An improved CVSS-based vulnerability scoring mechanism

Ruyi Wang
Dept. Computer Science and Technology
Northwest University
Xi'an, China
e-mail: wangruyi@nwu.edu.cn

Ling Gao/Qian Sun/Deheng Sun
Dept. Computer Science and Technology
Northwest University
Xi'an, China
e-mail: gl@nwu.edu.cn/sq@nwu.edu.cn
/sundeheng@nwu.edu.cn

***Abstract*—Through scoring vulnerabilities according to their risks, mastering statuses of vulnerabilities, security managers could adjust the configuration for computer security in time and give repair methods to different vulnerabilities flexibly. Since scoring vulnerabilities is significant for evaluating and repairing vulnerabilities, this paper presents a vulnerability scoring mechanism based on CVSS by analyzing advantages and disadvantages of CVSS and comparing with some improved CVSS-based methods. Our improved scoring mechanism makes the vulnerability evaluating more exactly and effectively, simplifying the process of vulnerability evaluating.**

Keywords- vulnerability evaluation; CVSS; vulnerability metrics

I. INTRODUCTION

In recent years, the number of various software vulnerabilities is rising continuously, which doesn't stop increasing along with the developing of the computer security techniques. Computer security principles, for example, Integrity, Confidentiality and Availability are threatened seriously by all kinds of Trojan and viruses, which attack the computer system through vulnerabilities. In order to defense against all kinds of vicious attacks, reduce the number of vulnerabilities, many security vendors have launched vulnerability detection tools, which scan computer operating system to find existing software vulnerabilities and repair them. Since different vulnerabilities have diverse impacts on computer security, the vulnerability scoring could quantify the potential risks of vulnerabilities commendably. On the basis of scores of vulnerabilities security managers could know the security situation of the host and the entire network more comprehensively. Dynamic configure the vulnerability repair strategy based on making best use of evaluation information of vulnerabilities and set the priority of vulnerability repair according to the risk level. Therefore, the study of vulnerability scoring mechanism is significant to the work of vulnerability assessment and repair.

Currently, there are many kinds of methods for evaluating vulnerability with different evaluation criterion and risk calculation methods. The CVSS almost unifies vulnerability evaluation standard and achieve the compatibility of multiple evaluation systems. This paper, combining with the advantages and disadvantages of CVSS, proposes an improved CVSS-based vulnerability scoring mechanism. This mechanism exploits the vulnerability information in existing vulnerability databases, references mathematical methods to quantify the vulnerability risk level and facilitate the process of vulnerability evaluation. Through the improved evaluation method we could obtain more accurate risk level of vulnerabilities to guide the strategy of vulnerability repair and enhance safety factor of hosts.

II. CVSS (COMMON VULNERABILITY SCORING SYSTEM)

CVSS is an open and free vulnerability evaluation criteria launched by NIAC and FIRST, has become the industry standard supported by most vendors. It solves the problem of chaos in the process of vulnerability evaluation, gives a concise vulnerability evaluation model, unifies the evaluation criteria and makes the majority of security information be compatible.

At present, CVSS has grown to 2.0 version. CVSS is composed of three metric groups: Base, Temporal and Environmental, each consisting of a set of metrics is shown in Fig. 1.

Base metric group represents the inherent and basic characteristics of a vulnerability which are not changed over time or environments. Temporal metric group represents the characters of a vulnerability that are changed over time. Environmental metric group represents the characters of a

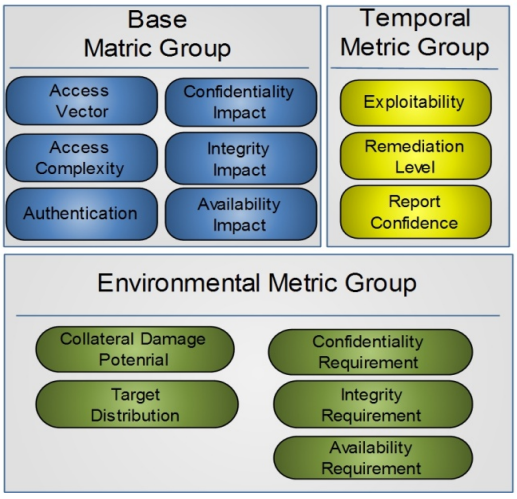

Figure 1. CVSS metric groups

978-0-7695-4559-2/11 $26.00 © 2011 IEEE
DOI 10.1109/MINES.2011.27

IEEE computer society

vulnerability that are relevant to the specific user's environment[1].

Scoring equations and algorithms for CVSS metric groups are shown below.

