CWE/CAPEC Board Meeting #3

Tuesday November 17, 2020 @ 1300-1500 EDT

Members in Attendance

Paul Anderson -- GrammaTech
Pietro Braione - Università degli Studi di Milano - Bicocca
Drew Buttner -- MITRE (CWE/CAPEC, Board Moderator)
Bill Curtis -- CISQ
Chris Eng -- Veracode
Alex Hoole -- Micro Focus
Joe Jarzombek -- Synopsys
Jason Lam -- SANS
Chris Levendis -- MITRE (CVE)
Jason Oberg -- Tortuga Logic
Kurt Seifried -- Cloud Security Alliance
Chris Turner -- NIST (NVD)

Review Recent CWE/CAPEC Accomplishments

- CWE/CAPEC blog on Medium
    - 2020 CWE Top 25 Analysis
    - Fixing Vulnerabilities Costs 100x More If You Don't Understand the Weakness
    - CWE-23: Starbucks misses a weakness, almost loses over 50% of their 2019 profit ($15B)

Review of Previous Action Items

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.02	Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.04	Request clarification from MITRE's general counsel regarding the ability for a non-board member to request the contents of a private list through the Freedom of Information Act or the Patriot Act.	Drew Buttner	In Progress	Assigned on 2020/08/06.
2020.08.06.07	Research options and establish an online meeting agenda collaboration capability.	Drew Buttner	Completed	Assigned on 2020/08/06.
2020.08.06.08	Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.09	Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.09.14.01	Create and propose a potential charter for the CWE/CAPEC Board.	Andrew van der Stock Joe Jarzombek Paul Anderson	Not Started	Assigned on 2020/09/14.
2020.09.14.02	Establish both a private and a public document repository.	Drew Buttner	Completed	Assigned on 2020/09/14.
2020.09.14.03	Contact AFRL and get more info about what they are trying to do.	Drew Buttner	Completed	Assigned on 2020/09/14.
2020.09.14.04	Respond to potential members and relay that board is coming up with a process.	Drew Buttner	Completed	Assigned on 2020/09/14.
2020.09.14.05	Conduct a doodle poll to pick a recuring day/time for CWE/CAPEC Board meetings.	Drew Buttner	Completed	Assigned on 2020/09/14.

Agenda with Discussion Summary

A) Use of Trello for Setting Agenda
- For this board meeting, Trello was used to capture potential agenda topics.
- Questions
    i. Was this helpful and should it be leveraged going forward?

The board found Trello useful and overall liked if for coordinating the agenda.

The column "Future Discussion Topics" is being viewed as a backlog of items that should/could be chosen for a future agenda. There was discussion about the need for a trimming policy as the "Future Discussion Topics" column will likely get overwhelming. There was mention of having one person (e.g., the Board Moderator) coordinate the space.

ACTION: The moderator will propose a short policy to guide the use of Trello and the setting of an agenda.

B) Charter Proposal
- Update from the working group putting together a proposed charter.

The working group was not able to put any time toward this. The action is being carried over to the next meeting.

There was discussion about if we wanted a single document covering both the charter and the bylaws. The board agreed that these should be separate documents as a single document gets long and unwieldy and separating them allows one to be modified / change without having to affect the other.

C) Upcoming Releases

- CAPEC Version 3.3 (Dec 17)
    i. 3-4 new attack patterns
    ii. a small number of new additional execution flows
    iii. review and streamline of descriptions that are considered too lengthy
    iv. a review of CAPEC<->CWE mappings
- CWE Version 4.3 (Dec 10)
    i. a set of new hardware-related weaknesses, likely 10+ minimum
    ii. 2-3 new software-related weaknesses
    iii. new data protection view
    iv. initial guidance material intended for vulnerability mapping

The board had no issues with the plan for these upcoming releases.

D) Release Roadmap
- Discuss the pros and cons of moving to a defined release schedule.
- Questions
    i. Should CWE/CAPEC adopt a set release schedule?
    ii. If adopted, what schedule would work best?

After the review of items scheduled for the upcoming releases, there was discussion about how items discussed by the board factor into the planning for a release. The understanding within the CWE/CAPEC team is that the topics addressed during these board discussions will shape the upcoming releases. The board is asked to oversee this and point out if this is not happening.

The board asked how release planning is currently done. Today, the planning is ad hoc. trying for 3-4 releases a year, scheduled around tasks (e.g., a release around the Top 25) and the amount of "stuff" that is ready.

The board agreed that it is more important to know what will be in each release, as opposed to focusing on a specific data. For example, knowing in Q1 the release will include the Top 25 and some new hardware content, and in Q2 the release will include XYZ.

The board also agreed that flexibility with the exact release date can be beneficial. It is valid to slightly push back a release to fit something addressing a current news item. With the tradeoff being that the other stuff in the release now has to wait.

Discussion about event driven releases was had. Allowing a "hotfix" release to address new threats should be possible.

ACTION: Establish and maintain a topic release schedule for the next 4 releases, post on public website, do not include a hard date but rather a timeframe like Q1, include a note that minor releases in addition to this schedule are still possible.

