CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, August 24, 2022

Members in Attendance

Alec J Summers – MITRE
Przemyslaw Roguski – Red Hat
Kirsten Gantenbein
Steven Christey
Christopher Sundberg
John Keane - Guest
Yves Younan - Cisco
Paul Wortman – Wells Fargo
Shadya Beatriz Maldonado Rosado - Sandia
Jay Jacobs - Guest
John Keane - Guest
Farbod Fooman – Security Compass
Steven M Christey - MITRE
Nick - Red Hat
Matthew Coles - Dell
Rich Piazza - MITRE
Velian - Guest
Milind Kulkarni - Nvidia
Bob Natale – MITRE

General/Initial Discussion

Agenda topics:

- Housekeeping
- Definitions! (continued…)
    - Why are we doing this? The questions we asked ourselves…
    - Distillation of the many responses we received
    - Present newly proposed definitions
- Personas and Presentation Filters

Housekeeping (Alec Summers)

- UEWG reminders (mission, next quarterly CWE/CAPEC Board meeting is TBD Sept/Oct, and solicit participation from your contacts).
- Plans are underway to develop and stand up a collaborative content development space. This will provide the community with a transparent view into the status of ongoing content development work, and provide a convenient forum for collaboration among users on their own schedules. This will be a topic for a future meeting.

Personas and Presentation Filters (Alec Summers)

- Topic was moved up in the agenda to accommodate participant schedules.
- The plan is to make personas and filters part of the release that comes in September or early October for both CAPEC and CWE. Dates are tentatively set.
- The release will publish formally the user persona definitions that have been discussed previously, and also implement some changes to presentation filters.
- A proposal was made to remove incident response teams from the defined personas. The reasoning is that these teams are one step removed from the initial CWE/CAPEC audience. There was no disagreement to the proposal.
- The proposal to have two main types of users – Theoretical and Technical – was revisited.
    - Examples of Theoretical users are educators and technical writers who don't usually have a need for technical detail about a weakness.
    - Examples of Technical users are tool developers and security researchers who manage security issues and need more granularity/detail about the nature of weaknesses.
    - A proposed list of data elements for the two groups was presented. Also presented were data elements to enhance mapping-friendly capabilities, and the idea to make the complete record data elements available.
    - Feedback on the proposed data elements was requested. A recommendation was made to change 'Technical users' to 'Operational user.'
    - Members have two to three more weeks to provide final feedback.
    - More awareness among the CWE community of presentation filters is needed. Members are encouraged to offer up recommendations about how.
    - A suggestion was made to change 'presentation filter' to an action, e.g., 'Customize User View.'
    - Another recommendation was to add the feature where a user hovers the mouse over something of interest and information about content appears.

Definitions! (continued…) (Alec Summers)

- Harmonizing common terms across CWE and CAPEC has been going on the last few months. It was brought to the UEWG attention that there are three different definitions for 'vulnerability' across CVE, CWE and CAPEC.
- Improving the language situation is something the program can control, and will help ensure there is a common understanding of terms related to weaknesses, vulnerabilities, attack patterns, etc. in communications with related programs.
- A question of interest is "are circular definitions problematic or essential?"
- Another question of interest is "can we accommodate with the CVE vulnerability definition without changes?" The CVE definition was vetted across a large stakeholder audience, so it's worthwhile to accommodate the definition if possible.
- When defining 'weakness' the program is not interested in weaknesses in items like physical security/locks or issues related to spelling. Also out of scope is the enumeration of human weaknesses, for example social engineering attack patterns and the underlying human weakness.

- Feedback on definitions, based on at least 30 different records that were processed:
    - Delete "...in a range of products made by different vendors." There's consensus around making it more clear and concise, as well as security specific.
    - Follow CVE vulnerability definition format/style.
    - Using the term “flaw” may create a circular definition.
    - Leverage the term “condition” instead of “defect” in reference to a weakness.
    - May or may not be exploitable.
    - Vulnerability can be thought of as one of more weaknesses plus a known exploit, and a weakness can be thought of as one or more conditions that lead to undesirable behavior.
- The question was asked "what is the definition of a condition?" Defects, flaws, and intent of the introduction of a weakness (purposeful, incidental) were mentioned as examples of a condition. A challenge with defining new terms (like condition) is that it usually requires additional definitions for terms used in the definition. A comment was made about feedback that liked the term 'characteristic' over 'condition' although feedback from the community does favor 'condition.'
- A preferred definition for the term 'Vulnerability' was presented. It adopts CVE's definition.
- A proposed definition for the term 'weakness' was presented: "A condition in a software, firmware, hardware, or service component that, under the right conditions could contribute to the introduction of vulnerabilities." Feedback resulted in changing 'right conditions' to 'right circumstances.'
- The proposed definition for 'weakness' includes the word vulnerabilities. This gets back to the idea of circular definitions. Should the definition include the term 'vulnerabilities' or 'exploits?' Vulnerabilities can exist without being exploitable. The consensus was to keep 'vulnerabilities' in the definition and not add 'exploits.'
- There was discussion about the meanings of weakness, vulnerability and exploit, and their inter-relationships. A weakness can exist without being exploitable and/or without being a vulnerability.
- There was agreement to the revised definition for weakness: "A condition in a software, firmware, hardware, or service component that, under the right circumstances could contribute to the introduction of vulnerabilities."
- There will be another round of review of the proposed definitions.

Next Meeting

September 21, 2022 (12 pm ET)