Study on the Distribution of CVSS Environmental Score

Han LI
National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)
Beijing, China
lihan@cert.org.cn

Rongrong XI
Institute of Information Engineering, Chinese Academy of Sciences
Beijing, China
xirongrong@iie.ac.cn

Li ZHAO
School of Information Technology and Engineering, Jinzhong University
Jinzhong, Shaxi province, China
ldzhaoli@163.com

Abstract—**This paper focuses on analyzing the distribution of CVSS environmental score. Firstly we extract CVSS base score from the NVD database and calculate their corresponding environmental score by simulating all possible combinations of different environmental metrics, then analyze the distribution of the environmental score. Two conclusions are obtained: first, for any given vulnerability, there exists a mode value among all its possible environmental scores; second, the relationships between the maximum decrease or increase of the environmental score and the base score fits particular functions. Finally we use three vulnerabilities provided by NVD as a case study to verify the conclusions proposed in this paper.**

Keywords-Common Vulnerability Scoring System; Environmental Score distribution; Mode; Maximum deviation

I. INTRODUCTION

The Common Vulnerability Scoring System (CVSS) [1, 2] is the most widely accepted quantitative standard for network vulnerabilities measurement. It provides a metric for evaluating the severity of vulnerabilities. The most prominent application is in the National Vulnerability Database (NVD) of the National Institute of Standards and Technology (NIST) of the U.S.. The NVD is a public directory of software vulnerabilities and serves as one of the standard data-sources for security management applications. The NVD employs the CVSS Base-Metric as a severity indicator for all recorded vulnerabilities. However, the Environmental metrics are omitted. Since the Base-Metric is unaware of an organization's contexts, the NVD scoring alone is of limited use for vulnerability evaluation in practice [3].

To fill this kind of missing information, one would normally have to collect them from other sources. In practice, however, collecting these data from secondary sources represents a significant organizational or financial effort. Moreover, the environmental metric is usually associated with user's IT environment, it is often impossible to collect information from other sources. In this paper, we will consider the missing context information by studying the distribution and statistical features of the quantified environmental information to improve the quality of CVSS-based vulnerability evaluation.

II. ENVIRONMENTAL METRICS

Environmental metrics [4] group contextualizes vulnerability, thus reflecting the imminent threat to a particular environment. Three different environmental characteristics of vulnerability are measured, namely (1) Collateral Damage Potential (CDP), which measures the degree of loss to information, revenue, life or physical assets through damage as a result of exposure to a particular vulnerability; (2) Target Distribution (TD), which measures the percentage of systems within a particular environment affected by the vulnerability; (3) Three security requirements, i.e., Confidentiality Requirement (CR), Integrity Requirement (IR), and Availability Requirement(AR) impacts. These three characteristics above are helpful to customize CVSS Environmental Score depending on the requirement of affected IT assets relative to confidentiality, availability, and integrity within the user's organization. Their values are shown in Table 1 [1].

III. ENVIRONMENTAL SCORE DISTRIBUTION ANALYSIS

Ref. [3] provides the mathematical relation between CVSS Base Score and Environmental Score. For any given base score value, there are total 5 environmental metrics to be determined for environmental score calculation and each metric has multiple values as shown in table 1. It can be concluded that there are 1920 possible combinations of values for 5 metrics, which could result in 1920 possible corresponding environmental scores. Furthermore, with values for *Not Defined* ruled out, 540 valid environmental score values can be obtained[5]. By simulating 540 different combinations of values of 5 metrics, we can observe different change added to the base score to gain different environmental scores.

This work was supported by Youth Fund 2014QN-34 of CNCERT/CC

978-1-4799-7284-5 /15/$31.00 ©2015 IEEE

TABLEI CVSS ENVIRONMENTAL METRICS

Collateral Damage Potential (CDP)	***None***	N	0.00
	Low	L	0.10
	Low-Medium	LM	0.30
	Medium-High	MH	0.40
	High	H	0.50
	Not Defined	ND	0.00
Target Distribution (TD)	***None***	N	0.00
	Low	L	0.25
	Medium	M	0.75
	High	H	1.00
	Not Defined	ND	1.00
Confidentiality (CR) Integrity (IR) Availability (AR)	***Low***	L	0.50
	Medium	M	1.00
	High	H	1.51
	Not Defined	ND	1.00

Rather than show all obtained results through simulations, we demonstrate two major observations for environment score that stand out in this research, namely:

- The distribution of the mode.
- The distribution of the maximum deviation.

As an example, we simulate 540 possible value combinations for 5 environmental metrics when base score value is selected 5.75 to illustrate their impacts. Outcomes are shown in Fig. 1.

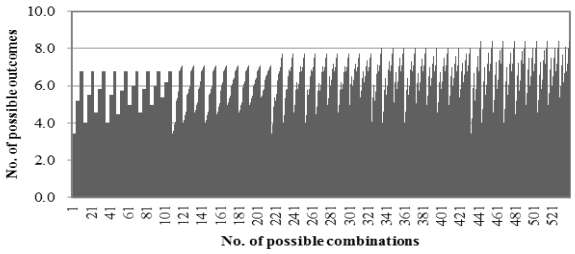

Figure1. Impact of different values for environmental metrics on the selected base score 5.75 when exploitability is 3.9 and impact subscore is 8.54

Fig. 1 shows that given base score being 5.75, its CVSS environmental score can possibly be as high as 8.39, and as low as 3.4. Figure 1 also shows that there are many duplicate values. By filtering and refinement, 113 valid values are obtained. Their distribution is shown in Fig. 2.

