Discussion Forum 2 Unit 7-9

Initial Post:

In their article "Time to Change the CVSS?" Spring et al. (2021) offer a critique of the Common Vulnerability Scoring System (CVSS). They highlight the following issues:

- CVSS focuses too much on static metrics that do not account for real-time, dynamic risks.
- The scoring system lacks granularity, which may result in oversimplified vulnerability assessments.
- CVSS translates qualitative responses into numerical values.
- The rigid structure of CVSS can lead to inaccurate risk evaluations for specific organizational contexts.

I agree with this critique, as numerous studies have highlighted CVSS's limitations in accurately conveying real-world risk. As threats change over time, the rigid structure of CVSS cannot keep pace, leading to outdated or inappropriate risk evaluations. Venkataramanan et al. (2019) propose the Cyber-Physical Resiliency Metric (CPRM), an enhancement of CVSS designed to measure the impact of cyber vulnerabilities on microgrid resilience. CPRM provides real-time score adjustments as attacks unfold, such as during privilege escalation, allowing for immediate operator intervention. In their case study on the Ukraine power grid cyber-attack, CPRM improved the MoD Impact score from 6.4 (CVSS) to 7.1, demonstrating a more dynamic and context-specific approach to vulnerability management (Venkataramanan et al., 2019).

One alternative discussed by Spring et al. is the Stakeholder-Specific Vulnerability Categorization (SSVC) system. SSVC emphasizes tailored decision-making processes based on specific stakeholder priorities, making it more flexible than CVSS. This framework encourages to weigh factors like exploit maturity, potential impact, and mission relevance before acting. SSVC's focus on stakeholder-specific needs, rather than generic metrics, allows organizations to better align security measures with their unique risk profiles. This adaptability makes it a strong candidate to replace CVSS, especially for organizations seeking a more nuanced and dynamic approach to vulnerability management (Spring et al., 2021).

Word count: 285

References:

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021) Time to Change the CVSS? *IEEE Security and Privacy 19*(2): 74–78. DOI: **https://doi.org/10.1109/MSEC.2020.3044475**

Venkataramanan,V. et al. (2029) Measuring and Enhancing Microgrid Resiliency Against Cyber Threat, *IEEE Transactions on Industry Applications* 55(6): 6303-6312. Doi: 10.1109/TIA.2019.2928495.

Respond Post 1:

Thank you, Tobi for your valid points.

Several measures could have been implemented to improve CVSS. One critical area for improvement is enhancing the transparency and empirical foundation of CVSS. As Spring et al. (2021) and you criticized, the current CVSS process lacks transparency and relies on an incomprehensible formula. By adopting more data-driven models, organizations could better prioritize vulnerabilities and improve risk management. A more open and well-documented process would allow stakeholders to trust vulnerability scores, reducing the risk of misinterpretation. The Stakeholder-Specific Vulnerability Categorization (SSVC) framework provides a viable alternative by tailoring decisions to organizational contexts and using decision trees for more flexible responses (Householder et al., 2021).

Moreover, regular updates to vulnerability scoring systems are crucial. CVSS v4.0, released in 2023, attempts to address some of these issues, making the system more adaptable to real-world decision-making (Red Hat, 2023). However, as Scip AG (2023) points out, even CVSS v4.0 has limitations—such as insufficient differentiation between vulnerability severity in complex environments. This raises the question: are incremental updates enough, or does the industry need a complete overhaul of how we evaluate vulnerabilities?

In summary, greater transparency, context-specific assessment tools like SSVC, and continuous updates are essential measures that could have prevented many critique points while improving overall security outcomes.

Word count: 212

References:

Householder, A. D., Wassermann, G., Manion, A., & King, C. (2021) Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization. Carnegie Mellon University. Available from: https://insights.sei.cmu.edu/library/prioritizing-vulnerability-response-a-stakeholder-specific-vulnerability-categorization/ [Accessed 19 September 2024].

Red Hat. (2023) FIRST Announces CVSS v4.0 Release. Available from: https://www.redhat.com/en/blog/first-announces-cvss-v40-release [Accessed 19 September 2024].

Scip AG. (2023) CVSS v4.0 – Better than v3.1? Available from: https://www.scip.ch/?labs.20240314 [Accessed 19 September 2024].