Discussion then shifted toward submission tracking. The board agreed with the need to enable visibility into the process that a submission goes through, and where a specific submission is within the process. One of the needed items within this process is a criteria for dismissal and how/when a submission is rejected.

The board would also like to see a capability for the community to share the load in content creation.

The board was in agreement that part of the submission process is a need to better define what is in scope for CWE.

ACTION: Create a proposal for a standardized content submission and tracking process enabling community visibility and shared effort into advancing submissions.

ACTION: Create a definition of scope that states what is allowed as part of CWE and what would be considered for rejection.

During the discussion around a release roadmap, and the notion that the board needs to keep a holistic picture in mind (not just focusing on metadata fields), the board asked for and update on a past project from NIST related to formalized weakness definitions.

ACTION: Reach out to Irena Bojanova (NIST) for an update on Bugs Framework and schedule a talk with the CWE/CAPEC Board.

E) CVE Root Cause
- Question
    i. Is there an opportunity to partner with the CVE Board to introduce a HW vs. SW root cause field into CVE?

Discussion on this started with a question about handling vulnerabilities that result from an intersection between hardware and software. There was also confusion about what the concern was. It was asked if this was specific to filtering between HW and SW.

Further discussion revealed a concern that for some vulnerabilities that involve both that only SW weakness are mapped. Need to find a way to avoid being too rigid. Need to provide clear guidance for those mapping.

ACTION: Work on proposal that can be brought to both the CVE and CWE/CAPEC Boards about high-level guidance for complex mapping between vulnerabilities and HW+SW weaknesses as well as the chaining relationships that may exist.

There was some discussion about a move to an ontology enabling more complex relationships to be defined. It was agreed that this is a future research topic.

F) Better Integrating CWE and CAPEC
- CWE and CAPEC currently exist as separate efforts. Each is centered around weaknesses, CWE about defining them and CAPEC about exploiting them. There is often confusion about what CAPEC is, and how to leverage it.
- Questions
    i. Should CWE and CAPEC be better aligned with each other?
    ii. How could we improve the value of each through integration?
    iii. Should they continue to be separate efforts, or be combined into a single effort?

This item was skipped due to time constraints but should be part of a future agenda.

G) CWE Compatibility / Effectiveness Testing
- Do we agree with the statement that the real value of CWE Compatibility is to differentiate tools and services in the marketplace?
- Does CWE want to be the leader in exposing differences to the community?

Discussion on effectiveness testing started around the fact this is a VERY hard problem, maybe the hardest problem that has been put on the table. The idea space is huge with a large number of languages, variants, etc.

It was pointed out that often two vendors may report different things and both vendors could be right. Solving this through testing is not often possible. There is a lot of history with this challenge within the NIST SAMATE project.

The board agreed that there is a general need this to verify claims by tools. It was mentioned that customers want this, they try to use Juliet, they almost always get it wrong. Customers will do it a bunch of different ways. Unfortunately, they may be using a test suite that has no similarity with the codebases they use or develop, and hence the testing is not relevant.

It was said that from a vendor point of view this is a minefield and a benchmarking effort will struggle to succeed.

Another point was made that what is reasonable is to establish better expectations around when it would be reasonable for a tool to claim effectiveness. Qualitative measurements as opposed to quantitative measurements should be pursued.

H) CWE and Data Protection
- An update on the work going on with a new Data Protection view

After an overview of the proposed view was given, a comment was made to explore using this view as an example to solve a more general solution beyond just data protection that results in privacy violations. No action was necessary at this time.

I) New Business
- Open floor for discussion.

No new business was brought forward.

Action Items Going Forward

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.02	Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.04	Request clarification from MITRE's general counsel regarding the ability for a non-board member to request the contents of a private list through the Freedom of Information Act or the Patriot Act.	Drew Buttner	In Progress	Assigned on 2020/08/06.
2020.08.06.08	Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.09	Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.09.14.01	Create and propose a potential charter for the CWE/CAPEC Board.	Andrew van der Stock Joe Jarzombek Paul Anderson	Not Started	Assigned on 2020/09/14.
2020.11.17.01	Create and propose a short policy to guide the use of Trello and the setting of an agenda.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.02	Establish and maintain a topic release schedule for the next 4 releases, post on public website, do not include a hard date but rather a timeframe like Q1, include a note that minor releases in addition to this schedule are still possible.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.03	Create a proposal for a standardized content submission and tracking process enabling community visibility and shared effort into advancing submissions.	Kurt Seifried	Not Started	Assigned on 2020/11/17.
2020.11.17.04	Create a definition of scope that states what is allowed as part of CWE and what would be considered for rejection.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.05	Reach out to Irena Bojanova (NIST) for an update on Bugs Framework and schedule a talk with the CWE/CAPEC Board.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.06	Work on proposal that can be brought to both the CVE and CWE/CAPEC Boards about high-level guidance for complex mapping between vulnerabilities and HW+SW weaknesses as well as the chaining relationships that may exist.	Jason Fung Jason Oberg Chris Turner	Not Started	Assigned on 2020/11/17.