

CWE/CAPEC User Experience Working Group (UEWG)

Wednesday, February 8, 2023

Members in Attendance

Alec J Summers – MITRE
Chris Coffin – MITRE
Przemyslaw Roguski – Red Hat
Steven Christey – MITRE
Matthew Coles – Dell
Rich Piazza – MITRE
Faheem Ahmed – CISA
Andreas Schweiger
John Christopher DeCarlo
Milind Kulkarni
David B Rothenberg
Wortman, Paul
Pablo Aguilar (LNXnetwork) (Invitado)

Agenda

- Purpose
- Housekeeping
- Primary topics
 - User Story Development
 - Demo: CWE Custom Presentation Filters
 - Open Discussion
- Reminders and adjourn

Purpose (Alec Summers)

- Mission: Identify 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 meeting scheduled for February 14, 2023).
- Solicit participation from your contacts (Contact: cwe@mitre.org & capec@mitre.org).

Housekeeping (Alec Summers)

- We are working to identify further UEWG opportunities and priorities for FY23.
 - See open discussion / topic 3.

User Story Development (Przemyslaw (Rogue) Roguski)

- Four potential user story and persona combinations have been suggested since the last meeting:
 - Security response teams using CWE in security bulletins and disclosures.
 - Management persona and how they “use/influence the use of” CWE/CAPEC.

- Technical writers (e.g., blogs, communications intermediary between engineers and design).
 - Hardware engineer and/or hardware verification engineer.
- Different personas may be interested in the same user story (different responsibilities and perspective).
- A problem that has been observed is that users are not able to identify themselves (persona) so it's difficult to see the benefit of using CWE data. Building out example persona and user story combinations should help.
- Reminder that CWE is both software and hardware and today they're distinct, but in the future there's potential for overlap, meaning a CWE could cover both software and hardware.
- Suggestion was made to provide more information (in the context of user stories and personas) about the connections between CWE, CAPEC, ATT&CK, Defend, etc.
- Question was asked about how Defend relates to CWE. Answer: Defend is focused more on techniques used to defend against attackers. There is some conceptual overlap with what CWE covers in the form of potential mitigations. Have not established a formal relationship. More discussion on this topic is needed.

CWE/CAPEC Presentation Filters (David Rothenberg)

- An update and demo was given on using custom filters to select CWE record data.
- Allows a user to pick their own selection criteria instead of using a pre-defined filter. A user can start with a pre-defined filter and then add any extra criteria.
- Contact John Decarlo for technical questions.
- The Description and Extended Description fields appear in all searches. Extended Description may be moved to the custom list (TBD).
- Go live date is TBD and not tied to a CWE update release. Prefer to have updated custom filtering in place by the next CWE release in May 2023.

Open Discussion

- Related to communications strategy, the suggestion was made to make demos about persona user stories and publish them, e.g., to YouTube. More discussion needed as well as further development of user stories. There could also be a demo about the new custom filtering of CWE data.

Reminders and Adjourn

- Next meeting is March 8 @ 12pm EST.