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021) Time to Change the CVSS? *IEEE Security and Privacy 19*(2): 74–78. DOI: **https://doi.org/10.1109/MSEC.2020.3044475**

Respond Post 2:

Hi Mark,

You've made some great points about the practical use of the Common Vulnerability Scoring System (CVSS), especially when presenting risks to top-level management. I agree that the simplicity of an integer score can be incredibly effective for communicating complex technical risks to non-technical stakeholders. It provides a clear, quantifiable metric that helps decision-makers see the value of risk mitigation efforts, which aligns well with established risk management frameworks (NIST, 2018).

However, I think Spring et al. (2021) are right in pointing out that CVSS has significant limitations, particularly the lack of context and consideration of material consequences. While you've illustrated how organizations like Varian adjust CVSS to their own environments, this requires a level of customization that smaller organizations or less experienced teams may not have the resources to perform. The issue with relying too heavily on CVSS alone is that it can lead to oversimplification of risks, which may not always capture the full impact on a specific business sector.

I also agree with Spring et al.'s (2020) argument that risk assessment should focus on actionable categories rather than just severity scores. While CVSS does a good job of highlighting the "what" (i.e., the severity of the vulnerability), it doesn't always address the "how" and "what next" in terms of specific actions organizations should take. This is where something like SSVC could add value by providing clearer guidance on prioritization.

So, while CVSS is useful, especially when combined with internal context, it could benefit from being part of a broader, more flexible framework like SSVC to avoid oversights.

Word count: 261

References:

NIST (2018) *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1) DOI: https://doi.org/10.6028/NIST.CSWP.04162018

Spring, J., Hatleback, E., Householder, A. (2020) *A Stakeholder-Specific Vulnerability Categorization.* [Podcast]. Available from: https://insights.sei.cmu.edu/library/a-stakeholder-specific-vulnerability-categorization/ [Accessed 22 September 2024]

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021) Time to Change the CVSS? *IEEE Security and Privacy 19*(2): 74–78. DOI: **https://doi.org/10.1109/MSEC.2020.3044475**

Summary Post:

The critique of the Common Vulnerability Scoring System (CVSS) by Spring et al. (2021) highlights several key issues. CVSS relies heavily on static metrics that fail to account for dynamic risks and lacks the granularity required for detailed vulnerability assessments. Additionally, its rigid structure may not suit the specific risk profiles of different organizations.
Further Venkataramanan et al. (2019) demonstrated in their study on the Cyber-Physical Resiliency Metric (CPRM), that CPRM provides real-time score adjustments and is more effective for specific scenarios. CPRM is producing a more context-aware risk assessment than CVSS but might not cover the entire scope of threats that CVSS addresses.

In response to this critique, I agree with Tobias that CVSS, often oversimplifies complex risks, making it hard to capture threats accurately. Further, different organizational departments might weigh risks differently, which CVSS cannot fully accommodate.
One potential solution is the Stakeholder-Specific Vulnerability Categorization (SSVC), which Spring et al. (2021) suggest as a flexible alternative. SSVC allows organizations to prioritize decisions based on exploit maturity, impact, and relevance to missions. This framework enables a more tailored and context-specific approach to vulnerability management.

In my first peer response, I further discuss CVSS improvements, stressing the need for transparency and data-driven models. The CVSS v4.0 update, while an improvement, still struggles with complex environments. In my second peer response, I highlighted how SSVC could provide actionable guidance, overcoming CVSS's tendency to oversimplify risks.

To sum it up, while frameworks like SSVC show promise, it remains unclear whether improvements will sufficiently address the increasing complexity of cybersecurity threats. Although SSVC offers more flexibility, it requires extensive customization and resources that smaller organizations may lack. Furthermore, reliance on real-time data and context-specific factors introduces potential errors. Instead of simply refining existing models, a more comprehensive overhaul of vulnerability assessment methodologies may be necessary.

Word count: 302

References:
Scip AG. (2023) CVSS v4.0 – Better than v3.1? Available from: https://www.scip.ch/?labs.20240314 [Accessed 19 September 2024].

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021) Time to Change the CVSS? *IEEE Security and Privacy 19*(2): 74–78. DOI: **https://doi.org/10.1109/MSEC.2020.3044475**

Venkataramanan,V. et al. (2029) Measuring and Enhancing Microgrid Resiliency Against Cyber Threat, *IEEE Transactions on Industry Applications* 55(6): 6303-6312. Doi: 10.1109/TIA.2019.2928495.