CWE/CAPEC Board Meeting #5

Tuesday, May 18, 2021 @ 1230-1430 EDT

Members in Attendance

Paul Anderson – GrammaTech
Chris Eng – Veracode
Jason Fung – Intel
Jay Gazlay – DHS CISA
Marisa Harriston MITRE – (CWE/CAPEC, Secretariat)
Alexander Hoole - Micro Focus
Joe Jarzombek – Synopsys
Jason Lam – SANS
Chris Levendis – MITRE
Jason Oberg - Tortuga Logic
Braione Pietro - Università degli Studi di Milano - Bicocca
Alec Summers - MITRE (CWE/CAPEC, Board Moderator)
Christopher Turner - NIST (NVD)

General Open Discussion

New Top N Lists

A member brought up their desire to see the CWE team engaged in developing other Top N lists, such as one specifically for aerospace and defense. He explained that in his work within the industry, weaknesses with the highest consequences (versus most exploited) take precedent, an approach that could be explored further when developing these lists. The possibility of accepting more than code level flaws was also mentioned.

The sponsor brought up the aviation industry as a prime example of a group that could also benefit from its own list.

Another member asked if the process would occur pre-compilation or post pre-processor. The other member had not yet factored this perspective in and elaborated on how suppliers would be a target audience.

The moderator acknowledged that the consensus among the group seemed to be in favor of industry/topic specific lists and discussed the process and methodology for developing the Hardware Top N List, so far, as an example.

CWE Submission Limitation

A member mentioned that he would like to discuss the rationale behind why text can be submitted for new CWEs, while diagrams and image files are not supported. He shared that this could be particularly useful for hardware-related entries.

What to do about Negative Community Feedback
See agenda for additional information

The moderator kicked off the conversation by discussing the value of CWE's data while making the case to make the content more digestible and easier to navigate based on feedback received from the community (CNA and others). A CWE team member added that the website is currently set up with power users in mind and that the experience is likely confusing for others.

A member responded by stating that the site uses terms in an "overloaded" manner. Also, items that use a CWE identifier aren't necessarily a CWE. This causes confusion and affects CVE mapping. The member also discussed the idea of using swim lanes to distinguish between software, hardware, and quality views. Another member expressed concern with putting the categories into silos and focusing on addressing the overall weakness. However, volume was brought up as a reason for why companies may have to divide the way that they address issues.

A CWE team member brought up the idea of establishing a quality working group to address these problems. This would consist of having the community come up with the potential solutions for best practices around content (defining effective ways to describe a weakness, etc.) to bring to the board.

The moderator acknowledged that some work has been done to this end (particularly through the HW SIG).

A member amplified what another member shared in chat – that a user experience working group sounded more appropriate (versus quality) based on the needs expressed since the issue is more about the way people want to use the site versus its current state. He elaborated on the need to focus on user stories, case studies, etc. Another member inquired about whether a UI/UX expert has been consulted.

A third member countered, stating that there may be more to address than user experience and he drew attention to feedback on inconsistent taxonomies and definitions, related to content. He also discussed the challenges of getting students in an academic environment to understand the relationship between a CVE and related weaknesses as there is not always a direct relationship. The same was said about the connection between weaknesses and attack patterns. Another member agreed, adding that there should be a resource developed to explain why new users should care about CWEs and how they can be exploited.

The moderator agreed with the need to better integrate entries across the different lists and that the new working group would potentially be able to address each of the challenges presented. He said that sorting/scaling the current content is not something that the CWE project team can necessarily which is where enlisting the help of an external group such as this becomes valuable.

A member wanted to draw the distinction between giving users what they want and the case for quality. The CWE team member acknowledged that there was a balance that needed to take place but that an emphasis should be placed on the internal team not making decisions in a vacuum without consulting the community. He also talked about the ability replicate what has worked for similar groups under CVE and the CWE HW SIG.

Another member emphasized the need to define the user groups/personas as an initial objective of the working group and stated that the quality is a perception of a given user.

The moderator recapped some of the audiences that have risen out of previous conversations such as software developers, tool vendors, users from academia, and CNAs reporting vulnerabilities. However, the formal collection of user feedback could potentially be conducted by the new group.

A member brought up the importance of clearly defining scope to properly address user issues in this context.

The CWE team member discussed the typical setup of the CVE working groups, interaction with the board, and requirements for membership. A member asked whether there might be enough interest to field a new group given that CVE currently has a larger following. The CWE member mentioned that building the CVE groups took time and eventually found success through trial and error. Additionally, interest in the CVE groups has increased over time because of the positive results produced.

