

CWE/CAPEC User Experience Working Group Meeting

March 8, 2023



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
 - User Stories Update
 - CWE/CAPEC Board readout for UEWG
 - Discussion: CWE IDs and Hierarchy
 - Discussion: CAPEC program
- **Reminders and Adjourn**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

UEWG: Purpose

- **Mission:** Identifying areas where CWE/CAPEC content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them
- **Periodic reporting of activities to CWE/CAPEC Board**
 - (next quarterly Board meeting TBD Q2-2023)
- **Please solicit participations from your contacts**
 - Contact: cwe@mitre.org & capec@mitre.org



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Housekeeping

- **We are working to identify further UEWG opportunities and priorities for FY23**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Topic 1

User Stories

Chris Coffin / Przemyslaw Roguski



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

User Story Development

- **Milind Kulkarni developed a draft for the “PSIRT team security bulletins and disclosures” user story**
- **Are there additional updates or developments?**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Topic 2

Board readout for UEWG efforts

Alec Summers



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Board readout on UEWG efforts

- **Board is happy with the progress and accomplishments so far**
 - User personas, harmonizing definitions, content filtering capabilities, and ongoing user story development
- **The level of community input and effort is well appreciated**
- **Board meeting included lots of conversation on different topics relevant to UEWG**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Topic 3

Discussion: CWE IDs

Alec Summers / Przemyslaw Roguski / Chris Coffin



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE IDs and Overall Hierarchy

- **Long-term usability topic**
- **Vulnerability Mapping is an important use case, but it is difficult! E.g.,**
 - Data problem: CVE does not require CWE mapping for disclosure
 - Root cause(s) analysis is hard!
 - CWE structure complexity
- **How could CWE hierarchy and structure be changed to help?**
 - Should CWE IDs be assigned only to ideal, mappable weaknesses?
 - e.g., not high-level classes, categories, views
 - If so, how could this be implemented
 - Above examples are important for research purposes and organizational structure
 - Could CWE-IDs contain nested relationship information (e.g., CWE-120:1, CWE-120:2)



Topic 4

Discussion: Current state of CAPEC

Chris Coffin/Alec Summers



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CAPEC: Background and Recent Activities

- **CWE/CAPEC Program Strategy:**

- Increase program adoption and program coverage through effective community engagement

- **CAPEC over previous ~12 Months**

- CAPEC Summit (2/22) didn't catalyze stakeholder engagement in major way
- The community has been less willing to contribute to CAPEC versus CWE
- CAPEC not widely adopted relative to year's strategic focus areas:
 - HW, Pen-Testing, Supply Chain



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CAPEC Current Status

- **While there are small pockets of community interest, there is little evidence of broad-based community adoption and participation**
 - 1 modification submission, 2 entry submissions (since April 2022)
 - Minimal expansion of adoption/coverage in strategic focus areas
 - No feedback on new Supply Chain View
 - In general, pen-testing vendors develop capabilities without CAPEC; customers don't ask for CAPEC-related information
 - HW SIG minimal interest in developing content
- **CAPEC's conceptual value has not resulted in widespread adoption**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CAPEC Next Steps

- **Given the lack of demonstrable, widespread adoption and value delivery, CAPEC will be a low priority going forward**
- **CWE/CAPEC Board is considering various options (not mutually exclusive)**
 - Continue to host CAPEC site on a server (definite)
 - potential banner of halted maintenance and development
 - Open-source ongoing maintenance and development
 - Transition program to a willing organization for ongoing maintenance and development
- **CAPEC stakeholder survey open through 3/10 (see any CAPEC page)**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Next Meeting – April 5 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

CAPEC@MITRE.ORG



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Backups



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE User Pain Points

- Pain point topics that the group is aware of or would like to discuss
- For those on the call, what were your biggest questions or concerns when beginning to use CWE?
- Are there common questions that CWE users have that are not covered in the current FAQ?
- Other potential opportunities:
 - Features we could expand or improve to make CWE consumption easier?
 - Maybe engage the community in one or more ways to solicit this kind of feedback (see topic #3)
- Other thoughts?



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Community Engagement Strategy

- **Develop a strategy for engaging the CWE user community for feedback**
- **What are the best methods to query the community on topics such as the pain points covered in topic #2**
- **What communication methods should be employed?**
 - E.g., polls, emails, web, social media
- **Should we target specific user types?**

- **Other thoughts?**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.