CWE/CAPEC Board Meeting #11

Tuesday, February 14, 2023, from 3:00 PM to 5:00 PM ET

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	Synopsis	✓
Chris Coffin	MITRE	✓
Gananand Kini	MITRE	✓
Luke W Malinowski	MITRE	✓
Matt Luallen	Illinois University	✓
Przemyslaw Roguski	Red Hat	✓
Rich Piazza	MITRE	✓
Stephen Bolotin	Nexight Group	✓

Agenda

- Welcome and Housekeeping (3:00PM)
- CAPEC (3:05PM)
- CWE Submissions and Content Development Platform (CDP) Status (3:25pm)
- Open Topic Discussion (3:45)
- Community Updates (4:00PM): ICS/OT Special Interest Group, User Experience Working Group, HW CWE SIG, REST API Working Group

Welcome and Housekeeping

- The Board was asked to think about the current quarterly meeting cadence and whether it should be revised. Options include: an hour per month, an hour and a half bi-monthly, keep current cadence and add voluntary monthly sessions (with read-out materials), etc.

CAPEC

- A reminder of the CWE/CAPEC Program strategy was provided: Increase program adoption and program coverage through effective community engagement.
- Refresher from the last Board meeting (Sep 2022):
    - CAPEC Summit did not catalyze stakeholder engagement in major way.
    - The community has been less willing to contribute to CAPEC than CWE.
    - CAPEC is not widely adopted in these strategic focus areas: HW, Pen-Testing, Supply Chain.
- While there are small pockets of community interest, there is little evidence of broad-based community adoption and participation, for example:
    - Since the summit, there has been one major modification submission and a couple text/grammar submissions. Also, only two submissions focused on a new attack pattern.
    - Minimal expansion of adoption coverage in strategic focus areas, virtually no feedback in any major way on the supply chain view.
    - Pen-testing vendors are developing capabilities without CAPEC, and customers are not asking for CAPEC related information in the vendors capabilities.
    - There's been minimal interest in the HW SIG in developing content.
- Next steps:
    - CAPEC will be a low priority going forward.
    - The Board was asked to provide their thoughts on what to do with CAPEC in the future. An initial list of options was presented:
        - Host CAPEC site on a server with banner of halted maintenance and development.
        - Use open source for maintenance and development (GitHub, others?)
        - Transition CAPEC to a willing organization for maintenance and development (e.g., Canadian Centre for Cybersecurity)
    - Question: Who is the intended CAPEC audience? And related, why is ATT&CK adoption more successful than CAPEC? Comments from meeting participants:
        - ATT&CK is more mature and CAPEC needs more time?
        - More MITRE support for ATT&CK?
        - CWE focuses on weaknesses and CAPEC looks at how to chain/relate weaknesses together to identify patterns. Maybe more CWE maturity (e.g., better record data) would help CAPEC use/adoption.
    - Other member comments:
        - As a long time CAPEC supporter, has seen little evidence of CAPEC usage by customers. Agree with deprecation and just keep the site up (unmaintained).

        - Want to maintain the CAPEC corpus, but without centralized curation.
        - Knowing who will be disappointed with CAPEC deprecation would help inform next steps.
        - Recommend maintenance mode only, low priority, reconsider if interest comes back.
        - Be careful with CWE links to CAPEC. Could impact the quality of the CWE site if it links to information that has not been maintained.
    - An out of band meeting will be scheduled for additional discussion and a vote on how best to proceed with CAPEC.

CWE Submissions and Content Development Platform (CDP) Status

- A content development goal is (1) helping the user community better navigate and understand the submission process, and (2) improving the ability to track submission status so anyone in the community (not just the submitter) can view the working queue and see submission status.
- Another content development goal is to use Crowd-source content development to better scale the program and leverage community expertise.
- Progress since last meeting:
    - An initial web form submission server was established.
    - Formalized what the entry development process looks like, the requirements for each stage in the process and how to process through them.
    - Developed boilerplate language for common submission problems.
    - Started developing CWE scope exclusions to better clarify what is covered in the program. In work with the WGs and SIGs.
    - Completed internal approval process for Google Services platform hosting.
- The list of scope exclusions from the WGs and SIGs was presented. Target to finalize and publish soon.
- An overview of the CWE submission process was provided. The process has four stages (Initial Proposal, Final Proposal, Production, Publication) and phases within each stage.
    - Important to recognize that the program can now track submissions through these stages. This will improve transparency on the content development platform.
- Common submission issue examples: poorly written, too specific, scope exclusions not well defined.
- Visuals (charts) were presented for: Submission Status (Open/Closed), External Submissions – Phases, and Submission Problems.
- Submission Problem Categories / "Quality" Issues were displayed. Related to common submission issues – more comprehensive.
- Content Development Platform:
    - Goal is to increase transparency and leverage community and get away from the email engagement.

    - Began Google Services platform testing and GitHub testing, searching for balance between GitHub trackers for optimized community input/discussions and Google Docs for document development.
    - Team training has begun on support.
    - Set up cwe-submissions@mitre.org email account for program communications.
    - Identifying ways to assign submission phases into the CDP.
    - Want to start using some of our recent submitters for volunteer testing. A request will be sent out.
- Question: Who has visibility into initial stages of CWE submissions? Is it just the content submitter and MITRE? Currently, that is correct, but the plan is to expand visibility.
- Question: Why wouldn't the program want stakeholders to submit content in the form of the grammar of the XML schema directly? Need to give thought to incorporating the XML development first.
- Question: Program wants to increase transparency, define more rigorous process and allow tracking. These are good but come at the expense of adding overhead to your team. Is that additional overhead justified, and does it help the achievement of getting from idea to content published more quickly? Answer: More decentralization, e.g., crowd sourcing, also relieves the team of being the only ones able to respond to the community, and serve as arbiter of good content.
- Question: Does CVE provide a template or samples of a good entry/submission? Answer: There are many examples, and guidelines for submissions will ultimately be updated.