ACTION: Announce establishment of working group, begin recruiting members and develop governance based on CVE's model.

CWE and OASIS SARIF
See agenda for more information

The member who proposed this topic gave a brief overview of the OASIS SARIF program:

- First standard came out just over a year ago
- The way it works: User runs static analysis tool, gets results in JSON file, and then receives a set of tools to manipulate results; a rules section gives findings or taxonomies
- There is a committee that is seeking participants for Board members who are interested (or if there are other you know who may be interested) in helping with additional guidance
    - There has been conversation about keeping the results static vs. changing to dynamic
- Who should own and maintain the mapping information?

A member asked if it was feasible for the CWE project team to host the SARIF instance on the CWE website.

Another member, familiar with the tool mentioned that the CWE team still needed to be briefed on what would be involved with hosting. The presenting member added that there the output was likely drawn from existing CWE descriptions but that there is additional information about the taxonomies. The member also asked for clarification on version control between the CWE team and a third party adding new information. The presenting member responded that there isn't anything currently in the taxonomy that identifies who made which additions and acknowledged the need for a digital signature should be addressed the SARIF group. The moderator asked for clarification on whether for each version of SARIF there is a direct mapping the CWE site with links. The member shared the advantage of having the CWE team own the process is currency and the fact that everyone would get a consistent view.

ACTION: The moderator will discuss if and how the CWE can support the effort.

Upcoming Releases
See agenda for more information

The moderator briefed the group on upcoming releases included CAPEC 3.5 on June 26 and CWE 4.5/Top 25 Software Weaknesses on July 20.

A member mentioned that in relation to mapping, a CWE may not always be linked to a CAPEC in case of a quality issue, for example.

The moderator agreed but also shared that the CAPEC team is looking to fill in gaps and conducting work around chaining. He also shared that the team has been more engaged recently with the penetration test tooling community to discuss how to collaborate in a similar way to the hardware community. Some of these groups were already mapping to CVE and even CWE.

A member requested an update to one of the proposed improvements for CWE 4.5, stating that there wasn't overlap between CWE-1310 and CWE-1277.

The moderator shared that the CWE team is working with the submitters to rework the phrasing regarding the relationship between the two CWEs and that they neither would necessarily be removed.

A member brought up his concern about introducing CWE-1104 as a base class and how it uses a component that is no longer maintained. This creates inconsistency and breaks from not having CWEs for vulnerable components. He asked if we should have a CWE for using a vulnerable component. Another member agreed and added that we should be able to score open source software.

One member asked for an update on the Top N Hardware list.

The moderator provided a summary of the initial feedback from the 11 HW CWE SIG respondents (slides available upon request). Topics covered in the initial included generating a title and how to define what is included in the list. After working with the SIG to refine and draft content, it's estimated that the public survey could be distributed this calendar year, if not before April 2022, when the period of performance concludes.

Another member expressed that he was pleased with the Top N efforts so far and emphasized that the process doesn't need to be an exact science and that an initial goal could be to collect as much information as possible.

A conversation then took place about how to generate more input in this initial data collection stage including the merits of getting the public more involved via social media. The moderator suggested socializing the new top N concept through the SIG members as a means of collecting more data and recruiting new SIG members. A member suggested having SIG members reach out to the CISO of their companies and then having them reach out to other CISOs from hardware companies to get them involved. The group also briefly discussed the cadence and making this new list a reoccurring feature.

New Podcast

The moderator provided an overview of what has occurred in regards to the development of the new CWE/CAPEC podcast and how the team is looking to emulate the success of the CVE podcast. The first episode of the monthly series, a primer on CWE and why it's important, is scheduled to be released in June. A similar episode will be created for CAPEC in July. The third episode will likely cover the Top 25 Software Weaknesses list.

A member expressed interest in discussing the relationship between CAPEC and CWE in a future episode.

Another member requested that user stories be incorporated to get a better sense of how companies are using CWE/CAPEC to make their products better.

ACTION: Board members are encouraged to share their thoughts on the music survey that was sent earlier in the month along with additional thoughts and suggestions on the podcast.

Outstanding Topics

The group circled back to the topic of creating industry and technology specific Top N lists. The moderator brought up the fact that the individual lists would need to be at least partially developed in collaboration with the target audience they're intended for and that the methodology would be different than what has been used for the software list, for example.

The topic of diagram limitations on content submissions was also brought up and the moderator requested that the member who brought up the topic follow up with his team to get specific examples of where this could be an issue. The idea of having a graphic representation for anything appearing on the Top 25 list was also proposed.

A member offered to share his organization's resource on how they CWEs are used as a reference for how graphics can be incorporated.