The base equation is:

$$V_B = (0.6 \times I + 0.4 \times E - 1.5) \times f(I) \quad (1)$$

$$I = 10.41 \times (1 - (1 - I_C)) \times (1 - I_I) \times (1 - I_A)$$

$$E = 20 \times AV \times AC \times Au$$

$$f(I) = \begin{cases} 0 & I = 0 \\ 1.176 & I \neq 0 \end{cases}$$

Here, I_C (Confidentiality Impact), I_I (Integrity Impact), I_A (Availability Impact), AV (Access Vector), AC (Access Complexity), Au (Authentication)

The temporal equation is:

$$V_T = V_B \times TE \times RL \times RC \quad (2)$$

Here, TE (Exploitability), RL (Remediation Level), RC (Report Confidence)

The environment equation is:

$$V_E = (A_T + (10 - A_T) \times CDP) \times TD \quad (3)$$

$$A_T = V_{B'}^{'} \times TE \times RL \times RC$$

$$V_B^{'} = (0.6 \times I^{'} + 0.4 \times E - 1.5) \times f(I)$$

$$I^{'} = \min(10, 10.41 \times (1 - (1 - I_C \times CR) \times (1 - I_I \times IR) \times (1 - I_A \times AR)))$$

Here, CDP (Collateral Damage Potential), TD (Target Distribution), CR (Confidentiality Requirement), IR (Integrity Requirement), AR (Availability Requirement)

Since the temporary and environment scores are changing with time and environment change, the scoring process of them is so subjective that the use of mathematical methods is difficult to quantify the metric factors. Meanwhile, the temporal and environment metric score of one host have no reference value for another host, therefore, most of the vulnerability databases only provide the base score of CVSS and don't use the temporal and environment score, which will impact the accuracy of vulnerability evaluation no doubt and even the future security deployment of network.

III. A NEW IMPROVED CVSS-BASED VULNERABILITY EVALUATION MECHANISM

Based on the above analysis, we find the main difficulties of these evaluation methods are that some subjective evaluation factors are too difficult to be quantified. So, these methods are not practical in the automatic vulnerability evaluation systems. This paper proposes an improved CVSS-based vulnerability scoring method by analyzing the advantages and disadvantages of the above vulnerability evaluation methods. Since the environment metrics in CVSS are so subjective that we can't be quantified easily, this improved method are more objective and easier to quantify, which discards some subjective factors such as environment metric group and adds some metric factors that can reflect the host environment.

A. Base Metrics

Host Environment item is added into base metric group, as shown in TABLE Ⅰ, which includes two evaluation elements: Server Type and OS Type.

Evaluation factors in Host Environment are described in detail below:

1) Server Type

Server Type evaluates the services provided by the host, which affects the importance and status of a host in the network directly. Server Type has three optional items: Common Client, Business Host and Server Host. If the host provides one or more important services, like WWW service, FTP service and SMTP service, which involve large amounts of data storage and some user information, requiring the highest security, then set it high level: Server Host. If the host is business endpoint which deals with business data frequently and requires higher confidentiality and integrity, it is set medium level: Business Host. If the host is a common client, and doesn't involve some important data processing and communications, it is set low level: Common Client.

2) OS Type

OS Type represents the operation system of a host. Many vulnerabilities are correlate to operation system. For example, the security of windows operation systems is worse comparing with other operation systems in consequence of vulnerabilities. Other non-windows operation systems, like Linux, have the higher relative security than windows. Therefore, according to the different operation systems, there are three optional cases:

a) Non-windows OS like Linux

b) Windows OS

c) Windows and other non-windows OS

The calculation process of improved base score is that the weighted values of Impact, Exploitability and Host Environment three parts are calculated to get a base score from 0 to 10. The base scoring equation is as follows:

TABLE I. METRIC FACTORS IN HOST ENVIRONMENT

Host Environment factors			
Metric	Description	Metric Value	Reference Value
Server Type	Type of host status	Common Client/ Business Host/ Server Host	0.5/0.8/1.0
OS Type	OS of host	Linux system/ Only windows system/ Windows and other systems	0.6/0.9/1.0

$$V_B^{'} = (\alpha \times I + \beta \times E + \gamma \times HS - \delta) \times f(I) \quad (4)$$

$$I = \lambda \times (1 - (1 - I_C)) \times (1 - I_I) \times (1 - I_A)$$

$$E = \mu \times AV \times AC \times Au$$

$$HS = \nu \times ST \times OT$$

$$f(I) = \begin{cases} 0 & I = 0 \\ 1.176 & I \neq 0 \end{cases}$$

Here, α is the weighted value which Impact factors account for the base metrics. β is the weighted value which Exploitability factors account for the base metrics. γ is the weighted value which Host Environment factors account for the base metrics. According to experience analysis and calculation, we respectively adjust the value of α, β, γ is 0.4，0.4，0.2. Reference CVSS 2.0 score model, as the fraction of base evaluation, δ is set 1.5. λ is the influence weight of Impact factors and the value is 10.41. μ is the influence weight of Exploitability factors and the value of it is 20. ν is the influence value of Host Environment factors whose value is set 10 generally according to empirical analysis and calculation. The meaning of other items references CVSS 2.0 score system.

