 800-126 Revision 2, The Technical Specification for the SCAP Version 1.2 was approved as final and is the SCAP technical specification. This document describes the 11 component specifications comprising SCAP as following:

- ● Languages:
  - Extensible Configuration Checklist Description Format (XCCDF), a language for authoring security checklists/benchmarks and for reporting results of evaluating them
  - Open Vulnerability and Assessment Language (OVAL), a language for representing system configuration information, assessing machine state, and reporting assessment results
  - Open Checklist Interactive Language (OCIL), a language for representing checks that collect information from people or from existing data stores made by other data collection efforts
- ● Reporting Formats:
  - Asset Reporting Format (ARF), a format for expressing the transport format of information about assets and the relationships between assets and reports
  - Asset Identification (AI), a format for uniquely identifying assets based on known identifiers and/or known information about the assets
- ● Enumerations:
  - Common Platform Enumeration (CPE), a nomenclature and dictionary of hardware, operating systems, and applications
  - Common Configuration Enumeration (CCE), a nomenclature and dictionary of software security configurations
  - Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaws
- ● Measurement and Scoring Systems:
  - Common Vulnerability Scoring System (CVSS), a specification for measuring the relative severity of software flaw vulnerabilities
  - Common Configuration Scoring System (CCSS), a specification for measuring the relative severity of system security configuration issues
- ● Integrity:
  - Trust Model for Security Automation Data (TMSAD), a specification for using digital signatures in a common trust model applied to security automation specifications

SCAP is being widely adopted by major software and hardware manufacturers and has become a significant component of information security management and governance programs. The protocol is expected to evolve and expand in support of the growing need to define and measure effective security controls; assess and monitor ongoing aspects of information security; remediate noncompliance; and successfully manage systems in accordance with the Risk Management Framework described in SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

2.2 NVD

NVD is the U.S. government repository of standards-based vulnerability management reference data. The NVD provides information regarding security vulnerabilities and configuration settings, vulnerability impact metrics, technical assessment methods, and references to remediation assistance and IT product identification data. The NVD reference data supports security automation efforts based on the SCAP. As of September 2011, the NVD contained the following resources:

- ● Over 47,000 vulnerability advisories with an average of 8 new vulnerabilities added daily

- 36 SCAP-expressed checklists containing thousands of low-level security configuration checks that can be used by SCAP-validated security products to perform automated evaluations of system state
- 159 non-SCAP security checklists
- 212 U.S. Computer Emergency Readiness Team (US-CERT) alerts, 2,529 US-CERT vulnerability summaries, and 6,854 SCAP machine-readable software flaw checks
- Product dictionary with 35,222 operating system, application, and hardware name entries
- 32,084 vulnerability advisories translated into Spanish

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security’s National Cyber Security Division. It supports the U.S. government multi-agency(OSD, DHS, NSA, DISA, and NIST) Information Security Automation Program. It is the U.S. government content repository for the SCAP.

NVD’s effective reach has been extended by the use of NVD SCAP data by commercial security products deployed in thousands of organizations worldwide. Increased adoption of SCAP is evidenced by the increasing demand for NVD XML data feeds and SCAP-expressed content from the NVD website. Concerted outreach efforts over the last year have resulted in an increase in the number of vendors providing SCAP-expressed content.

NVD continues to play a pivotal role in the payment card industry (PCI) efforts to mitigate vulnerabilities in credit card systems. PCI mandates the use of NVD vulnerability severity scores in measuring the risk to payment card servers worldwide and for prioritizing vulnerability patching. PCI’s use of NVD severity scores helps enhance credit card transaction security and protects consumers’ personal information.

The CVE, CWE, CVSS, NVD are referred from Open Source Vulnerability Database(OSVDB), the vulnerability database of Japan and China, and so on. The vulnerability data of NVD is as in the following;

- Vulnerability ID
- Original Release Date
- Last Revised
- Source
- Overview
- Impact(CVSS Severity, CVSS Version 2 Metrics)
- References to Advisories, Solutions, and Tools
- Vulnerable Software and Versions
- Vulnerability Type
- CVE Standard Vulnerability Entry

2.3 CVSS

Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk. But when there are so many to fix, with each being scored using different scales, how can IT managers convert this mountain of vulnerability data into actionable information. The CVSS is an open framework that addresses this issue.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure 1.