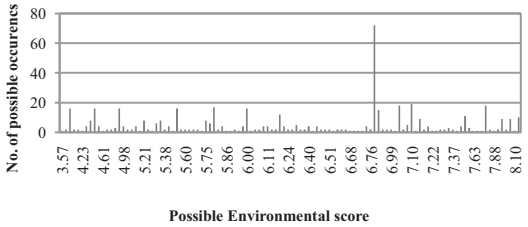

Figure2. Distribution of environmental scores given base score being 5.75

Fig. 2 shows that there exist a value of 6.77, which is repeated 72 times, or the most, among possible environment scores. That is to say, 6.77 is the mode of the set of all possible Environmental Score values. Through further simulations, we find that there exists a mode of the corresponding Environmental Score values for every CVSS Base Score value. Their distribution status is shown in Fig. 3.

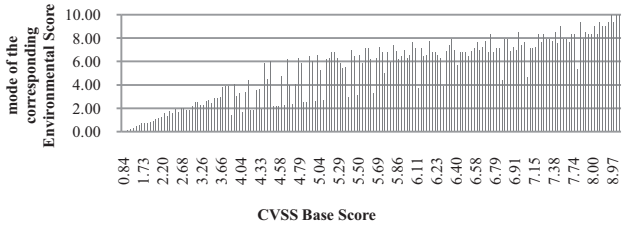

Figure3.The distribution of the modes of the corresponding Environmental Score values

For further analysis, we use fitting method to give function that matches this distribution. We try to fit commonly-used polynomial function to the data, i.e.:

$$Mode(x) = \alpha x + \beta \tag{1}$$

Where x represents CVSS Base Score value; α is selected 1.342 and β selected -1.051 which makes the fit the best match.

This research further investigates the maximum deviation of the Environmental Score. We calculate the maximum increase and the maximum decrease quantity of the Environmental Score for all possible CVSS Base Score values. Results are depicted in Fig. 4.

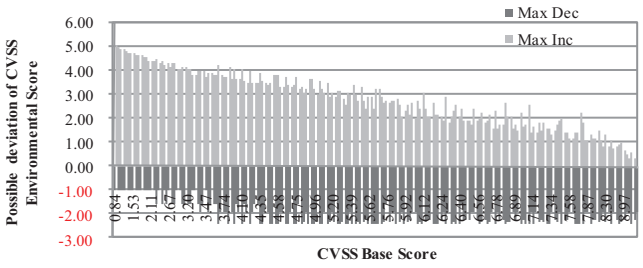

Figure4. Distribution of maximum deviation of the Environmental Score

Fig. 4 shows that the maximum increase quantity gradually reduces as CVSS Base Score increases, while the maximum decrease value remains a relative constant. From Figure 5, we can conclude that for lower vulnerabilities (Base Score 0 ~ 3.9), the maximum decrease value is maintained at around -1.01, for higher vulnerabilities (4 ~ 10), the value is approximately -2.424. So the maximum decrease trends can be described by Eq.(2).

$$Max_{dec.}(x) = \begin{cases} -1.01 & x < 4 \\ -2.424 & x \geq 4 \end{cases} \tag{2}$$

Where x also denotes the CVSS Base Score value.

On the other hand, the maximum increase value reduces from 5.084 to 0.003. Its trend is similar to the logarithmic

curve. By data fitting, we find that the maximum increase trend follows the Eq. (3):

$$Max_{Inc.}(x) = -k\ln(x) + \lambda \quad (3)$$

Where x is the CVSS Base Score value; k=2.256 and λ =6.4363.

In summary, we observe distributions of the modes and maximum deviations show predictable regularity. Conclusions are drawn as follows:

- For any given vulnerability, its possible CVSS Environmental Score values are not uniformly distributed within the interval, and there is a mode value whose occurrence is much more than that of any other value. This mode value can be estimated by Eq.(1).
- For any given vulnerability, with the increase of Basic Score value, the increase of its Environmental Score is weakened. That is the lower the Basic Score is, the greater its Environmental Score increase and the more environment impact it shows. The maximum increase of Environmental Score can be estimated by Eq.(3).
- If user environment leads to the decrease of vulnerability severity, there are normally two cases. For any lower severity vulnerabilities (Basic score value between 0 and 3.9), its maximum decrease value is approximately 1.01; for any higher vulnerability severity, its maximum decrease value is about 2.424.

IV. EXPERIMENT

In this section, three vulnerabilities extracted from NVD database [6] are analyzed to verify our conclusions. For general purpose, we extract three different severity vulnerabilities: high, medium and low. Table 2 gives more details about their basic quantitative indices. The distributions of their possible Environmental Score values are depicted in Figure 5 ~ 7 respectively.

