CWE/CAPEC Board Meeting #14

Monday, December 18, 2023, from 12:00 PM to 1:30 PM ET

Members in Attendance

Board Members	Organization	Attended
Alec Summers	The MITRE Corporation (Board Moderator)	X
Alex Hoole	Micro Focus	X
Bill Curtis	Consortium for IT Software Quality (CISQ)	X
Bob Heinemann	The MITRE Corporation	X
Chris Coffin	The MITRE Corporation	X
Chris Eng	Veracode	X
Chris Levendis	The MITRE Corporation	X
Chris Turner	National Institute of Standards and Technology (NIST)	X
Gananand G Kini	The MITRE Corporation	X
Jason Fung	Intel	
Jason Lam	SANS	X
Jason Oberg	Cycuity	X
Jay Gazlay	Cybersecurity and Infrastructure Security Agency (CISA)	X
Jeremy West	Red Hat, Inc.	X
Joe Jarzombek	Synopsys	X
Kurt Seifried	Cloud Security Alliance	X
Matthew Luallen		X
Paul Anderson	GrammaTech	
Rich Piazza	The MITRE Corporation	X
Robin Gandhi	University of Nebraska Omaha	X
Steve Christey Coley	The MITRE Corporation	X

Agenda

- Welcome (12:00–12:05 PM)
- CWE Community WG and SIG Updates
    - User Experience WG (12:05–12:20 PM)
    - HW CWE SIG (12:20–12:35 PM)
    - ICS/OT SIG (12:35–12:50 PM)
    - REST API WG (12:50–1:00 PM)
- CWE Coverage Discussion
    - CWE and SW license-related issues, scope Exclusions (1:00–1:20 PM)
- Update on the CWE GitHub Submissions Repository (1:20-1:30 PM)
- Adjourn (1:30 PM)

User Experience WG (Chris Coffin)

- UEWG Purpose: A community-driven effort to identify areas where CWE content, rules, guidelines, and best practices must improve to better support stakeholder use cases and work collaboratively to fix them.
- Monthly meetings are held the last Wednesday of the month.
- Topics/activities
    - "New to CWE" series of documents (one currently)
    - CWE mapping guidance
    - CWE graphics/diagrams
    - Better CWE data representation to allow easier navigation for users
    - Discovering options for easier weakness selection
    - Defining community engagement strategy
    - CWE assignment to CVE improvements options
- Recent activities to support updates to CWE 4.13 include cleaning up some weakness metadata descriptions, and then various updates for mapping notes.
- We've been encouraging more member involvement, and it seems to be helping. There have been a number of member presentations related to work they have been doing with CWE:
    - An effort to data mine CWE projects. This work is going to be integrated with REST API WG activities.
    - The Co-chair published a blog recently about Red Hat's CWE journey. Topics were mapping based on the CWE-699 Software Development view, working to improve CWE assignments to CVEs (and participating in the new Root Cause Mapping (RCM) working group, and weakness risk-patterns detections (not related to Common Attack Pattern Enumeration and Classification (CAPEC).
    - Presentation on software quality and how it's tied to security issues, and how tools can be integrated to better show quality impacts on security and technical weaknesses.
- There is an upcoming presentation at this week's meeting about using visuals/graphical representations to help users better understand CWE. The content will be based on the Top 25. The presentation will also include thoughts on CWE language to help new users get up to speed more quickly.
- A "New to CWE" page has been up since early this year. Designed to be helpful to the more casual or new user. Additional content is expected to be added.
- Mapping guidance for aligning CVEs with CWEs has been available since 2021. It includes quick tips and examples. A new working group will focus on improving mapping. Limited feedback received from users of the guidance.
- Another recent meeting covered the graphical views (available as PDFs) we have for understanding the hierarchy of the different CWE views.
- Future activities: expand "New to CWE" series documents and examples; determine how best to incorporate graphical diagrams to educate users on CWEs; expand and update CVE-to-CWE mapping guidance; define additional and update existing CWE user stories; encourage more UEWG member presentations.

- A new initiative from the UEWG is a new working group to focus on improving CVE-to-CWE mapping.
- An underlying subtext around the primary role of the UEWG and its focus going forward is finding ways to update the website and infrastructure in a meaningful way.
- A new initiative is underway to create a new working group to focus on mapping CVEs to their CWE root cause weakness. They will look into the feasibility of implementing a decentralized mapping approach, guidance, and tools to make mapping easier. Proposal has been put forward to put this topic on the agenda for VulnCon in March.
- Comment to consider using multiple raters to arrive at a consensus for the mapping.