B. Temporal Metrics

The temporal score uses the original temporal metric group of CVSS 2.0. However, the CVSS only gives some temporal evaluation elements and evaluation criteria, doesn't give the specific quantification method of each element. Some vulnerability databases only use base score and discard the temporal score, and the others could not get an objective score using temporal score. Therefore, we introduce a score method proposed in [3] which uses model in [4] to calculate the temporal score. Exploitability element in temporal metric group represents the exploit code of vulnerability. According to [4] research, the exploit code of vulnerability meets the Pareto distribution, so Exploitability factor could be calculated by the following equation:

$$TE^{'} = 1 - \left(\frac{k}{x}\right)^{a} \quad a = 0.26, k = 0.00161 \quad (5)$$

In the equation, x is the time span from the vulnerability discovered to now.

Through researching large number of vulnerabilities, In [4] Frei et al. found that the fix of the vulnerability meets the Weibull distribution. So we could use the following equation to calculate Remediation Level:

$$RL^{'} = 1 - \exp\left(-\frac{x}{\lambda}\right)^{k} \quad \lambda = 0.209, k = 4.04 \quad (6)$$

Here, x is the time when the vulnerability has been discovered.

Since there isn't available mathematical method to score Report Confidence and CVSS specifies the default state of these data points as "Not defined", its omission does not affect the outcome of the scoring.

The temporal scoring equation is:

$$V_T^{'} = V_B^{'} \times TE^{'} \times RL^{'} \times 1.0 \quad (7)$$

Through improving CVSS score system, we take temporary score as the final score of vulnerability risk level, which is more accurate and authentic to reflect the current state of vulnerability.

According to temporal score of vulnerability, four risk levels are defined as:

- Low, temporal score as 0.0~2.9.
- Medium, temporal score as 3.0~5.9.
- High, temporal score as 6.0~8.9.
- Critical, temporal score as 9.0~10.0.

IV. EXPERIMENTS AND ANALYSIS

In this section, we use the improved vulnerability evaluation mechanism in the previous section to score the specific vulnerability, demonstrate the evaluation process, and analyse the accuracy and effectiveness of the improved evaluation mechanism by comparing with the original CVSS score.

For example, CVE-2002-0392: Apache httpd Chunked encoding vulnerability.

According to the improved method, the specific evaluation process is as TABLE □.

Through (6) we come to base score:

Base Score = 8.3

CVE-2002-0392 was published on the March 7, 2002. According to probability model in [4], we come to Exploitability probability: *F(Ex)* = 0.98, then, referencing to CVSS Temporal metrics, we obtain Temporal Exploitability: *TC* = 1.00 that belongs to high level.

Through calculation remediation probability of CVE-2002-0392 is *F(RL)* = 0.99, referencing to CVSS Temporal

TABLE II. SCORES OF BASE METRICS

Metrics	*Value*	*Score*
Access Vector	Network	1.0
Access Complexity	Low	0.71
Authentication	None	0.704
Confidentiality	Partial	0.275
Integrity	Partial	0.275
Availability	Partial	0.275
Server Type	Server Host	1.0
OS Type	Windows and other OS	1.0

metrics, we obtain: *Remediation Level* = 0.87 that belongs to official-fix level.

Through above calculation, V_T = 7.2, considering to the above four risk levels we proposed, CVE-2002-0392 is a high risk vulnerability.

By above vulnerability evaluation results we find that the base score of CVE-2002-0392 is 0.8 points greater than the original base score 7.5 in NVD, that's because Server Type and OS Type factors are added into CVSS base metrics and impact the evaluation results. Since CVE-2002-0392 is a vulnerability of apache server software and apache server supports multi-platform, Server Type takes the maximum value: 1.00, OS Type takes the maximum value: 1.00, too. Therefore, Server Type and OS Type make the base score increase. Temporal score used as the final vulnerability evaluation score is 1.1 points greater than the original CVSS score, since CVE-2002-0392 has been published for a long time, using probability model in [4] (5)(6) Exploitability and Remediation probabilities are close to 1.0

We score some vulnerabilities discovered in 2010 and compare the improved scores with the original scores of these vulnerabilities. The results are shown in Fig. 2.

