Discussion Topic

Read Spring et al (2021) and then answer the following questions:

1. What characteristics of CVSS do the authors criticise? Do you agree with the critique? Justify your answer with academic references.
2. The authors also discuss a number of alternatives to CVSS. Select one of these alternatives and post an argument for why it should replace CVSS.

Initial Post

by Patricia Lapierre - Saturday, 1 October 2022, 4:05 AM

Collaborative Learning Discussion 2

Common Vulnerability Scoring System (CVSS) is a risk assessment based on a scoring method. The latest version, v3.0, is constituted of eight questions that can be answered by a scale from "0 to 10 in 1/10 increments" (Spring *et al.*, 2021). According to the authors, Spring *et al*., the CVSS 'qualitative' risk assessment has strong weaknesses has it has been "designed to identify the technical severity of a vulnerability" (*Ibid*). The authors argue that this method was never intended to be used by enterprises to evaluate organisational security, as technical vulnerabilities are not the only reasons for security incidents. The paper lists three main problems with CVSS: it overlooks the context, it disregards material consequences of the vulnerability, it has "operational scoring" issues. On the last critic, Kai *et al.* (2021) underlines that CVSS relies on people perceptions of vulnerabilities, which impacts the final score. Also, according to them, "the weight of CVSS metrics is more subjective" increasing the chance of scoring error (Kai *et al.*, 2021: 25). Another issue of the CVSS risk assessment method, highlighted by Goohs *et al.* (2022), is the fact that this model presents detailed information about exploitable vulnerabilities for potential malicious individuals to use on unpatched organisations.

Spring *et al.* (2021) suggests using Stakeholder-Specific Vulnerability Categorization (SSVC) model to execute risk assessments. The paper argues that in order to be scientifically accurate, it is necessary to involve stakeholders in the evaluation, which in turn, will benefit the decision-making process. Furthermore, Kioskli & Plemi (2022) reiterates the mistake of CVSS in not including human factor in the development of the model. In their paper, they present a cybersecurity scoring system based on attackers' profile that they consider should be included in the "Environmental Metric Group of the CVSS3.1" (*Ibid*, 2022: 146). By including cyberpsychology metrics in the CVSS model, there is a strong believe that the estimates will be more accurate, which in turn will better protect organisations who use CVSS.

References

Goohs, J., Mier, R., Deist, P., & Casey, W. (2022). Reducing Attack Surface by Learning Adversarial Bag of Tricks.

Kai, S., Zheng, J., Shi, F., & Lu, Z. (2021, December). A CVSS-based Vulnerability Assessment Method for Reducing Scoring Error. In *2021 2nd International Conference on Electronics, Communication, and Information Technology (CECIT)*, 25-32. IEEE.

Kioskli, K., & Polemi, N. (2022). Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores.

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021). Time to Change the CVSS?. *IEEE Security & Privacy*, 19(2), 74-78.

Summary post

by Patricia Lapierre - Sunday, 30 October 2022, 4:49 AM

After reading the comments, it seems evident that my initial post was very insightful. My peers agree with me about the fact that CVSS is a qualitative risk assessment and not a quantitative one. This posture is justifiable on the fact that this is a scoring method based on subjective perception of risks by individuals. As Doynikoca & Kotenko (2017) suggest, there are some probabilistic methodologies that could ensure a better quantitative risk assessment than CVSS. Also, as I mentioned previously, CVSS has some questionable calculation formula as highlighted in the article by Spring et al (2021).

Finally, there seems to have three different options to run a better alternative to CVSS v3.0. The first one is the Stakeholder-Specific Vulnerability Categorization (SSVC). This methodology takes in account stakeholders' perception of risk as bonfires to the assessment. The second option is the inclusion of the cyberpsychology metrics in the CVSS model (Kioskli & Plemi: 2022). Lastly, there is the possibility to assess risks through probabilistic technique, like Monte Carlo and the Baysian Theorem.

References:

Doynikova, E., & Kotenko, I. (2017, March). CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)* (pp. 346-353). IEEE.

Kioskli, K., & Polemi, N. (2022). Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores.

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021). Time to Change the CVSS?. *IEEE Security & Privacy*, 19(2), 74-78.