HW CWE SIG (Bob Heinemann)

- Selected HW CWE SIG Meeting Topics since June. We've been looking at ways to make the meetings more engaging and informative. General categories of topics:
    - Informational (Becoming a CNA, D3FEND and Hardware Coverage, CVE QWG Hardware and Software Tagging – Proposal)
    - Research (Weaknesses dealing with HW initialization [Nordic APPROTECT], Resonant and Harmonic Based Weaknesses)
    - Discussion (Missing Initialization Weakness Sneak Preview, Inclusive Language and HW CWEs, Covert Channels and CWE.
- New HW SIG Members since June
    - Current membership is 131 members (based on email addresses in the membership list). Have added 13 new members.
    - The top three membership categories are industry, semiconductor, and academia.
    - Over 45% of the members are from industry, e.g., Microsoft, Dell, various security companies.
    - Semiconductors comprises over 25% of the members, e.g., AMD, Broadcom, Lattice.
    - Academia includes professors, students, and anyone with .edu in their email address.
    - About 5% of members are from the US government, mostly CISA. A couple of National Labs are also part of the membership, including Sandia and Los Alamos.
    - Current membership is more represented in the chip and hardware design space than in storage.
    - Suggestion was made to intentionally bring in members from different industries due to varying attack vectors.
- CWE Nit Bits
    - A recurring, short educational segment for SIG members.
    - Topics covered include CWE Key Concepts, CWE Mindset, Vulnerability Mapping Notes, Custom Filtering, Observed Examples, and Demonstrated Examples.
    - The next topic to be discussed is Composites and Chains.
- Microarchitectural Weaknesses Update

    - A new working group, facilitated by MITRE, has been formed with Intel, ARM, AMD, Cycuity, and Riscure on defining microarchitectural weaknesses
    - The group has been productive and has four initial submissions. These were generated with public input on Git Hub. We are working on compiling all the data generated into full submissions, which will be available for review, comment, and approval at the beginning of next year. Once approved, they will be added to CWE.
- HACK@DAC Demonstrative Examples
    - Many HW CWEs do not have code-based demonstrative examples (DEMOX).
    - Proposal was made to use HACK@DAC, a pre-SI HW capture-the-flag competition to populate DEMOXs. Academic partners, including Texas A&M and University Darmstadt, have been providing DEMOXs from this repository. They do the initial mapping, technical reviews, and generate the first draft of the demonstrate examples, which are then reviewed and edited for style.
    - Three DEMOXs were added in release 4.12, another 11 in 4.13, and nine are being worked for the next release.

ICS/OT SIG (Matt Luallen)

- The IST/OT SIG was launched in May 2022. The SIG has made hundreds of updates in CWE 4.11, 4.12, and 4.13. More are planned for the next release.
- Have many group and sub-group meetings. In 2024, moving to monthly meetings.
- The number of participants has doubled from the low hundreds to around 250, partly due to personal socialization of the effort and opportunities to present at conferences.
- Five task groups (ICS Communications, ICS Dependencies, ICS Supply Chain, ICS Engineering, and ICS Operations).
- Mapping to 62443 has been valuable due to its widespread use in numerous verticals and support. Four individual CWEs resulted from this effort.
- Going forward, additional CWEs need to be enhanced, and there will be a focus on recruitment.

REST API WG (Rich Piazza)

- Established in 2022. There are 45 members, e.g., Synopsys, Cadence, AMD, Intel, Home Depot, Attack Forge, that have helped develop the specification.
- Deployed an initial minimum viable product on a MITRE server in June that was used for initial testing by working group members. Pulled down in July, due to a MITRE policy change around external facing capabilities. Moving toward an AWS implementation.
- The API architecture is going through MITRE approval process. We have the docker containers of API code, and we will be deploying them this week to ECS instances.
- CWE infrastructure. The code for creating and deploying the website has been modernized. Implemented the Hugo framework for updates, which significantly reduced the website generation time from hours to a minute or two. Have also been working on the content submission web form, which allows users to suggest changes to existing

CWEs. The new form will be launched as part of the Content Development Repository early next year.

CWE Coverage Discussion (Alec Summers)

- Improper software licensing was determined to be out of CWE scope in 2018; it was considered to be a policy/programmatic exploitation. However, there has been recent discussion on the listserv about reconsidering this position. What does the Board think, what are exclusions of scope? Comments, questions:
    - Consider (for both HW and SW) fitness for use, a very important thing for supply chain risk management. Licensing is a way that we understand if a product or component is fit for use. We should not be silent about that.
    - Until we can both define and deliver cybersecurity related weakness types, should we be considering scope expansion of the program to include licensing?
    - If we're going to cover things like licensing, do we also start covering social engineering attacks? Need to have a clear rationale for expanding scope.
    - The CWE scope has evolved (SW—Quality—HW), but there is no formal CWE scope statement. There is a page of scope exclusions in the CDR. A goal should be to define a scope of coverage and share it with the community. Also consider resource requirements associated with expanded scope.
    - Scope has been, more or less, defined on the definition of what a weakness is. What we have found in a lot of new submissions is that people stretch or don't follow that definition.
    - Question for the Board to consider: Everything in the CWE taxonomy solves a very specific purpose. It allows you to identify, categorize, associate and report, and then mitigate. And CWEs have a symbiotic relationship with CVE, so the question would be if we were to consider something like license as a weakness, does it enable a similar workflow?
    - There are many tools today that can identify licenses and license conflicts with the intended use.
    - When there's a buffer overflow, who's the responsible party for mitigating? If there's a licensing problem in your software stack in your transitive set of dependencies, who's responsible for fixing it?
    - Might be useful to examine what a licensing CWE would look like and what would it solve? What would be the use case that we would introduce?

Update on the CWE GitHub Submissions Repository (Alec Summers)

- Out of time. Alec will send the update.

Wrap Up and Reminders (Alec Summers)

- CWE v4.14 – TBD (February 2024 target timeframe)
- CWE REST API – Early 2024 release
- CWE Content Development Repository (CDR) – Early 2024
- Root Cause Mapping Working Group (RCM WG) – January 2024