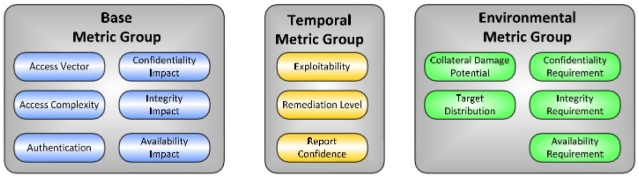


Figure 1. The Three Metric Groups of CVSS

These metric groups are described as follows;

- Base Metric Group: represents the intrinsic and fundamental characteristics of vulnerabilities that are constant over time and user environments.
- Temporal Metric Group: represents the characteristics of vulnerabilities that change over time but not among user environments.
- Environmental Metric Group: represents the characteristics of vulnerabilities that are relevant and unique to a particular user’ s environment.

The purpose of the Base Metric Group is to define and communicate the fundamental characteristics of vulnerabilities. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of vulnerabilities. Users can then invoke the Temporal and Environmental Metric Groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

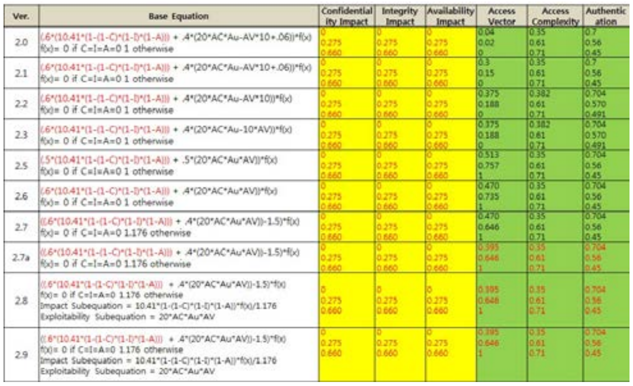
The major target of security is confidentiality, integrity, availability, they are called CIA. The Base Metric Group consists of base metrics such as confidentiality, integrity, availability, authentication, access control. It measures the severity of vulnerabilities based on the base metrics. The confidentiality, integrity, availability is used as the facts to calculate the impact score of CVSS.

The major target of security is confidentiality, integrity, availability, they are called CIA. The Base Metric Group consists of base metrics such as confidentiality, integrity, availability, authentication, access control. It measures the severity of vulnerabilities based on the base metrics. The

confidentiality, integrity, availability is used as the facts to calculate the impact score of CVSS.

The NVD of the federal government provides only the base score and the score of base metrics of Base Metric Group. Figure 2 expresses the CVSS history. The CVSS research has been carried out to version 2.9. We can see that the base equation assign the rate of CIA 60%

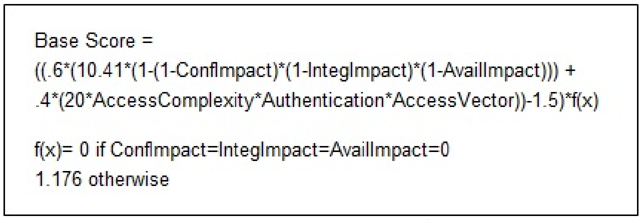
We can see no change in the base equation and the score of the base metrics after version 2.7a through Figure 2. The base score is calculated as 0~10 through the base equation.



