SCIENCE CHINA
Information Sciences

• LETTER •

March 2019, Vol. 62 039102:1–039102:3
https://doi.org/10.1007/s11432-017-9445-4

A revised CVSS-based system to improve the dispersion of vulnerability risk scores

Chensi WU[1], Tao WEN[2] & Yuqing ZHANG[1,3*]

[1]*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 101408*, China;*
[2]*China Academy of Electronics and Information Technology, Beijing* 100041*, China;*
[3]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China*

Received 19 June 2017/Accepted 19 April 2018/Published online 11 September 2018

Citation Wu C S, Wen T, Zhang Y Q. A revised CVSS-based system to improve the dispersion of vulnerability risk scores. Sci China Inf Sci, 2019, 62(3): 039102, https://doi.org/10.1007/s11432-017-9445-4

Dear editor,

We propose a new vulnerability risk assessment system, CVSS_PCA, for improving CVSS based on principal component analysis (PCA) [1]. With the increasing number of security vulnerabilities, vulnerability risk measurement becomes more significant. For a quantitative evaluation system, vulnerability risk scores should be sufficiently subdivided. The process of quantitative security vulnerability assessment includes: choosing metrics to reflect the impact of the vulnerability, assigning value to these metrics, and integrating these metrics in order to gain the risk score of vulnerability. CVSS (common vulnerability scoring system)[1)] is a quantitative vulnerability assessment system and can score the vulnerability. The score helps us know the priority of vulnerability which will have to be repaired. However, there are some deficiencies in the dispersion of CVSS scores, which affect all these applications based on CVSS directly.

For any assessment system, objectivity and dispersion should be satisfied. Objectivity refers to that the assessment results can well reflect the nature of the practical samples. Dispersion [2] includes the distinguishing degree and the distribution of the results assessed. There are a lot of researches on the objectivity of CVSS [3–6]. However, there are few researches on the dispersion. In fact, because of poor dispersion leading to most of the vulnerabilities accumulation in the few values, the role of dispersion should not be overlooked. In extreme condition, when all vulnerabilities are marked by the same risk value, there is no practical significance even with perfect objectivity. Therefore, the upper limit of objectivity is decided by dispersion. Only in the case that dispersion is natural enough, objectivity would be significant practically.

The contributions of this study are as follows. Please see the Appendix A for the details.

• Based on statistical analysis, we proposed three criteria for metric values:

(1) The probabilities of metric values should be equilibrated;

(2) The total number of metric values should be large enough;

(3) The correlations should be as fewer as possible. The correlations mean the degree of interaction between CVSS metrics, which is the conditional probability distribution of metric values.

The dispersion of vulnerability risk assessment system is affected by the above three criteria, and CVSS does not meet the three criteria largely.

• Correlations between metrics have been analyzed qualitatively and divided into three ranks (strong dependence, weak dependence and no de-

* Corresponding author (email: zhangyq@nipc.org.cn)

1) Common vulnerability scoring system. https://nvd.nist.gov/cvss.cfm.

pendence). The proportions of these three ranks are 28.89%, 45.93%, and 25.18%, respectively, which indicates that the independent CVSS metrics are only a quarter of all cases.

• CVSS is improved based on PCA (principal component analysis) [1], and a new vulnerability risk assessment system, CVSS_PCA, is proposed. CVSS_PCA creates new metrics with linear combination of original CVSS metrics. New metrics can meet the above three criteria largely without changing original CVSS metric values.

• CVSS_PCA has been applied to 40007 vulnerabilities, and compared with CVSS 2.0 and VRSS 2.0 [7]. Experiment results show that better dispersion of risk scores can be achieved, and the distribution pattern is closer to manual marking.

The aims of CVSS_PCA we revising and proposing are as follows:

(a) Equilibrating probability of metric values;

(b) Increasing the number of total metric values;

(c) Reducing the correlation between metrics;

(d) Improving the dispersion of risk scores without undermining the objectivity.

