CWE/CAPEC Board Meeting #8

Tuesday, February 15, 2022 @

Members in Attendance

Paul Anderson – GrammaTech
Bill Curtis – Consortium for IT Software Quality (CISQ)
Chris Eng – Veracode
Jason Fung – Intel
Alex Hoole – Microfocus
Chris Levendis – MITRE
Jason Oberg – Tortuga Logic
Alec Summers – MITRE (CWE/CAPEC, Board Moderator)

General Discussion/Agenda

Item 1: Requests for the Establishment of New Community Engagement Groups

The Board was joined by a representative of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) within the Department of Energy (DoE), as well as several community members representing the Securing Energy Infrastructure Executive Task Force (SEI ETF) who presented their idea for establishing a CWE-CAPEC ICS/OT Special Interest Group. This group would bring together an established set of stakeholders in this domain and refocus their efforts to expand and contribute to the way ICS and OT is represented in CWE in order to advance engineering of secure systems. *A member suggested they also think about relevant attack patterns (CAPECs) associated with the weaknesses they enumerate*. The guests recognized this point and said it was part of their plans. *A member asked if the plethora of IoT protocols and the vulnerabilities within them would apply.* The guests affirmed that this was part of their plans and expounded on what the working group had done thus far in looking at weaknesses that are ICS specific – specifically those in the energy manufacturing and distribution. How they differentiated from the traditional IT vulnerabilities, for example. *A member relayed an example of devices with JTAG interfaces that facilitate complete access to a device.* The guests agreed and shared that these and others were the types of ‘engineering foibles’ that we want to try and enumerate and ultimately have avoided. *A member talked about weakness scoring – referencing past efforts with CWRAF.* The Board thanked the guests for attending. The guests thanked the Board for the opportunity.

Action: The Board voted in favor of approving the establishment of a CWE-CAPEC ICS/OT SIG

A member asked for clarification on who is responsible for CWE “grammar” and making sure things keep their semantic meaning as the scope of CWE/CAPEC continues to expand. The moderator said that this is an ongoing effort within the HW CWE SIG and gave an example. *A member agreed and said that there is a lot of work that goes into getting the weaknesses* *defined according to the CWE schema and making sure they make sense to the wider community. They highlighted the harder part being on the CVE side where they'd hope we could accelerate the adoption of denoting SW, HW, and FW within CVE records. A member wondered about CWE's support of images – which for architecture are important.* The moderator pointed out the initial foray into supporting images by linking to a jpeg image directly from CWE pages.

The moderator presented the community request for the establishment of a CWE/CAPEC REST API Working Group. The request comes from several members within the Accellera Systems Initiative IPSA Working Group. *Board members asked questions as to the details of what target objectives for the working group would be. There were also questions as to the timeline, organizational structure, and technical specifications (e.g., using GraphQL instead of a REST API).* The moderator said many of these details would be part of the working group's initial efforts – i.e., establishing group protocols and determining the technical specifications. *A Board member raised concerns as to whether the backend infrastructure could support whatever the working group proposes.*

Action: The Moderator will go back to the community members proposing the REST API Working Group with the Board members questions. The Moderator will both relay the questions in writing as well as connect the community members directly with the Board members via email to better facilitate direct engagement.

Item 2: The CAPEC Community Summit

The moderator presented the current state of planning and preparation for the first ever CAPEC Community Summit to be held on February 23. There are going to be 6 session topics including "Pen Testing and Execution Flows," "Using CAPEC for Education," "Hardware and CAPEC," "CAPEC Entry Completeness and Quality," "CAPEC and Supply Chain," and "Community Discussion: Vision for the Future of the Program." Guest presenters and panelists are submitting materials in the build-up to the event. *A Board member asked if it will be recorded.* The Moderator said yes, and the videos will be subsequently published on the CWE/CAPEC YouTube channel by session in a similar way to the CWE Compatibility Program Vendor Summit of 2021. *A Board member requested more information as to the registration process and which organizations have registered.* The Moderator shared a spreadsheet of current registrants. *A member asked as to the goals of the summit.* The Moderator explained that there are several: firstly, the program hearing directly from its community stakeholders how CAPEC is currently or could be used; secondly, identify opportunities for improvement in a number of key modernization areas (e.g., content, user experience); thirdly, provide a catalyst opportunity for further CAPEC community engagement in a similar way to how the CWE Compatibility Vendor User Summit was for the CWE program. *Members asked for more details on several of the sessions previously listed.* The moderator gave additional information regarding the session presenters and a brief overview of their talks.