Ver.	Base Equation	Confidentiality Impact	Integrity Impact	Availability Impact	Access Vector	Access Complexity	Authentication
2.0	(.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au-AV*10+.06))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.04 0.02 0	0.35 0.61 0.71	0.7 0.56 0.45
2.1	(.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au-AV*10+.06))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.3 0.15 0	0.35 0.61 0.71	0.7 0.56 0.45
2.2	(.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au-AV*10))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.375 0.188 0	0.382 0.61 0.71	0.704 0.570 0.491
2.3	(.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au-10*AV))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.375 0.188 0	0.382 0.61 0.71	0.704 0.570 0.491
2.5	(.5*(10.41*(1-(1-C)*(1-I)*(1-A))) + .5*(20*AC*Au*AV))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.513 0.757 1	0.35 0.61 0.71	0.704 0.56 0.45
2.6	(.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au*AV))*f(x) f(x)= 0 if C=I=A=0 1 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.470 0.735 1	0.35 0.61 0.71	0.704 0.56 0.45
2.7	((.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au*AV))-1.5)*f(x) f(x)= 0 if C=I=A=0 1.176 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.470 0.646 1	0.35 0.61 0.71	0.704 0.56 0.45
2.7a	((.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au*AV))-1.5)*f(x) f(x)= 0 if C=I=A=0 1.176 otherwise	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.395 0.646 1	0.35 0.61 0.71	0.704 0.56 0.45
2.8	((.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au*AV))-1.5)*f(x) f(x)= 0 if C=I=A=0 1.176 otherwise Impact Subequation = 10.41*(1-(1-C)*(1-I)*(1-A))*f(x)/1.176 Exploitability Subequation = 20*AC*Au*AV	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.395 0.646 1	0.35 0.61 0.71	0.704 0.56 0.45
2.9	((.6*(10.41*(1-(1-C)*(1-I)*(1-A))) + .4*(20*AC*Au*AV))-1.5)*f(x) f(x)= 0 if C=I=A=0 1.176 otherwise Impact Subequation = 10.41*(1-(1-C)*(1-I)*(1-A))*f(x)/1.176 Exploitability Subequation = 20*AC*Au*AV	0 0.275 0.660	0 0.275 0.660	0 0.275 0.660	0.395 0.646 1	0.35 0.61 0.71	0.704 0.56 0.45

Figure 2. The CVSS History

The more remote attacker can attack the target host, the greater the vulnerability score is assigned in case of the "Access Vector" of the Base Metrics Group. The "Access Vector" means the more the hacker can attack the system in the distance, the more it is vulnerable. A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network. The possible values for this "Access Vector" metric are "Local", "Adjacent Network", and "Network", and the each score of the values for this "Access Vector" metric of CVSS v2.9 is 0.395, 0.646, and 1.0. The value of "Network" among "Local", "Adjacent Network", and "Network" is the highest value "1".



Base Score =
((.6*(10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))) +
.4*(20*AccessComplexity*Authentication*AccessVector))-1.5)*f(x)

f(x)= 0 if ConfImpact=IntegImpact=AvailImpact=0
1.176 otherwise

Figure 3. The Base Score Equation of CVSS v2.9

The base score of CVSS is calculated with the values of the base metrics by the base score equation. The base score equation of CVSS v2.9 is as shown in Figure3.

NVD provides only the base score and the score of the base metrics, not the temporal and environmental score.

3. The Vulnerability Management System

3.1 The Structure of the Vulnerability Management System

The structure of the Vulnerability Management System is as shown in Figure 4. It consists of DB Management Block, Vulnerability Selection Block, Patch Management Block, Security Enhancement Block, and Vulnerability Assessment Block.

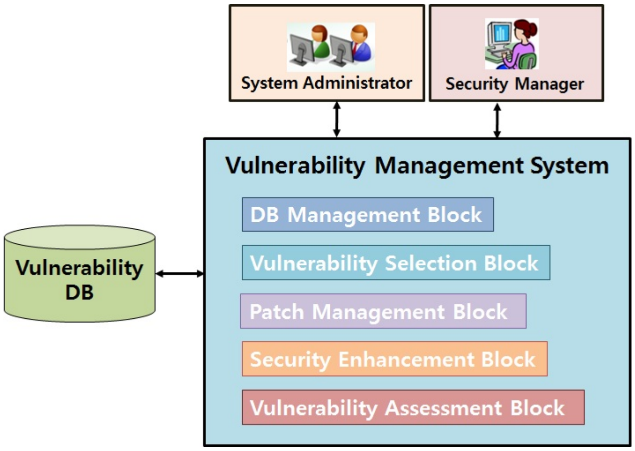

System Administrator
Security Manager
Vulnerability Management System
DB Management Block
Vulnerability Selection Block
Patch Management Block
Security Enhancement Block
Vulnerability Assessment Block
Vulnerability DB

Figure 4. The Structure of the Vulnerability Management System

DB Management Block executes the function constructing and managing vulnerability database. The type of vulnerability database is two, public database and private database. The detailed information is explained at the next chapter.

Vulnerability Selection Block executes the function selecting the priority vulnerabilities among lots of vulnerabilities to work out the patch of software rapidly in advance. So, the system administrator can manage and respond calmly for lots of vulnerabilities.

Patch Management Block executes the function checking whether the vulnerabilities include patch information or not, and working out the patch of software. The system can work out the patch of software by making a connection with the Patch Management System(PMS).

