CWE/CAPEC Board Meeting #10

Thursday, September 29, 2022 from 2:00 PM to 4:00 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
Bob Heinemann	MITRE	✓
Gananand Kini	MITRE	✓
Gregory E. Shannon	INL	✓
Luke W Malinowski	MITRE	✓
Shadya Beatriz Maldonado Rosado	Sandia	✓
Stephen Bolotin	Nexight Group	✓
Steven M Christey	MITRE	✓

General Discussion/Agenda

The moderator introduced Dr. Robin Gandhi, the Board's newest member.

Next quarterly Board meeting will be in the first quarter of 2023.

Today's agenda may need an off-cycle meeting for continued discussion.

Agenda items:

- CAPEC: Current Status and Moving Forward
- Strategic Discussion: Weakness Mapping
- CWE External Submissions Process and Content Development Platform Status

Commented [AR1]: I'm assuming this is the Paul showing as 'guest' in the spreadsheet (without any identifying info).

- Community Working Groups Update

Item 1: CAPEC: Current Status and Moving Forward

CAPEC provides a common language for attack patterns in collaboration with CWE. Program typically does biannual releases. A community summit was held in February and was well attended. Its purpose was to explore future areas of focus for the program and encourage broader membership and participation. An interesting data point was that two thirds (2/3) of the attendees cited either no familiarity with CAPEC or limited use of CAPEC.

Current activities are focused on engaging the community to drive modernization in content development and increasing adoption. Specific focus areas include expanding hardware coverage via engagement with the Hardware CWE SIG; engaging the penetration testing vendor and stakeholder community; supply chain content development; and improving community education about CAPEC, CWE, and CVE by working with academic partners.

Reflecting on recent impact, CAPEC has incomplete integration with CWE, the summit did not change stakeholder engagement in a major way (unlike the vendor compatibility summit two years ago), and the community has been less willing to contribute to CAPEC relative to CWE (e.g., no feedback from listserv email preview of the new Supply Chain Lifecycle view in CAPEC v3.8).

Options for the way forward were presented. Additional input included: better messaging about the importance of CAPEC to CWE (explain the relationship better, including relationship with CVE), encouraging the establishment of a ‘stub’ even with incomplete information, increasing hardware-related content, providing better education on how CAPEC can supplement service provider testing, and better integrating with existing penetration testing tools.

Item 2: Strategic Discussion: Weakness Mapping

Weakness analysis for vulnerabilities is valuable because it gets to the root cause and can help eliminate or minimize the vulnerability in the first place.

There was discussion about the Top 25 Remapping Analysis (mapping between CWE and CVE). Remapping is based on the availability of real-world data. It’s important to get the wider community to identify root causes more accurately when they're reporting.

Problems with CVE data include few details and references when the CVE is new, descriptions focused on impact and not root cause, and low percentage of CVEs with a CWE mapping (often incorrect).

There is also lack of demand for understanding root weaknesses (there is more interest on impact). A better understanding of the distinctions among technical impact, attacker prerequisites, and weakness is needed. Other issues include difficulty identifying the correct weakness (CWE structure and hierarchy is complex), challenging site navigation, and lack of clarity for CVEs with multiple CWEs.

Possible next steps discussion included the idea to require a CVE to identify an associated CWE (to be discussed among CNAs, but not a good idea for independent researchers (better tools needed).

Member comments included: encouraging a best guess identifying an associated CWE at the time of record creation, with the expectation that revisions be made within a certain period of time; asking for a "precision rating" when assigning a CWE(s) to a CVE; providing a ranking of confidence in the identified CWE, and the potential for using AI to help with the ranking; vendors have an accountability to make sure that the CWE is accurate, and that may mean revising in the future.

Item 3: CWE External Submissions Process and Content Development Platform Status

An overview of recent activities related to external submissions was presented. Examples included formalizing CWE scope exclusions, initiating the build of internal capabilities to track and report on submissions, and developing email templates for common status messages.

An overview of the submission process was provided (3 stages: Proposal, Production, Publication). Consultation with the submitter for better understanding of the submission requires the most back and forth. This can happen between proposal and production, and between production and publication.

An overview of submission problem categories / quality issues was provided. The key point is that the program now has problem categories, and knows which ones are the most serious or not.

A recent analysis of 15 submission problems showed that seven had a relationship problem (not clear how the CWE related to other CWEs). The program is using more automation and tracking to help watch for trends, get a better sense where delays are, and where improvements could be made.

Item 4: Community Working Groups Update

CWE/CAPEC ICS/OT Special Interest Group. The listserv has 167 members and includes international participation. Two working groups were launched (community-led) to get into details related to the SIG (Boosting CWE Content and CWE to ISA 62443). CWE v4.9 (October 2022) will include new ICS/OT related content updates. Participation at SIG meetings has been very broad, including asset owners and operators, manufacturers, vendors, security professionals, academia, and there has been representation from Asia, Middle East, Europe, and North America. A third working group focused on education and training is planned for later this year or early in 2023.

CWE/CAPEC REST API Working Group. Current membership size is 36. Significant progress has been made crafting RESTful API syntax and semantics to access CWE and CAPEC web services. There is on-going discussion on how to determine which content and in what format the server will deliver back to users. Other activities mentioned: reviewing previous decisions; continuing MITRE-led development work; Waiting on contract mod to do implementation in AWS; moving towards December MVP which is more expansive than original MVP design.

Commented [AR2]: Could not follow this discussion well.

CWE/CAPEC User Experience Working Group. Three focus areas over the last couple months: finalizing user persona definitions for publication on CWE/CAPEC websites (estimated delivery: October, pending approval); modernizing CWE & CAPEC presentation filters (estimated delivery: October 13); and harmonizing definitions for key terms (estimated delivery: October, pending approval). There are six user personas, and there is some overlap, similar use case scenarios, similar information needs. *A member commented that the personas seem more like "profiles" based on their descriptions and are not very detailed.* The four presentation filters are: conceptual, operational, mapping friendly, and complete. These are pre-set views to help users find the information they're looking for. Future releases may include additional filtering capabilities, e.g., user-defined filters. A follow-on email will be sent to members about harmonizing definitions. *A member commented that it would be helpful if members could exercise the presentation filters to provide feedback. This not currently possible due to the system being on the MITRE network (demos have been used in the past), but potential solutions can be investigated.*

HW CWE Special Interest Group. Working to increase the engagement of the SIG in the quarterly CWE release cycle, from planning to execution to release. Presented information on the SIG's Microarchitectural Weaknesses Rework initiative.

Commented [AR3]: Could not follow this discussion well.

Other

A member mentioned that there seem to be a lot of recent CWE entries where language is either not relevant or language is not what would traditionally be under CWE. May need some consideration moving forward as CWE expands into hardware infrastructures, code, supply chain type issues.

The moderator introduced the idea of moving to a monthly board meeting schedule. An email will be sent for further discussion on this topic.