CWE/CAPEC Board Meeting #9

Friday, June 3, 2022 from 12:00 PM to 2:00 PM EDT

Members in Attendance

Board Members	**Organization**	**Attended**
Alec Summers	MITRE (CWE/CAPEC Board Moderator)	✓
Alex Hoole	Micro Focus	✓
Bill Curtis	Consortium for IT Software Quality (CISQ)	✓
Chris Eng	Veracode	✓
Chris Levendis	MITRE	
Chris Turner	National Institute of Standards and Technology (NIST)	
Jason Fung	Intel	✓
Jason Lam	SANS	
Jason Oberg	Cycuity	
Jay Gazlay	Cybersecurity and Infrastructure Security Agency (CISA)	
Jeremy West	Red Hat, Inc.	✓
Joe Jarzombek	Synopsys	✓
Kurt Seifried	Cloud Security Alliance	
Paul Anderson	GrammaTech	✓
Robin Gandhi	University of Nebraska Omaha	

Guests	**Organization**	**Attended**
Adam Cron	Synopsys	✓
Dave Morse	MITRE	✓
Gregory E. Shannon	INL	✓
Luke W Malinowski	MITRE	✓
Rushi B Purohit	MITRE	✓
Steven M Christey	MITRE	✓

General Discussion/Agenda

The moderator welcomed new Board member, Jeremy West (Red Hat).

Item 1: Report from CWE/CAPEC REST API Working Group

The working group Chair and Vice-chair presented on the Goals, Membership, group Status, and their plan for Content. The group's focus is to support automation via the crafting of RESTful API syntax and semantics for accessing CWE and CAPEC web services.

The presenter mentioned the example the recent Accelerate SA EDI standard which has some links to CWE. This working group was approved to start in March, 2022 and held it's first meeting on April 11th. Meetings are weekly at 09:00 AM, EDT. The group uses a MITRE hosted mailing list as well as GitHub. Group members agreed that "backend" database management decisions will be managed by MITRE. The format of the "response" will be JSON and is planned to be STIX compliant. One of the tools being looked at is GraphQL. Near term work includes defining use cases and milestones.

A member asked whether versioning and version control has been or is being planned for the schema. The presenter replied that, yes, that is the intent.

A member asked whether this will be purely a read only RESTful API, or whether it will support write operations. The presenter replied that the current interface is read only.

A member asked for an overview of the industries represented by the working group members. The presenter replied that it includes EDA, government, security, hardware. *The member then asked whether it is anticipated that software companies will also participate*. The presenter replied yes and that they expect to have prototypes for the community to use by next summer.

Item 2: Report from CWE-CAPEC ICS/OT Special Interest Group

The moderator gave background on the startup of this group, approved in February and having its first meeting on May 18th. The first meeting was unexpectedly large with approximately 140 attendees. The group as both public and private GitHub repos. The listserv has approximately 142 members. Discussion is ongoing whether to split the group for better operational cadence and process. The presenter then described this group as expected to have near term impact on CWE/CAPEC. This is informed by the congressional mandate for a cyber informed engineering strategy. The group's work plan includes review of recent CWE work and making further incorporations, in alignment with current content and submission requirements. Exploring weakness advisories to address information gaps present in manufacturing infrastructures.

The moderator mentioned the possibility of expanding the groups scope around the types of weaknesses and a member added that one example, hardware left unattended on a loading dock, is a weakness not currently in the scope of CWE. It introduces another domain.
There then followed discussion of the difficulty of developing an ontology.

The moderator mentioned the idea of going to the Board to propose a working group just on the problem of scoping.

A member mentioned the importance of knowing the target audience - scoping should consider who the ultimate consumer of the information is.

Item 3: Report from CWE/CAPEC User Experience Working Group

The moderator announced a new community co-chair. The group is restarting monthly meetings and focusing on harmonizing the definitions of key common terms. Also, they are working on the formal definition of user personas for publication on the CWE website.

