CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, September 27, 2023

Members in Attendance

Erin Alexander – CISA
Aliasghar Arab - Nuro
Kris Britton – MITRE
Vishal Chauhan - Microsoft
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew Coles – Dell
Jonathan Dutson - Microsoft
Farbod Foomany - Security Compass
Parth Jamodkar - Hyland Software
Milind Kulkarni - Ericsson
David Maxwell - BlueCat Networks
Lisa Olson - Microsoft
Rich Piazza – MITRE
Gerald Rigdon - Boston Scientific Corporation
Remy Stolworthy - INL
Alec Summers - MITRE
Christopher Sundberg – Woodward, Inc.
Cindy Sutherland - Lockheed Martin
Umberto Vizcaino - Merysol Security
Blaine Wilson - BMO Financial Group
Paul Wortman – Wells Fargo
Oana

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - CWE Element / Information Presentation Mockup
    - CWE Demonstrative Examples
    - CWE Graphical Depiction PDFs
    - Red Hat CWE Blog
    - Open Discussion
- Reminders and Adjourn

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 Q4 2023).
- Please solicit participation from your network (contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- UEWG meeting frequency has changed; they now occur on the last Wednesday of the month. It was noted that the correct meeting invitation is from Chris Coffin. If you have one from Alec Summers on your calendar, delete it.
- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org.

CWE Element/Information Presentation (Chris Coffin)

- This topic is about elements/information of CWEs, and how they're presented to a user. Highlights of the August meeting discussion were shared for those unable to attend.
- For next steps:
  - Who is the audience (new, experienced, all users)?
  - What elements are most important to those users? How should they be presented?
  - Should the program investigate or create a graphical presentation of a CWE?
- Since the August meeting, the program created a mockup that may be helpful for a new CWE user who wants a limited view. Elements shown in the mockup include: description, extended description, consequences, demonstrative examples, relationships to other CWEs (maybe present in a graphical format?), and references. Comments for modifying the selected elements are welcome.
- Question: *Have we ever tried to do something more like a database for CWE where you can drill into those relationships, rather than just a graphical representation which doesn't give the whole picture necessarily?* Answer: There is a relationships view that allows the user to drill into CWE relationships (parent and children). The program has not really explored more dynamic ways to browse information, but that is something we would like to have.
- Comment: *A member commented that he downloaded CWE data, converted it to XML and translated that into a SQLite database where SQL queries can be run. The script (how to) for this can be shared if interested.*
- It was noted that there is a working group devoted to REST API development for the CWE corpus. The group is open to the public, email CWE@mitre.org if you are interested.
- Comment: *The Idaho National Laboratory has a tool called STIG (structural threat intelligence graph), available as a free download at GitHub. A member commented on how helpful the tool is for CWE and CVE navigation. A future meeting will include additional education on STIG.*

- Question: *Is the mockup somewhere we can access it, like a playground where we can experiment?* Answer: No, the mockup in the slides was generated using the custom filter capability. Slides will be made available.
- Comment: *We have a bunch of different personas. We need to find out who the new users are and make sure we present information appropriate to them.*

CWE Demonstrative Examples (Chris Coffin)

- Not all CWEs have a demox (521 do, 412 do not, including one on the Top 25 list). Of those that do not, reasons include: may not have good examples, e.g., in the case of HW CWEs; program priority was on populating the corpus; and the significant time and expertise that goes into creating good examples.
- It was commented that the demox is probably the most difficult data element to get correct.
- Question: *Of the 412 CWEs that don't have examples, could we cross reference CAPEC to supplement with some of that information?* Answer: (1) Many of those CWEs have mappings to CAPEC. I wouldn't say that very often, CAPEC fills the need of a demonstrative example in the same kind of way. (2) CAPEC shows the execution flow which is kind of similar to examples; could be an interesting starting point. (3) We want examples to be CWE-specific and there are many-to-many relationships between attacks and weaknesses.
- CWEs can inherit a demox from a child. Would like to get to a point where every higher level CWE inherits a demox from each child.
- The HW SIG is working to add demox content for HW CWEs. Expecting about 10 new examples in the next release.
- Having an example based on the code or process or data flows would be important when training developers.
- Contact the program if you have content for a demox or ideas about community involvement. The program is working on a GitHub solution for making content suggestions – more to come later.

CWE Graphical Depiction PDFs (Steve Christey Coley)

- The program has PDF files on its website that show different graphical views and the hierarchical layout of these views. Rationale was to show the structure implied by parent-child relationships. Different colors are used to highlight different levels of abstraction.
- Trying to help users conduct mapping more quickly and accurately.
- There are not many downloads of these PDFs per month, and the program doesn't know who the users are or what they are using the downloads for. The PDFs are not intentionally hidden, but are not easy to find.
- Example graphics were presented for CWE-1194 (hardware view), CWE-699 (development view), and CWE-1000 (research view). See meeting slides.
- Questions for the UEWG:
    - Are you aware of the PDFs?

    - Is anyone using them?
    - What kinds of users would care about hierarchical depictions of views?
    - Do they provide value in their current form?
    - Could they be improved upon?
- Comments: *Multiple comments in chat noted that members were not aware of these PDFs. One comment in chat noted that they were aware but were not using the PDFs.*

Red Hat CWE Blog

- The presentation will be at a later date. The link to the read-ahead material was shared.

Open Discussion

- At the last meeting, there was discussion about using quizzes about CWE as a fun way to generate interest in the program and get more people involved. Does anyone have interest in developing some questions? Contact CWE@mitre.org with suggestions.
- Comments: *Comments in chat included CWE Jeopardy, a CWE addendum to "Cybersecurity Myths and Misconceptions" by Prof Spafford, and posing the question "What is the difference between CWE and CVE?"*
- Question: *If there is a U.S. government shutdown, will that affect the UEWG October meeting?* Answer: No.

Reminders and Adjourn

- Next meeting is October 25 at 12pm EDT.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.