Item 3: Overview of Community Engagement

The Moderator provided an update on the latest CWE/CAPEC community engagement publications across podcasts and blogs. *A member asked as if the Moderator could share stats on readership/listenership of these.* The Moderator said that those numbers can be obtained but he did not have them right now. *A member also asked through what channels the program promotes these publications.* The Moderator explained they are published via Medium (blogs), and several platforms for podcasts (e.g., YouTube, Spotify, Apple Podcasts). Twitter and LinkedIn are used for amplification and awareness. *A member asked about a particular blog focusing on the Log4Shell event.* The Moderator and Board membership debated details of the related vulnerability and some of the content in the blog.

Action: The Moderator will connect Steve Christey Coley (CWE/CAPEC Technical Lead) with the Board members via email to discuss the blog contents and determine a course of action.

The Moderator provided an overview of survey results that were received over the previous months with respect to the CWE/CAPEC program community engagement publications (i.e., blogs and podcasts). The Moderator then provided an update on the CWE/CAPEC User Experience Working Group (UEWG) and its recent activities. The group was established in late Summer 2021 and has initially focused its efforts on formally defining CWE/CAPEC "user personas", or user types, as well as their respective use case scenarios and needs. The Moderator gave the example of the user experience discussion around CWE/CAPEC entries regarding the <status> attribute for each entry. The community often misunderstood the meaning of the various status values (e.g., Draft, Stable), and so the group/team decided to remove this attribute from entry pages. It will remain in the XML data for the team to facilitate completeness and other research, but the "status" of each entry will be removed from the public facing webpages for CWE and CAPEC entries. The Moderator provided an update on the upcoming UEWG plans including continued efforts to formally define (and subsequently share/publish) CWE/CAPEC User Personas, discuss possible content expansion areas (e.g., cloud, ICS), and begin identifying ways to better connect user persona needs to content presentation. *A member asked if we could better track the various community groups that we have and what they are actively doing*. The Moderator agreed and pointed out the existing areas where they are tracked and visible. *A Board member brought up an old document published on behalf of DoD related to software assurance and detection methods for various CWEs. The member suggested we find that document and update it with respect to all the recently published, new CWEs. Another member suggested we standardize the community groups in a new way on the website such that people can read about them, their objectives, and how to get involved.* The Moderator agreed that would be helpful.

Action: The Moderator will go back to the team and begin to develop standardization for SIG/WG awareness on the sites.

The Moderator provided an update as to the HW CWE SIG and its recent activities including new entry development, domain expansion (e.g., indicators of non-conformance, tamper, etc.), technical discussions, and debates on delineating between HW, FW, and SW content on our sites.

The Moderator provided an update on the continued preparations for publishing the 2022 CWE Top 25. This included an overview of the NVD data set contents, coordination meetings with the NIST NVD team, and timeline planning. *A member requested if it was possible for us working with the NVD team to improve CWE-mapping to HW entries when appropriate*. The Moderator said that he can follow up on that. *A member asked for clarification on the 2022 Top 25 dataset – specifically, what CVE data is in it.* The Moderator clarified that the data set contains what is in NVD over the previous two calendar years at a fixed date in time. This date (when the NVD data is pulled and analyzed) is published along with the Top 25. *A member asked if the Board should suggest a 'vignette' for a new Top25 product that focused on weaknesses in a new contextual domain*. *Top 25 data is biased in certain ways (e.g., widely disclosed), and one thing to consider is the many weaknesses that don't make it into the list. The member asked for deliberation from the rest of the Board on such possibilities as weaknesses related to web applications, hardware, mobile applications… is the necessary data for such new lists available?*

The Moderator provided an update on planned content publications including CAPEC 3.7 and CWE 4.7. This included new weakness/attack pattern content, increased entry details in several domains, and the aforementioned status attribute issue.

Item 4: Board Membership

The Moderator brought up the inactive Board member and explained the efforts undertaken to contact them. *The members agreed that more efforts should be undertaken to contact the member before any action is taken.* The Moderator turned the floor over to a member to discuss the nomination of a new Board member.

A member formally nominated a candidate to the CWE/CAPEC Board. The Moderator said there will be an interview opportunity for the Board members to ask the nominee questions, and that they should be on the lookout for an invite to come.