TABLEII THREE VULNERABILITIES IN NVD AS SUBJECTS

CVE-ID	Base Score	Impact Subscore	Exploitability SubScore	Security Impact
CVE-2013-0648	9.3	10	8.6	C:C/I:C/A:C
CVE-2013-0708	4.3	2.9	8.6	C:N/I:P/A:N
CVE-2013-0162	2.1	2.9	3.9	C:N/I:P/A:N

Figs. 5-7 show that there exist the modes, the maximum increase, and the maximum decrease among their possible Environmental Score values. These values are then compared with the values calculated by our empirical equations given in section III. The results are shown in Table III.

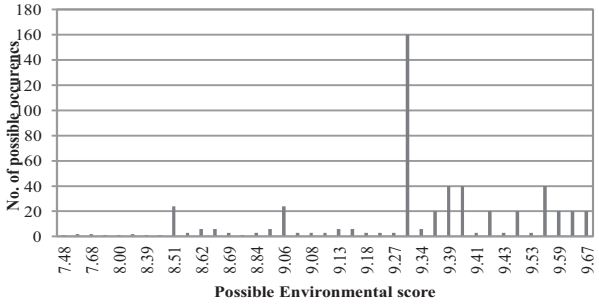

Figure5. The distribution of simulated environmental score of CVE-2013-0648

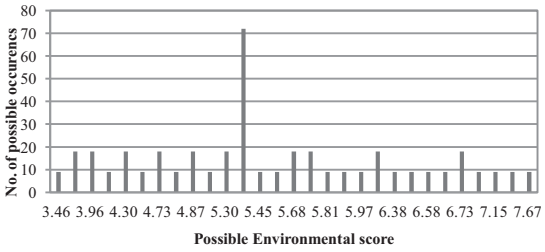

Figure6. The distribution of simulated environmental score of CVE-2013-0708

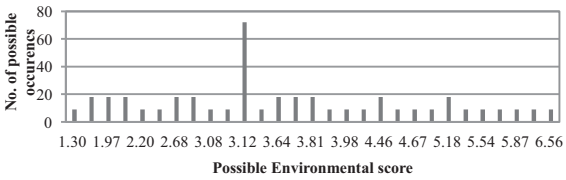

Figure7. The distribution of simulated environmental score of CVE-2013-0162

TABLEIII RESULTS OF CASE STUDY ON THREE VULNERABILITIES IN NVD

CVE-ID	Base score	Environmental score					
		Maximum Decrease		*Maximum Increase*		*Mode*	
		Real value	*Calculated value*	*Real value*	*Calculated value*	*Real value*	*Calculated value*
CVE-2013-0648	9.3	6.92	**6.88**	9.67	**11.5**	9.34	**11.42**
CVE-2013-0708	4.3	2.09	**1.88**	7.67	**9.73**	5.33	**4.71**
CVE-2013-0162	2.1	1.08	**1.09**	6.56	**8.10**	3.12	**1.76**

In Table III, we find that:

(1) The maximum decrease value is consistent with the real value. It can be correctly estimated by the Base Score value using Eq. (2).

(2) The maximum increase value is slightly deviated from the real value. Their calculated values

are bigger than the real values. Specially, for CVE-2013-0648, the calculated maximum increase value (11.5) is out of CVSS score range (≤ 10). It implicates that although Eq. (2) may be acceptable, it still needs further improvement.

(3) Mode values practically exist for all three vulnerabilities. However, they are inconsistent with the calculated values. For CVE-2013-0648, its calculated mode is 11.42 and is also out of CVSS score range. We will analyze the mode from other perspectives and improve the estimation method in the future work.

V. CONCLUSION

In this paper, we study the impacts of Environmental Score by simulating all possible combinations of different environmental metrics based on different CVSS Base Score values. The distribution and some statistical features of Environmental Score values are analyzed. Equipped with the conclusions summarized in this paper, one can try to quantitatively estimate the impact of environmental metrics on vulnerability severity. Based on these studies, network administrators can have a high-level view with the impact of environmental metrics, thus determine the priority of processing different vulnerabilities and take appropriate mitigation measures to ensure network security.

REFERENCES

[1] Scarfone K, Mell P. An analysis of CVSS version 2 vulnerability scoring. In: Proceeding of the 3rd International Symposium on Empirical Software Engineering and Measurement, IEEE, 2009, 516-525.

[2] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system. Security & Privacy, 2006, 4(6). 85-89

[3] Gallon L. On the impact of environmental metrics on CVSS scores. In: Proceedings of the Second IEEE International Conference on Social Computing. IEEE, 2010, 987-992.

[4] Mell P, Scarfone K, Romanosky S. A complete guide to the common vulnerability scoring system version 2.0. In: Proceedings of the FIRST-Forum of Incident Response and Security Teams. 2007, 1-23.

[5] Ali A, Zavarsky P, Lindskog D, et al. A software application to analyze the effects of temporal and environmental metrics on overall CVSS v2 score. In: Proceedings of the 2011 World Congress on Internet Security. IEEE, 2011, 109-113.

[6] National Vulnerability Database, http://nvd.nist.gov/, 2015.