CWE/CAPEC Board Meeting #6

Tuesday, August 17, 2021 @ 1000-1200 EDT

Paul Anderson – GrammaTech
Bill Curtis – CISQ
Chris Eng – Veracode
Jason Fung – Intel
Jay Gazlay – DHS CISA
Marisa Harriston MITRE – (CWE/CAPEC, Secretariat)
Alex Hoole – Microfocus
Joe Jarzombek – Synopsys
Chris Levendis – MITRE
Jason Oberg – Tortuga Logic
Alec Summers – MITRE (CWE/CAPEC, Board Moderator)

General Discussion/Agenda

Item 1: What to do about negative community feedback

The moderator briefed the Board on what steps have been taken to address concerns, such as the establishment of the CWE/CAPEC User Experience Working Group. A recap of the group's initial activities and general findings upon enumerating the CWE/CAPEC personas was provided. Next steps for this group will include enumerating usage scenarios.

A member shared that he had participated in one of the group's meetings but was surprised that auditor or acceptance tester weren't listed among the personas. The sponsor asked for clarification on the difference between the personas mentioned and the risk assessors. The member shared that his suggestions could be subsets of a risk assessment category.

A member brought up hardware roles (e.g. designers, architects, verification team member). The moderator expressed the need to have more involvement from the HW SIG members for a more representative persona listing. The member also brought up the idea that software and hardware usage may have more in common than distinct.

A member suggested condensing the list down so that future development work in bound by a specific scope. He also reiterated the need for hardware representation. Another member followed up to share the potential value of getting more specific with the personas for the purpose of mapping them to specific CWEs. A third member addressed this by offering options such as adding different sections for each audience within an entry. He said that there are different approaches available (e.g. views vs entries.

A member asked when the Board can expect to see the developed personas. The moderator gave an overview of the timeline over the next few months as well as plans for creating a landing page that would house more frequent updates between different CWE/CAPEC groups.

Item 2: Overview of Recent Content-Related Events
See agenda for more information
The moderator provided status updates on the following content-related activities:

- 2021 CWE Top 25 – Incorporating NIST NVD into a new data-driven methodology
- Releases of CAPEC 3.5 and CWE 4.5 – Supplemental highlights include the "New to CAPEC" page to orient new users and the expansion of "Vendor Usage" page
- Launch of the CWE/CAPEC Podcast, Out of Bounds Read – Initial episodes cover the basics of CWE and CAPEC. Future topics will cover the Top 25 and the CWE's 15th anniversary.
- Other routine engagement across social media and the blogs

A member expressed an interest in participating in the 15th anniversary podcast episode.

Item 3: CWE-CAPEC Mapping Discussion
See slides for more information.

The presenter (CAPEC task lead) provided background on how the mapping between CWE weaknesses and CAPEC attack patterns are key to the broader ecosystem, which includes CVE. Historically, these mappings have been developed by the CAPEC team, but the CWE team became more involved recently. Because releases from the two projects are in sync, inconsistencies are exposed between the two corpuses. Top challenges of the current mapping were also covered.

A top-down approach was proposed as an alternative to the current static method. This would include dynamic mapping that displays relevant weaknesses at the same abstraction level as CAPEC as well as an option to see relevant children. Constraints of implementation for the team include the lack of guidelines and a time-consuming process as well as users finding the fully expanded list of weaknesses large and overwhelming.

A bottom-up approach was also proposed, with static mapping, a hover gesture to show where weaknesses are within the hierarchy, and fewer leaves as CAPEC hierarchy is traversed and attacks become more specific, as an easier to implement solution. However, multiple constraints exist, such as large lists, implied inclusion problem uncertainty, and weaknesses with "multiple parents."

The ultimate goal is to have more consistent hierarchies across CWE and CAPEC.

A member asked if all CWE associated have one or more CAPEC IDs. The presenter said that there were for the most part but that it wasn't necessarily the case in the reverse situation. He also reminded the members that CAPEC features entries on social engineering and other items that don't have mapping to CWE currently. The member noted that there are groups within financial services that are using CWEs to enumerate human weaknesses. The member also expressed uncertainty around changing parent/child relationships.

A member expressed support for the top-down approach but acknowledged the challenges. Another member suggested including the tree and highlighting the relevant child so that context isn't lost. The presenter clarified that there are filters on the current website that incorporate a similar functionality but that it may not the best way to display this information.

A member brought up the idea of allowing submitters to include information on confidence and fit with regards to mapping (related to many to many vs many to one). The idea of not mapping at the meta level of CAPEC as well as how execution flows should be handled was brought up.

Adding process and behavioral weaknesses was discussed again. The concept of bringing subject matter experts in when appropriate was mentioned.

Item 4: HW CWE Update

- Upcoming HW CWE Top-N List – Aiming to release at the end of October 2021 and include 10 entries. There were five clear contenders from the initial informal survey. Next steps include conducting a card sorting exercise with the HW SIG at the September meeting to finalize the list and soliciting support from board members as part of awareness campaign after publication.
- Content expansion – proposed by subset of HW SIG; enumerating indicators for non-conforming, counterfeit and tampered hardware components (supply chain)

A member brought up *the State-of-the-Art Resources* Report community as a target audience for the HW top-N list since the weaknesses generally are not detectable by tools.

Item 5: CWE/CAPEC Board Charter

- Drawing from recently revised CVE Board charter
- CWE/CAPEC team will send out draft proposal for Board approval in coming weeks
- Priorities include direction around Board membership and addressing Red Hat's interest in membership

A member proposed separating the mission information from the bylaws information because of challenges that could occur with updating a single document. Another member agreed. A third member felt that they should be kept together similar to what is in the CVE charter.

The moderator agreed to separate the information for the initial proposal and distribution.