Another advantage of CVSS_PCA is that neither auxiliary information (e.g., CWE categories) nor new metrics are required. CVSS_PCA can be applied to any quantitative vulnerability risk assessment system. CVSS has six base metrics, accessvector, accesscomplexity, authentication, confidentiality, integrity, availability. Eqs. (1)–(4) are the calculation formulas of CVSS 2.0.

$$\begin{aligned}\text{Risk Score} = \text{round}(((0.6 \times \text{Impact}) + (0.4 \\ \times \text{Exploitability}) - 1.5) \\ \times f(\text{Impact})),\end{aligned} \tag{1}$$

$$\begin{aligned}\text{Impact} = 10.41 \times (1 - (1 - C) \times (1 - I) \\ \times (1 - A)),\end{aligned} \tag{2}$$

$$\text{Exploitability} = 20 \times \text{Av} \times \text{Ac} \times \text{Au}, \tag{3}$$

$$f(\text{Impact}) = 0 \text{ if Impact} = 0, 1.176 \text{ otherwise}. \tag{4}$$

Analysis of CVSS dispersion and metrics. From the analysis of vulnerabilities published on NVD, we can find that there are three defects of CVSS, which may contribute to a poor dispersion of risk scores.

• The probabilities of different metric values are uneven, so consequently, the distribution of risk scores is uneven. In fact, an uneven probability may be more objective, but it may deviate from an ideal dispersion. This contradiction needs to be solved.

• The total number of all metric values is so small that the risk scores are concentrated, which lead to a poor dispersion.

• There are obvious correlations between metrics, that is, each metric value is not completely independent. In this case, when combining some specific metrics, the probability of the combination is larger, which leads to be uneven.

These defects also exist in other versions of CVSS, such as 1.0 and 3.0.

Introduction of CVSS_PCA. CVSS_PCA creates new metrics with linear combination of original metrics, instead of creating new metrics. The overall procedure of CVSS_PCA is shown in Figure 1, where the light-colored modules are inherent steps of CVSS 2.0, and the dark-colored modules are new steps of CVSS_PCA. The detailed steps are as follows.

• Step 1. Obtain values of all the six CVSS metrics, e.g., Av = 1.0 and Ac = 0.6. Both CVSS and CVSS_PCA performs this step.

• Step 2. Compute new metrics with PCA. This step can be regarded as a black box. The inputs are six metric values above-mentioned, and the outputs are six transformed metric values, each of which is a linear combination of the original metrics. For example,

$$\begin{aligned}\text{Comp}_{\text{Av}} = \ & x_1 \times \text{Av} + x_2 \times \text{Ac} + x_3 \times \text{Au} \\ & + x_4 \times C + x_5 \times I + x_6 \times A.\end{aligned}$$

x_1–x_6 are coefficients, and they are different for each new metric. This step is the core step of CVSS_PCA.

• Step 3. Normalize the new metrics. The range of new metrics is uncertain, and should be normalized to reach an acceptable range of formulas.

• Step 4. Calculate the impact and exploitability. Put normalized metric values into (2) and (3) to calculate the values of impact and exploitability. Both CVSS and CVSS_PCA performs this step.

• Step 5. Calculate risk score. Put values of impact and exploitability into (1) and (4) to calculate a risk score. Both CVSS and CVSS_PCA performs this step.

• Step 6. Map and normalize CVSS risk scores. According to the order of PCA risk scores obtained in step 5, map the vulnerabilities, which marked by the same CVSS risk score.

Conclusion and future work. In order to reduce the loss caused by vulnerabilities, the risk of vulnerabilities must be evaluated objectively. Based on statistical analysis, three criteria about metric values have been proposed. 40007 vulnerabilities published on NVD have been analyzed in detail, focusing on the objectivity of the CVSS risk scores. There are three defects of CVSS to influence the dispersion of risk scores.

