CWE/CAPEC Board Meeting #12

Friday, June 2, 2023, from 12:00 PM to 2:00 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	Synopsys	
Bob Heinemann	MITRE	✓
Bryan Owen	Aveva	✓
Chris Coffin	MITRE	✓
Gananand Kini	MITRE	✓
Howard Grimes	CyManII	✓
Luke W Malinowski	MITRE	✓
Matt Luallen	CyManII	
Przemyslaw Roguski	Red Hat	
Rich Piazza	MITRE	
Stephen Bolotin	Nexight Group	✓
Steve Christey Coley	MITRE	✓

Agenda

- Welcome (12:00PM)
- Improving CVE-to-CWE Mapping (12:05PM)
  - Discussing CVE data, CWE complexity, technology
- CWE’s Role in the Vulnerability Management Ecosystem (12:45PM)

    - CISA’s “Secure by Design / Secure by Default” Strategy
- Community Updates (1:15pm)
    - User Experience Working Group (1:15pm)
    - ICS/OT SIG (1:25 pm)
    - REST API Working Group (1:35 pm)
    - HW CWE SIG (1:45 pm)
- Housekeeping (1:55PM)
- Adjourn (2:00PM)

Improving CVE-to-CWE Mapping

- Weaknesses are the root causes of vulnerabilities. Understanding and avoiding weaknesses as early as possible in the product life cycle is better for everyone involved.
- To understand the weaknesses that result in vulnerabilities, weaknesses must be accurately mapped to each vulnerability.
- Mapping to root cause weaknesses is not done consistently and accurately at scale throughout the community. The number of CVE records is growing every year and we’re seeing many of the same kinds of mistakes being made.
- Mapping problems:
    - Often, users of the information are focusing on remediation and not necessarily the root cause. The root cause analysis may not be worth the effort to them, and it’s also not required data in a CVE record.
    - The CWE hierarchy and content is difficult to navigate for vulnerability mapping.
    - Limited technical capabilities to perform root cause analysis (labor intensive).
- Mapping solutions:
    - Improve CVE data by bringing together the CVE and CWE stakeholder communities (to include boards and working groups/SIGs) to develop solutions to increase accurate root cause mapping in disclosure.
    - Increase CWE usability by leveraging the User Experience Working Group to develop solutions for improving the CWE hierarchy and relationships to enable more consistent and accurate root cause mapping (e.g., improve guidance in scope and form, expand mapping notes throughout corpus).
    - Create community-driven solution(s) to help simplify the root cause mapping process to address the labor / expertise challenge. For example, get a vulnerability researcher to partner with the CWE community.
- Board comments:
    - We’re using the term “root cause” a lot. That may raise concerns for companies regarding their liability for indicated defects. Maybe just leave it CVE-to-CWE mapping. Or change to “contributing factor” to the generation of new CVEs.
    - Root cause is a well understood term, and industry standard term across InfoSec, so would be cautious moving away from it.
    - Consider adding a confidence level indicator for mapping. A lot of variability in the community in experience, capability level, etc.
    - Increasing push from customers/government to do things faster leads to our analysts going faster, which means it’s not always as accurate.

    - We use an internal report to review CVE mapping, and do a lessons learned to help coach the security analyst on how to improve.
    - I think we need to add some accountability measures for folks who submit the CVE. Consider named accounts.
    - Create a system that enables the community to propose, discuss, or even vote on the appropriate root causes of the CVE.
    - To reduce CWE complexity, need to find a way to reduce the number of entries (software side has 700 plus entries, hardware has about 100). Makes mapping difficult.
    - From the CVE perspective, a key starting point is with the CNAs, not the independent researcher community. That's based on experience and knowing who the good ones are and who is not thorough enough.
    - The development community has a vested interest in getting the CWE mapping right. Should be part of training regime.
    - Question: I noticed that putting a CWE as part of a CVE is not required. What if it was required and not optional? Or is there a reason it is not required?
        - Answer: Both programs believe that would make the quality of mappings worse. Currently, only about 40% of CVEs include a mapping to a weakness, and of those the majority are incorrect. Before making it required, we need to make it easier to identify the weakness(es).