Security Enhancement Block executes the function analyzing what security solutions are needed to resolve the vulnerabilities and analyzing how security enhancement degree is when deploying security solutions for the vulnerabilities.

Vulnerability Assessment Block executes the function assessing the vulnerability severity by checking whether the system administrator works out the patches of the vulnerabilities or not, and the existence of security solutions for the vulnerabilities.

3.2 The Vulnerability Database Construction

The construction procedure of the vulnerability database that is used in this vulnerability management system is as shown in Figure 5.

The vulnerabilities of software such as operating systems and applications have been already collected and managed through NVD of USA, OSVDB as the open vulnerability database, the commercial vulnerability database, etc. It is a good idea that this vulnerability management system makes full use of established vulnerability databases. However, the vulnerability management system must construct the private database for the vulnerabilities of the domestic software because they don’t exist in the public vulnerability databases.

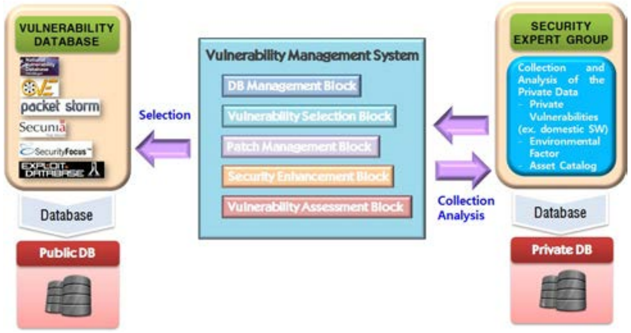


Figure 5. The Vulnerability Database Construction

We recommend that the vulnerability management system manages the vulnerabilities for the domestic software behind closed doors. The security expert group that collects and analyzes the vulnerabilities of the domestic software is needed to construct the private vulnerability database. And, the government-level system is needed to research and manage the vulnerabilities of the domestic software continuously.

NVD as the public vulnerability database of USA includes only the base score of CVSS, but it doesn’t include the temporal score and the environmental score of CVSS. The system must input the each score of the temporal metrics into the temporal equation and the each score of the environmental metrics into the environmental equation to get the temporal score and the environmental score. The vulnerability management system must manage these data in private because they are able to be used maliciously. The security expert group that estimates the score of the CVSS environmental metrics is needed.

3.3 Priority Vulnerabilities Selection Procedure

The number of software that makes up the system can be dozens of software, and the number of vulnerabilities that belong to the software can be dozens of vulnerability. So, the number of vulnerabilities associated with the system can be hundreds or more. The number of vulnerability that NVD has managed is more than 50,000. And the 10~20 vulnerabilities per day have been registered. As time goes on, the number of vulnerabilities will increase continually. The system must have the method to respond to hundreds of vulnerability, because the system administrator is in confusion when encountering lots of vulnerabilities.

NVD provides several data about vulnerabilities, and the useful data of those is the patch information. If the vulnerability management system works out the patch of software, the vulnerability of it disappears. So, to work out the patch of software is the most clear response method for the vulnerability, because the vulnerability disappears completely through working out the patch of software. The vulnerability management system must have the selection method for the priority vulnerabilities that it must work out the patch urgently among lots of vulnerabilities and have another security method for the vulnerabilities without path information.

The procedure selecting the priority vulnerabilities in vulnerability management system is as Figure 6.

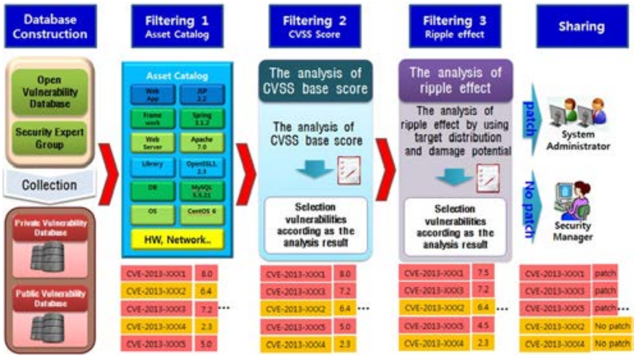


Figure 6. The Procedure to Select the Priority Vulnerabilities.