Open Topic Discussion

- Comment: The recent release of CWE and it's inclusion of CWE 1395 and the update to 1357, highlights a deficiency in CWE in terms of being able to address multiple communities. There's a no meaningful way to determine whether a particular CWE is relevant to a particular audience (e.g., software, hardware).

Community Updates

- ICS/OT Special Interest Group
    - Matt Luallen was introduced as the new co-chair.
    - Consistent growth with robust engagement and discussion.
    - Two new working groups: (1) Boosting CWE Content (focused on improving CWE’s ICS/OT coverage), (2) CWE to ISA 62443 (mapping exercise between CWE and a key cybersecurity standard.
        - Boosting CWE Content has 5 task groups reviewing the 20 SEI ETF categories and mapping them as clearly as possible to existing CWEs. Some findings were incorporated into CWE 4.10. Next steps are to complete the work and report results.
        - CWE to ISA 62443 has determined the top 10 CWEs (most exploited) in ICS/OT. Large task, there are over 1,000 pages associated with this standard. Some findings were incorporated into CWE 4.10. Next steps are

to complete the work and determine next CWEs to map. The mapping spreadsheet used by the group is a living document, not final.

- User Experience Working Group
    - Przemyslaw Roguski was introduced as the new Community co-chair.
    - Chris Coffin was introduced as the new CWE/CAPEC Team co-chair.
    - Recent activities include developing User Stories to accompany User Personas, finalizing User Persona definitions, defining community engagement strategy, and supporting content customization.
    - Purpose of User Personas is to inform the user base about who CWE is designed to serve. Currently six User Personas: Educators, Technical Writers, Security Researchers/Analysts, Hardware Designers/Verification Engineers, Software Developers/Assurance Engineers, and Security Architects. Two are under consideration: Management / Risk Owner, and Incident Response Engineer.
    - User Stories complement User Personas to help users identify with one or more particular roles. User stories help a user understand how CWE data may be helpful to them. A user story must articulate a business problem, consider the user persona’s responsibilities, and demonstrate the value brought by using CWE data. An example user story with a Security Architect and Software Developer was shown for the same use case. Volunteers are helping write additional user stories and other volunteers are welcome.
    - An overview of the custom CWE presentation filtering capability was provided. This capability will help users better target specific data of interest from the corpus.
- HW CWE Special Interest Group
    - Highlights since the last Board meeting:
        - CWE 4.9 and 4.10 were released.
        - Changed over 400 CWE descriptions to replace “software” with “product” to better allow the scope of those CWEs to include hardware.
        - Changed categories and relationships in the Hardware View (CWE-1194).
        - Improved names, descriptions, and/or demonstrative examples of multiple hardware weaknesses.
        - Recategorized several hardware CWEs as a result of the new CWE-1388: Physical Access Issues and Concerns.
    - Working on microarchitectural weaknesses specifically related to transient execution. Started with a clean slate; did not look at existing entries that mentioned microarchitectural weaknesses. Question: What is the timeline for completion? Answer: Goal is May release, but quality driven, not time driven.
    - Engaging and enabling the community update:
        - Encouraging more community involvement in CWE release planning (from HW side).
        - Implemented sub working groups for larger efforts.
        - Trying to invite guest speakers to SIG calls.

        - After experimenting with multiple tools (e.g., Box, Google Docs), selected GitHub to pilot collaborative editing capability. Seems to be catching on.
        - Encouraging more active involvement by the community to take the lead on resolving working queue items. Board members were asked to reach out to their networks for help identifying volunteers.
- REST API Working Group
    - Overview of working group goals and status:
        - (Partial) Craft RESTful API syntax and semantics to access CWE and CAPEC web services.
        - (Partial) Determine which content and in what format the server will deliver back to users.
        - (Acknowledged) Determine missing structure or content for particular use cases (e.g., for Accellera SA-EDI standard).
        - (Active Discussion) Support further automation requirements (such as versioning, etc.).
        - MVP telemetry to finalize above bullets (goals).
    - Current activity status:
        - Reviewing previous decisions, seeking telemetry from prototype before finalizing.
        - MITRE-internal beta server has been developed.
        - Working Group primarily seeks a test interface for prototyping against.
        - Contract mod to support AWS implementation proceeding.
        - Moving towards February MVP, awaiting MITRE Infosec approval for implementation.
        - Issues like versioning have been partly resolved.
    - Question: Is there an estimated timeline for the releases of these new feature sets or is that still TBD? Answer: It is TBD but want a beta version in the next few weeks or months.

Possible Voting Actions

- Board meeting cadence. Discussion will continue using email.
- Several requests from community about CWSS. Further discussion will take place via email and subsequent meetings.
- Board nominations – No members have nominations at this time.

Shareable Items

- Program will provide to the Board:
    - Scope Exclusions
    - ICS/OT CWE to ISA/IEC 62443 Draft Mappings
    - Ongoing Research RFI
    - Analytical Reports: “Current Weakness Trends in Publicly Disclosed Vulnerability Data,” and "Mapping Weakness Types to CVE Records: Challenges in Consistently and Accurately Identifying the Root Causes for Vulnerabilities.”