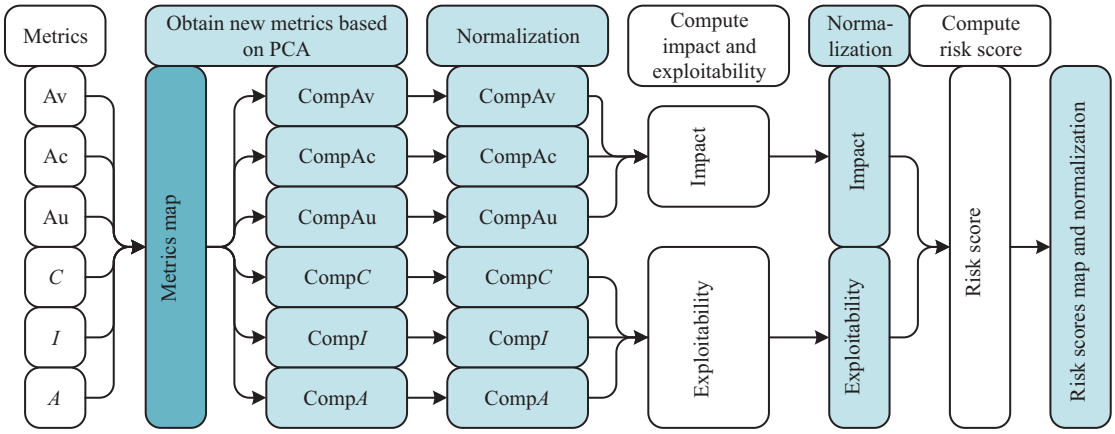

Figure 1 (Color online) Implementation process of CVSS_PCA.

To deal with the poor dispersion of risk scores of CVSS, CVSS_PCA is introduced to further differentiate the vulnerabilities. CVSS_PCA creates new metrics with linear combination of CVSS metrics. Assuming that vulnerabilities [8] marked manually are objective risk assessment, comparisons between CVSS 2.0 and CVSS_PCA show that CVSS_PCA does not undermine the objectivity of CVSS. Actually, the variance of risk scores between CVSS_PCA and manual marking is smaller.

CVSS_PCA directly puts new metrics into the original formulas of CVSS to calculate the risk score. In our future work, we will try to answer the question whether adjusting the formulas is necessary for the objectivity. In addition, we will also focus on the correlation between metrics, and refine more efficient metrics as the inputs.

Acknowledgements This work was supported by National Key R&D Program of China (Grant No. 2016YFB0800700), National Natural Science Foundation of China (Grant Nos. 61572460, 61272481), Open Project Program of State Key Laboratory of Information Security (Grant No. 2017-ZD-01), National Information Security Special Projects of National Development and Reform Commission of China (Grant No. (2012)1424), and Programme of Introducing Talents of Discipline to Universities (111 Project) (Grant No. B16037).

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Shlens J. A tutorial on principal component analysis. 2014. ArXiv:1404.1100
2 Mell P, Scarfone K. Improving the common vulnerability scoring system. IET Inf Secur, 2007, 1: 119–127
3 Holm H, Afridi K K. An expert-based investigation of the common vulnerability scoring system. Comput Secur, 2015, 53: 18–30
4 Fruhwirth C, Mannisto T. Improving CVSS-based vulnerability prioritization and response with context information. In: Proceedings of the 3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, 2009. 535–544
5 Ghani H, Luna J, Suri N. Quantitative assessment of software vulnerabilities based on economic-driven security metrics. In: Proceedings of International Conference on Risks and Security of Internet and Systems, La Rochelle, 2013
6 Keramati M, Keramati M. Novel security metrics for ranking vulnerabilities in computer networks. In: Proceedings of the 7th International Symposium on Telecommunications, Tehran, 2015. 883–888
7 Liu Q X, Zhang Y Q, Kong Y, et al. Improving VRSS-based vulnerability prioritization using analytic hierarchy process. J Syst Softw, 2012, 85: 1699–1708
8 Keramati M. New vulnerability scoring system for dynamic security evaluation. In: Proceedings of the 8th International Symposium on Telecommunications, Tehran, 2017. 746–751