A member brought up the need to be aware of the different audiences or consumers and accessibility of the data.

The moderator then described the UEWG definitions issue, or the variety of definitions across industry; Vulnerability, Weakness, Attack Pattern. The hope is to have something actionable on this relatively soon.

A member suggested the proposed definition of weakness goes too far.

A discussion ensued, including whether coming up with a grammar and a set theory was necessary. The risks involved with re-defining were discussed.

Item 4: Report from HW CWE Special Interest Group

The Moderator announced that the group has moderators that facilitate it. The group meets monthly and remains productive between meetings. There has been recent interest amongst the members for creation of a new HW CWE category relating to Physical Attacks. The group continues to work on submission in the queue, discussions of Scope Exclusions, refining of schema, and restructuring a new category.

A member asked for clarification of the schema change. The moderator described the removal of "IP" addendum to technology name.

Item 5: 2022 Top 25 Most Dangerous Software Weaknesses

The Moderator welcomed the technical and team leads for the effort. The list will be published on June 28th. It is built using CVE data within the NVD from the previous two years. The team preforms remapping against approximately 40,000 CVSS scores to develop the top 25 CWEs. Approximately 700 mappings remain to be done to meet the publication date.

A member shared that improvements in the mapping process, such as removing some categories and looking at higher level classes, have reduced the mapping work load. However, mapping issues remain, such as incorrect application of weaknesses when they are not actually causative. They also mentioned that it is one week out from the "freeze" to the list.

A member asked if the data could be made available for further analysis along with the vignette discussion. The moderator responded that it was a good idea and has been in discussion and may have additional utility in combination with the DHS Known Exploited Vulnerabilities list.

Item 6: CWE Content

The Moderator stated that the next release of CWE Content will accompany the Top25 release. It is a minor release with some description changes related to discussions in the last Board meeting. Updates were given on the new Web-submission capability and efforts to simplify submission. Plans for post-Top25 publication include establishing a transparent community platform for support collaborative work, working on queue items and revamping presentation filters.

A member asked whether the idea is to have the ability to submit new CW proposals. The moderator responded that it is. A discussion followed to that the goal is to break submission into stages, making it easier for initial submission with decision steps to reduce effort if the submission may not actually qualify as a CWE.

A member noted their support for a "viewing period" for community comment on entries prior to maturing to release candidate. This supports transparency and provides a timeline for feedback.

Item 7: CAPEC Content

The Moderator stated that the user experience working group and the CAPEC summit in February had discussions about the need for clarification on definitions within the descriptions of entries. Approximately 140 entries have been clarified so far. Via the Working Groups, identifying opportunities for other content development in focus areas such as hardware, supply chain, and penetration testing. A request to include a Vendor Page highlights an area that has opportunity for streamlining the process of CAPEC tools validation and inclusion.

Item 8: CAPEC Community Engagement

The Moderator described initial efforts at engaging academia stakeholders with a forum to be held on June 8 on security focused curriculum. Also, initial collaborations with several tool vendors in penetration testing have resulted in some success in mapping tool findings to CAPEC entries. There is strong interest in a common language for penetration testing findings.

A member commented that test completeness is important in penetration testing and that CAPEC can play a role. The moderator responded that this is an opportunity to tie this not only to CAPEC, but to all the information such as product security, network, and physical.

Item 6: CWE/CAPEC Board Charter/Operations Discussion

The Moderator raised the topic of voting mechanics and voting for a nominee to the Board. Reference was made to the language of the charter. Further discussion on this particular vote will be via emails with the Board members.

A member commented that "silence is concurrence with the outcome of those who voted". The moderator responded that there was not enough time for debate during this meeting, but that discussion could continue via email.

The moderator described difficulty in contacting a Board member to discuss participation. Mention was made of options provided in the charter. Discussion of a path forward to be discussed via email.

A member commented that members count towards quorum and thus participation is important. The moderator agreed with that point, then thanked the attendees and noted the next meeting would be in September.