In advance, the construction of vulnerability databases is needed to select the priority vulnerabilities. The system that manages the vulnerability database persistently such as the collection and analysis of vulnerabilities and is in cooperation with other organizations and countries is needed. We recommend that the vulnerability databases are classified into the public database and the private database. The public database is constructed by using the open vulnerability databases such as NVD of the federal government, OSVDB which is an independent and open web-based vulnerability database created for the security community, the commercial vulnerability databases etc. The private database is constructed to manage private and major information such as the vulnerabilities of software developed in homeland or organization, the values of CVSS environmental metrics of organization, and so forth.

The vulnerability management system can extract the vulnerabilities of software from vulnerability databases by using the type and the version of software such as operating system, database, web server, and so on.

First, the system catalogs assets by surveying software composing internet service, and it extracts the vulnerability list of software related to assets from vulnerability databases. The system can search the vulnerability list of software related to assets by using names and versions of assets because NVD includes CPE information with vulnerability data. And it filters again the vulnerability list with the high severity relatively by referring to the base score of CVSS from the vulnerability list related to the asset catalog. Finally, it calculates again the CVSS score by reflecting the values of the environmental metrics for the vulnerability list having the high severity. It selects the final vulnerabilities by using the final CVSS score of them.

The CVSS score represents the relative severity of internet service with the score from 0 to 10. But the administrator is in confusion when encountering lots of vulnerabilities. The system needs to select some priority vulnerabilities and provide users the priority vulnerability group and solutions. But the vulnerabilities that don't belong to priority vulnerability group are not unimportant. The organization must have the response method for the trivial vulnerability, because hackers can attack through it even if it is a trivial vulnerability.

The CVSS score can be classified into 3 groups such as "warning", "critical", "very critical" and the vulnerability management system can select the vulnerabilities with the CVSS score from 8 to 10 as the priority vulnerabilities of "very critical" group among 3 groups. It can select the vulnerability list of Top N, or the top M % of the final vulnerabilities as the priority vulnerabilities.

The method classifying the vulnerabilities into 3 groups according to the CVSS score or selecting the priority vulnerabilities must be researched by security expert group. NVD includes only the CVSS base score. The method assigning the values of the temporal metrics and the environmental metrics in each organization must be analyzed by the security expert group.

Because the priority vulnerabilities need to be treated more rapid than other vulnerabilities, the system must have the method sharing and responding for them. Our system provides the priority vulnerabilities with patch information for the system administrator, the priority vulnerabilities without patch information for the security manager. The security manager must have other security plan for them.

3.4 Vulnerability Severity Assessment Procedure

As mentioned earlier, this vulnerability management system selects the vulnerabilities of software by using asset catalog. The system can know the each severity of the selected vulnerabilities through the CVSS score of vulnerabilities, because the selected vulnerabilities include the CVSS score. And the system can know the severity of the entire service through the sum of the CVSS score. If the sum of the CVSS score is larger, the severity of the internet service is the higher. If the sum of the CVSS score is "0", the severity of the internet service is "0". So, the vulnerability management system must set a goal of "0" in the sum of the CVSS score by working out the patch of software. But, all vulnerabilities don't include the patch information. The internet service always has the dangerous factors. The vulnerability management system can decrease the severity of the internet service by deploying security solutions for the vulnerabilities without the patch information. For example, if the internet service has the vulnerability for Denial of Service(DOS) attack, the severity of the internet service is decreased through the security solution that can defend against the DOS attack. The vulnerability management system also needs the research that how the internet service is able to be defended perfectly from the attack, how the severity of the internet service is decreased through the security solution, or what security solution is needed to decrease the severity of the internet service.

