CWE/CAPEC Board Meeting #7

Tuesday, November 16, 2021 @ 1200-1400 EST

Members in Attendance

Paul Anderson – GrammaTech
Pietro Braione - Università degli Studi di Milano – Bicocca
Chris Eng – Veracode
Jason Fung – Intel
Marisa Harriston MITRE – (CWE/CAPEC, Secretariat)
Alex Hoole – Microfocus
Chris Levendis – MITRE
Jason Oberg – Tortuga Logic
Kurt Seifried – Cloud Security Alliance
Alec Summers – MITRE (CWE/CAPEC, Board Moderator)
Christopher Turner – NIST

General Discussion/Agenda

Item 1: CWE/CAPEC Board Charter

The group discussed dates for reviewing and updating the CWE/CAPEC Board Charter and Code of Conduct in addition to voting on the documents. *A member expressed an interest in having the code of conduct be the first item for review as it could set the precent for the other item.*

There was a question about voting and whether or not the process would take place via call of email. Since a formal process has not been approved, voting will take place via email on this occasion. The option for proxy voting was also discussed (see charter for more information).

The CWE/CAPEC Project Lead expressed thoughts on how he felt that not everything has to be voted on via email, only the larger priority topics.

Office 365 (versus emailing attachments) was discussed as an option for ease of access when editing.

ACTION: The editable documents and all deadlines will be shared with members following the meeting.

Item 2: Overview of Content-Related Events

The moderator provided a recap of the most recent minor releases (CAPEC 3.6 and CWE 4.6) in addition to some of the supporting assets (blog and podcast).

CAPEC 3.6

- Execution Flow element expansion throughout the corpus (40+ entries)
- Updated entries on supply chain attack patterns

A member proposed looking closer at software component analysis in the supply chain (e.g. dependency confusion, typo squatting, Unicode control characters in trojan attacks, and potentially, people downloading dynamic source code components). The moderator agreed that these could be useful to look at along with a view that takes different lifecycle development phases into consideration.

A member asked if CWE has inclusion rules (criteria) similar to CVE. He also brought up an issue with items that should be documented but may not lead directly to vulnerabilities (example provided was Python Pickle) and the need for source control. Another member agreed and shared that CWE was becoming a "Swiss army knife" and the difficulty in trying to find what you're looking for with the presence of other irrelevant information.

The moderator stated that there are guidelines for submitting entries/what is needed for CWE on the website. In regards to the one to one relationship between entries of the different corpuses, CVE to CWE or CWE to CAPEC hasn't formally been declared because the team has not considered enumerating weaknesses related to social engineering. He acknowledged that the CWE team needs to determine whether they would get into the business of enumerating best practices. The team was approached by SAE 32 about enumerating indicators of weaknesses of potential compromise with counterfeiting (after analyzing CWE entries it was determined that some fit, others are more relevant to CAPEC, and others don't fit at all).

The first member mentioned that CWE originated with weaknesses and source code but as time has gone on, things that didn't used to be represented in code are now represented. Another member expressed disinterest in seeing the CWEs cover software engineering development activities because it broadens the scope too much and the conversation continued around scope creep. The two members discussed examples (following up on Python Pickle) of what is intentionally (versus unintentionally) dangerous. The moderator shared his thoughts on the difference between adding new content and creating a new view as well as the importance of a taxonomy definitions. *Other members brought up factors like maintainability and usability.*

The moderator then acknowledged that the program team has heard feedback from the community about a lack of clarity and that the submission form is time consuming. When interested parties approach the team, they're usually able to provide a title and abbreviated description initially. Core components should consist of intended behavior, mistake, effected resource, and effected technology. Suggestions often don't make it in because there is already an existing weakness. In these cases, they could be added as an example instance.

In response, a member suggested providing more transparency by having the program share what is in the pipeline. A method for flagging specific entries for prioritization was also proposed. The concept of hosting office hours came up as an idea for discussing why a submission didn't end up becoming an entry so that submitters can understand the thought process during reviews. The moderator discussed an early tracking tool that was created for CWE HW SIG members to track what was being developed during the initial hardware expansion. GitHub was also suggested as another approach for tracking. Use of the new web submission form (still in development) will also help with some of these issues.

Item 3: Overview of Recent CWE/CAPEC Working Group Activity

The moderator provided a recap of how and why the User Experience Working Group was stood up. One of the first and latest products of the group work, a condensed user personal list, was shared. The categories are:

- Those who:
    - Build systems
    - Use systems
    - Protect infrastructure around those systems
- Educators & tech editors/researchers
- PSIRT/CSIRT/SIRT

A member asked about how the distilled personas fit with the CVE personas and went on to ask whether or not the use cases of each of the original 14 personas needed to be analyzed. The moderator acknowledged that the categories could be made clearer for the purpose of CVE/CNA mappings.

Another member asked about where tool vendors fit. The moderator shared that it would depend on the type of tool vendor but that they may market/build to those in the use case box. There were also similarities drawn between the researchers and this group.

Next, there was also discussion regarding whether or not MITRE had any REST APIs working with the CWE site. This is something that is being worked on by another group and the CWE team is in the early stages of accomplishing this.

The moderator also shared that the cadence of the UEWG meetings was switching from biweekly to monthly.

Item 4: Overview of recent HW CWE SIG Activity

The moderator provided an overview of the activities that have been occurring between the Counterfeit SAE group and the CWE team.

A member asked about the progress on whether a connection had been made between the counterfeit SAE group and CWE. The moderator shared that the CWE team is still assessing the relevance but that the SAE group will be attending a future SIG meeting to present potential buckets for incorporation. *The member also asked about how supply chain security in software is handled.* The moderator stated that the topic wasn't currently clearly addressed but discussed the merits of a previously proposed idea, adding tags (vs views). *Adding on, a member stated that between CWE and CAPEC, not all domains are covered appropriately. He went on to say that we shouldn't try to boil all of the domains down and force them into certain categories. Another member said that if something can't be mapped, a decision needs to be made about whether it is a good fit for creating a new entry or category or whether it's completely out of scope. Other members were in agreement.*

Item 5: Other Items/Topics
Harmonizing the glossaries of CWE, CAPEC, and ideally, CVE

The member who proposed this topic discussed the discrepancies in definitions between the different corpuses and the need for consistency potentially through a unified glossary. Another member asked if there would be room for multiple definitions for different terms when warranted. The moderator expressed an interest in conducting a delta check.

The moderator also recapped some of the items that were entered into the chat including an official syntax for communicating CWE chain. Due to time constraints, this topic will be discussed at a future meeting.