CWE's Role in the Vulnerability Management Ecosystem

- Hope everyone had a chance to read the CISA document titled "Shifting the Balance of Cybersecurity Risk: Security-by-Design and Default Principles" referenced in earlier email.
- We want to move software assurance to the left in the product development life cycle. Lessen the burden on downstream users to identify product weaknesses that lead to vulnerabilities, and incentivize vendors to do more during design/development around security.
- Use both the CWE and CVE stakeholder communities to drive home the Secure by Design / Secure by Default strategy.
- The CISA document includes recommendations/tactics, such as memory safe programming languages and CVE record completeness (design), and mandatory MFA for privileged users (default).
- Comments and recommended actions to promote change:
    - I like that the report separates the design work. I think that's where CWEs can have a lot of impact.
    - A bit disappointed that CWE was only mentioned once (in a reactive way). CWE could be used more proactively, especially in the recommendations section.
    - From a vendor standpoint, we're struggling with scaling out across the entire product portfolio.

    - Provide guidance about specific actions to take to reduce weaknesses. Align the actions with a typical system development lifecycle (SDL) that most would be familiar with. The use of automation tools is important.
    - Engaging and educating the community should be a focus.

Community Updates

- User Experience Working Group
    - Working to create higher level guidance for new or casual users.
    - The recent CWE 4.11 release included an initial set of user stories and personas to help different types of users understand how to use CWE. Ongoing effort to add more to the set.
    - Created a New to CWE page which provides a brief overview of CWE and how it is used. It includes an example, and feedback so far is to consider adding more examples.
    - Thinking about creating short (~5 minute) videos with guidance on how to perform various tasks on the CWE web site, walk the viewer through certain features of CWE, or walk through certain use cases.
    - Suggestion to add a video for CNAs about how to do a better mapping to CWE. Find CNAs known for quality and solicit their input to share with the broader community.
    - We have personas now. Can we add domain-specific views and training to the videos? For example, web application security vs. database security. Identify common problems in the domains.
    - Add to videos about how to search CWE for an associated vulnerability.

- ICS/OT SIG
    - There are two current working groups. One is focused on boosting CWE content for ICS/OT coverage, and the other is mapping CWE to the ISA 62443 set of standards.
    - Several content updates that relate to ICS/OT were included in the CWE 4.11 release.
    - The boosting group launched last October. It is organized around five CWE Super-categories: ICS Communications, ICS Dependencies, ICS Supply Chain, ICS Engineering, ICS Operations. Want to boost information and breadth of CWEs in these categories. Results so far have been incorporated into CWE 4.10 and 4.11.
    - The CWE to ISA 62443 group launched last October and is organized around four sub-groups. The idea is to review CWEs to find mitigations in the 62443 standard that apply.

- REST API Working Group
    - We've been working on the REST API standard and the deployment of a prototype version to motivate finalization of the standard.
    - Need MVP telemetry from people working with the API to come to conclusions on the exact specifics of some of the requests and endpoints.
    - Current status:

        - MITRE internal beta server has been developed.
        - Working Group primarily seeks a test interface for prototyping against.
        - Planning to transition to AWS infrastructure after MVP publication.
        - MVP Production deployment attempt scheduled for Monday, June 5.

- HW CWE SIG
    - Been thinking about SIG expansion and potential strategic partnerships. We now have ARM participating which is good for micro architectural work. Want to focus on recruitment to fill out gaps in CWE HW coverage.
    - The last D3FEND update included mappings to some software CWEs on the Top 25 list.
    - Conducted an IEEE Hardware Oriented Security and Trust Tutorial Session (May 1) about "Designing and Building More Secure Hardware with CWE" and engaging the next cohort of potential SIG members. Lots of good feedback.
    - Ongoing research includes how resonant frequencies disrupt HW (Harmonic Faults) and microarchitectural weaknesses.
    - For microarchitectural weaknesses, there is a GitHub issues tracker and there have been a lot of contributors and updates to enumerate weaknesses. Next steps are to have ARM review and comment, and then finalize and close out for future release.
    - Planned activities:
        - Expand CWE-1384: Improper Handling of Physical or Environmental Conditions by adding additional base level CWEs.
        - Look deeper into crypto CWEs for hardware.
        - Speaking with MITRE Legal about adding HACK@Event demonstrative examples of HW weaknesses in HW CWE entries.
        - Considering when to publish next iteration of Most Important Hardware Weaknesses List.

Housekeeping

- CAPEC Update
    - Site is active, content development and community engagement on hiatus.
    - New CWEs will map to existing CAPECs whenever possible.
    - Awaiting MITRE Legal response concerning using open-source for ongoing development.
- Board Meeting Cadence
    - Should meetings be more frequent with a shorter duration? For example, monthly for an hour.
    - Send comments/thoughts via email.
- Common Weakness Scoring System (CWSS™) Summit Proposal
    - Mechanism for prioritizing weaknesses for remediation; Last updated in 2014.
    - Several requests from community (e.g., Board, UEWG) on this subject.
- Board Nominations
    - If anybody has any board nominations, please bring them forward.