In Fig. 2, we found some improved scores are lower than original scores, since in the improved score process we consider Server Type and OS Type factors, meanwhile, the improved scores use temporal scores as the final evaluation scores which are closer to the real-time risk situation than before. At the same time, we note that the score of CVE-2010-3937 is a little greater than before, since CVE-2010-3937 is a vulnerability on Microsoft Exchange Server, whose Server Type is Server Host. Once CVE-2010-3937 is exploited, the risk of host and network is increasing. As a whole, the scores of vulnerabilities haven't changed very much, however, these subtle changes are likely to lead to risk level changes, further may impact on the configuration

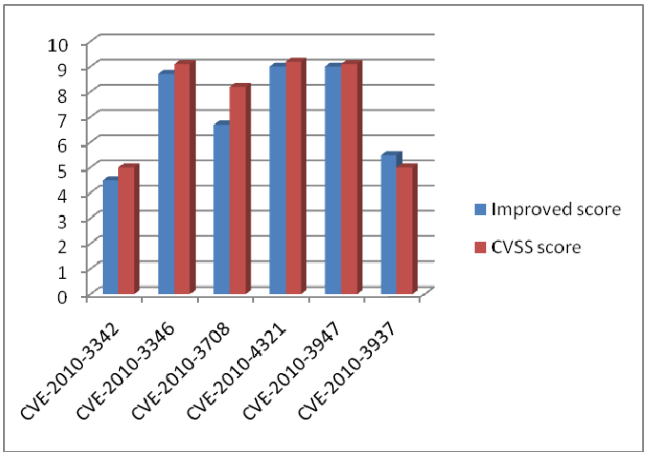

Figure 2. The comparison of scores

of repair strategy. Therefore, the accurate vulnerability assessment has more important guiding significance to repair work.

V. SUMMARY

Based on the study and analysis of CVSS evaluation method, this paper proposes an improved CVSS evaluation method, which avoids the subjective and indeterminable factors in CVSS, quantifies the fuzzy temporal factors, discards the uncertain environment evaluation and add the evaluation factors reflected host state in base metrics. The improved evaluation mechanism takes temporal score as vulnerability risk level score and reflects the state changes of vulnerability. The experimental results show that the improved evaluation mechanism is more accurate and credible. It could be foreseen that the accurate assessment has the vital significance.

ACKNOWLEDGMENT

This work is partially supported by the "13115"scientific and technological innovation program of Shaanxi Province under Grant No.2009FWPT-06; the key projects of International cooperation of Shaanxi Province under Grant No.2010kw-04; the National Natural Science Foundation of China under Grant No.61070177; the Department of Education research project of Shaanxi Province under Grant No.2010JK864.

REFERENCES

[1] P. Mell, K. Scarfone, S. Romanosky, "A complete guide to the Common Vulnerability Scoring System version 2.0," [cited 5 May 2011]. Available from URL: http://www.first.org/cvss/cvss-guide.pdf.

[2] Wang Qiu-yan, ZHANG Yu-qing, "Common Vulnerability Rating Method," Computer Engineering, vol. 34, No. 19, October 2008.

[3] C. Frühwirth, T. Männistö, "Improving CVSS-based vulnerability prioritization and response with context information," Third International Symposium on Empirical Software Engineering and Measurement, IEEE, 2009, pp. 535-544.

[4] S. Frei, M. May, U. Fiedler, B. Plattner. "Large-Scale Vulnerability Analysis," SIGCOMM' 06 Workshops, 2006, pp. 131-138.

[5] O. H. Alhazmi, Y. K. Malaiya. "Quantitative vulnerability assessment of systems software," Reliability and Maintainability Symposium, 2005, pp. 615-620.

[6] K. Scarfone, P. Mell. "An Analysis of CVSS Version 2 Vulnerability Scoring," Third International Symposium on Empirical Software Engineering and Measurement, IEEE, 2009, pp. 516-525.

[7] V. Sridharan, D. R. kaeli. "Quantifying Software Vulnerability," WREFT'08, 2008, pp. 323-328.

[8] G. Vache. "Vulnerability Analysis for a Quantitative Security Evaluation," Third International Symposium on Empirical Software Engineering and Measurement, IEEE, 2009, pp. 526-534.

[9] K. Scarfone, P. Mell. "Vulnerability Scoring for Security Configuration Settings," QoP'08, 2008, pp. 3-7.