CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, October 19, 2022

Members in Attendance

Alec J Summers – MITRE
Przemyslaw Roguski – Red Hat
Erin Alexander – CISA
Doug Nichols – GE Aviation
Steven Christey – MITRE
Farbod Foomany – Security Compass
Shadya Beatriz Maldonado Rosado – Sandia
Nick – Red Hat
Matthew Coles – Dell
Rich Piazza – MITRE
Chris Levendis – MITRE
John Keane (Guest)
Suzanna Schmeelk (Guest)
Kirsten Gantenbein (Guest)

Agenda

- Housekeeping
- Topics
    - Review CWE & CAPEC Recent Content Releases
    - Feedback: Personas and Presentation Filters
    - Discussion: Possible Opportunities for UEWG Activity
- Reminders and Adjourn

Housekeeping (Alec Summers)

- Working to identify further opportunities and priorities for FY23.
- (Underway) Collaborative CWE/CAPEC content development collaboration space. This is an internal test bed for content suggestions received through the web app for content submissions and forms.
- Board provided final comments on the personas list and definitions (see topic 2).

Review CWE & CAPEC Recent Content Releases (Rich Piazza, Steve Christey Coley)

- CAPEC v3.8
    - Three focus areas: supply chain domain, hardware domain, a review/update of the mapping from CAPEC to ATT&CK.
    - Introduced a new view for supply chain CAPEC entries, based on CISA supply chain life cycle.
    - Introduced six new categories for supply chain CAPECs and put all entries into one or more of the categories.
    - Added new CAPEC entries to address identified gaps in CWE hardware and CAPEC hardware mappings.

    - Added about 150 new mappings between CAPEC and ATT&CK. Added text to entries to "see parent" when applicable.
    - Additional work is needed in the hardware domain, and the HW SIG can be helpful supporting that effort.
- CWE v4.9
    - This was a maintenance-heavy release with close to 700 modified entries.
    - A diff report is available that shows on a per CWE basis which fields changed and the significance of the change.
    - Content changes (new entries or modification to existing entries) were received via a submission server set up earlier this year.
    - Started to branch out into ICS/OT. Added observed examples based on a study called ICEFALL that looked at OT systems from different vendors.
    - Working with the NIST NVD team, modified view 1003 (view for mapping CVEs to CWEs) and started prohibiting or discouraging mapping to commonly misused CWEs using mapping notes.
    - Other content changes include: new entries, especially in the area of weak authentication and credentials; added new observed examples related to software written in Go or Python; and content normalization and clean up to support the CWE REST API.
    - An open question to the UEWG is how to communicate CWE changes to the broader community. Are there better options than the diff report?

      A member suggested that, for weaknesses in the weak authentication class, it would be helpful to add a relationship to other views like 699 (software development view). There was agreement, so this capability will be included in v4.10 (est. January 2023).

      A member asked if it was intentional that default credentials are associated with weak credentials, since a default credential can be strong. The intention was to cover defaults that do not change across deployments – that can be made clearer.

      A member asked if there is a "concept" of completeness of mapping between CAPEC and CWE, especially in light of the CAPEC update. That's an area that is being looked into going forward. For CAPECs without a mapping to CWE, figure out whether they should, and if not, provide a reason.

Feedback: Personas, Definitions, and Presentation Filters (Alec Summers)

- Personas
    - The Board suggested adding Verification Engineer to the Hardware Designer persona and adding Assurance (testing) Engineer to the Software Developer persona. They also suggested simplifying the Tool Developer persona description

to include all products in a security domain that find weaknesses or aim to attack systems.

A member asked if there is a strong argument for separating Software Developers from Tool Developers. Maybe call the persona Tool Designers instead.

Another member suggested adding to the Tool Developer persona description that they also "attest to the lack of weaknesses in a product."

- Definitions
    - The definition of Attack Pattern has been updated to parallel the language in the definitions of Vulnerability and Weakness.
    - In the Weakness definition, "right circumstances" (subjective) was changed to "certain circumstances."
    - There were no objections to the updated Definitions.
- Presentation Filters (CWE)
    - Filters are used to view customized information (select data fields).
    - Members were asked if they had used the filters, and if they had any feedback.

      One member responded favorably – the filters work and make sense.

    - In the future, the program intends to add a static page that shows the elements of an entry for each filter.
    - Adding new views to CAPEC (beyond Basic and Complete) is something for the future. Could the same model as CWE be used? It was mentioned that CAPEC is working on a draft of how it would do filters, and it will be sent out when done.

Possible UEWG Activities and Focus Areas (Alec Summers)

- The UEWG leadership group plans to meet over the next couple weeks to plan strategic priorities. These could be enhancements to existing capabilities or new initiatives. Results will be shared at the next meeting. Some initial ideas were presented, e.g., engaging other working groups or users.
- Members were asked for their ideas about future priorities.

  A member asked a question about what is happening with CWSS (scoring system). It is still used, but not maintained, due to deprioritization. Is this an area to look into? Something to consider is developing a roadmap for future maintenance.
  Another member (from a university) asked if it would be OK to query students about their experience with the CWE website and get their feedback. There were no objections. The approval process may take a few weeks.

Reminders and Adjourn

- Next Meeting is November 16 (12 pm EST)