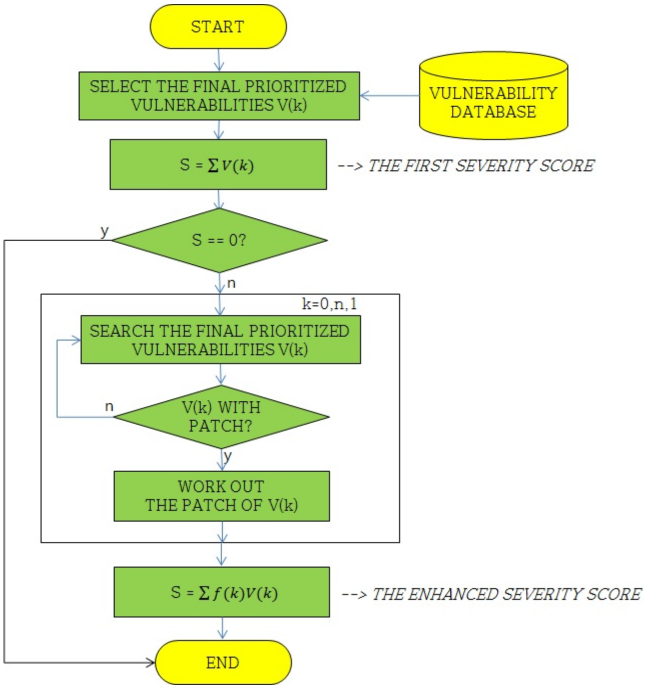

START
SELECT THE FINAL PRIORITIZED VULNERABILITIES V(k)
VULNERABILITY DATABASE
$S = \sum V(k)$
--> THE FIRST SEVERITY SCORE
S == 0?
y
n
k=0,n,1
SEARCH THE FINAL PRIORITIZED VULNERABILITIES V(k)
n
V(k) WITH PATCH?
y
WORK OUT THE PATCH OF V(k)
$S = \sum f(k)V(k)$
--> THE ENHANCED SEVERITY SCORE
END

Figure 7. The Procedure to Assess the Severity of Vulnerabilities

Figure 7 shows the procedure assessing the severity and the security enhancement degree of the internet service. As mentioned earlier, the vulnerability management system can get the first severity score through the sum of the CVSS score. If the first severity score is 0, the procedure is ended. And, the severity score is decreased through working out the patch of software, and the vulnerability management system can get the enhanced severity score in security finally by checking the security solution for the vulnerabilities.

4. Conclusion

Other countries such as USA, Japan have constructed and managed their vulnerability databases in cooperation with other countries and organizations to collect, analyze, and respond vulnerabilities rapidly. But the security organizations in Korea aren't in cooperation with other countries and organizations to collect, analyze and respond vulnerabilities and don't have the integrated vulnerability databases and the organized management systems for vulnerabilities.

In this paper, we suggest the system that selects the priority vulnerabilities for the response, calculates the relative severity of software flaw vulnerabilities within information technology systems, and assesses the security enhancement degree. And this paper describes the method constructing the vulnerability databases including the public vulnerability database and the private vulnerability database to manage lots of vulnerabilities

This system allows us know the priority vulnerabilities about lots of software and application programs of systems and the relative severity through the CVSS representing how this internet service is vulnerable. So it has the merit that we can plan countermeasures for lots of vulnerabilities according to the relative score in advance.

Acknowledgments

This work was supported by the IT R&D program (10043959, Development of EAL 4 level military fusion security solution for protecting against unauthorized accesses and ensuring a trusted execution environment in mobile devices) of KEIT, Korea.

References

[1] SCAP, http://scap.nist.gov
[2] SCAP Version 1.2, http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf
[3] NIST Computer Security Division 2011 Annual Report, http://csrc.nist.gov/publications/nistir/ir7816/nistir_7816.pdf
[4] NVD, http://nvd.nist.gov
[5] OSVDB, http://osvdb.org
[6] http://www.first.org/cvss/history
[7] http://www.first.org/cvss/cvss-guide.html
[8] CPE, http://cpe.mitre.org
[9] JVN, http://jvn.jp

GeonLyang Kim received the B.S. and M.S. degrees in Computer Science from Chonnam National University in 1999 and 2001, respectively. She is a senior researcher of Electronics and Telecommunications Research Institute (ETRI) in Korea.

JinTae Oh received the B.S. and M.S. degrees in Electronics Engineering from Kyungpook National University in 1990 and 1992, respectively. He received his Ph. D. degree in Computer Engineering from Chungnam National University in 2010. He is a principal researcher and executive director of Creative Service Research Section of ETRI in Korea.

DongIl Seo received the B.S. in Electronic from KyungPook National University in 1989, the M.E. in Computer Network from POSTECH in 1994, and the Ph.D in Computer Science from ChungBuk National University in 2004. He is a principal researcher of ETRI in Korea.

JeongNyeo Kim received the B.S. in Computer Science and Statistics from Chonnam National University in 1987, the M.E. and D.E. degrees in Computer Engineering from Chungnam National University in 2000 and 2004, respectively. She is a principal researcher and the leader of Mobile Security Research Section of ETRI in Korea.