CWE/CAPEC Board Meeting #2

Monday September 14, 2020 @ 1000-1200 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
Jason Fung -- Intel
Jay Gazlay -- DHS CISA
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)
Andrew van der Stock -- OWASP

Review Recent CWE/CAPEC Accomplishments

- CWE Version 4.2
- 2020 CWE Top 25
- CWE/CAPEC blog on Medium

Review of Previous Action Items

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.01	Circulate the CVE Board Charter to the CWE/CAPEC board members.	Chris Levendis	Completed	Charter link sent via private list
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.
2020.08.06.03	Establish a private, non-publicly archived email list for CWE/CAPEC board members.	Drew Buttner	Completed	List created.
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	Not Started	Assigned on 2020/08/06.
2020.08.06.05	Establish a capability to record the board meetings.	Drew Buttner	Completed	Recordings through Teams

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.06	Research and make a proposal for both a private and a public document repository.	Drew Buttner	Completed	To be presented at Board meeting
2020.08.06.07	Research options and establish an online meeting agenda collaboration capability.	Drew Buttner	Not Started	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.

Agenda with Discussion Summary

A) Bylaws
- Currently there are no formal bylaws.
    i. The Board was in agreement at the last meeting that bylaws are something that should be put together, and done so by the board itself.
- Questions
    i. Should a working group be established to create a proposed set of bylaws?

It was asked what the difference between bylaws and a charter was. A member offered that bylaws focus on how one forms something (e.g., membership / rules, elections, committees being set up) while a charter is less formal and focused on what a group does, and how does it do it.

The board was in agreement to start with a charter and then create more formal bylaws at a later time if necessary.

A working group was established to create and propose a charter for the CWE/CAPEC Board. The three members of the working group are:

Andrew van der Stock
Joe Jarzombek
Paul Anderson

ACTION: The working group will create and propose a potential charter for the CWE/CAPEC Board.

B) Document Repositories
- Currently there is no document repository for Board communication.
    i. The Board was previously in full agreement about the need for a member-only document repository.
- Proposal for both a private and a public document repository.

i. Set up a new GitHub organization named "CweCapec" using the free plan.
ii. Create a public repository named "board-documents" under the CweCapec organization to hold public board material such as the meeting minutes, charter, etc.
iii. Create a private repository named "private-board-documents" under the CweCapec organization to hold private board material such as meeting recordings, etc.

The board was in agreement with the proposal

ACTION: The moderator will establish both a private and a public document repository.

C) Hardware Vulnerability Database
- AFRL is collecting data to construct a Hardware Vulnerability Database. This database will enable the tracking of high-level descriptions of vulnerabilities and will be made available through the DoD's Trusted Silicon Stratus (TSS). Additionally, the intent of this HVD is to enable the cross functionality of assurance and design tools to validate the absence of known hardware vulnerabilities within designs and exemplars.
- Questions
    i. What do we know so far about this effort?
    ii. How does the AFRL proposal fit/conflict with CWE?
    iii.

The board discussed what is currently known / assumed regarding this effort. One question was if this was a classified database. Members of the board mentioned that any known hardware related vulnerability would likely be classified due to the challenge in patching/fixing such flaws. However other board members didn't think that the intention of the effort was to have a classified repo. The intent so far is just to survey the community to see what should be in such a repository.

Many board members see the two efforts as complimentary, similar to NVD and CWE. The efforts should be connected as there is potentially a lot of overlap.

ACTION – The moderator will contact AFRL and get more info about what they are trying to do.

D) Long term road map
- Currently planned CWE and CAPEC minor releases around the new year.
- 2021 CWE Top 25 in late spring / early summer
- CWE 5.0 on the horizon
- Questions
    i. What areas should be considered for focus / advancement within CWE/CAPEC over the next 2 years?

A board member stated the need to look at other standards and encourage them to adopt CWE/CAPEC more formally. There is a significant need for these standards to reference CWE/CAPEC more accurately. There is also the need to perform a gap analysis and

determine where CWE/CAPEC is falling short. A different board member pointed out that this task is difficult due to the many-to-many mapping relationships that exist, and the fact that there are a lot of standards out there.

The board was in agreement that more guidance is needed for how to accurately map to CWE. Is there a way to help a user select a CWE based on properties that have been provided? A member stated the need to help a user find / select the correct entry, for example maybe leveraging better searching / tagging, or maybe using machine learning on whatever search text was provided.

A board member presented the need to define what it means for a vendor to say they cover a CWE.

Another board member stated that every CWE should have an associated CAPEC. If it doesn't, and there is no way to attack it, then is that weakness of actual interest?

A board member mentioned the need for Top 25 for hardware.

A board member mentioned the need to expand the list of weaknesses about errors in business process.

A board member stated the need to update the currently demonstrative examples and add some for newer languages.

E) Board Membership

- There have been a few requests to join the board.
    i. The Board was in agreement at the last meeting that bylaws are something that should be put together, and done so by the board itself.
- Questions
    i. Is the current overall size correct?
    ii. When and how should new members be added?

The board felt that there was no current expectation to grow the board. However, it was also stated that they don't want restrict things to the current size. Instead of focusing on size, the focus should be on what differencing value would a new member bring. For example, adding a new member that represents a significant under-represented constituency.

The board was also in agreement that the process needs to be refined and should be part of the charter. The board should be very transparent about the process.

ACTION – The moderator will respond to potential members and relay that board is coming up with a process.

F) Participation Expectations (if time permits)

The board was in agreement to push this discussion to the working group establishing the charter, and to discuss the proposal once it is available. It was noted that the CVE charter

was potentially sufficient and that the working group should see if that language is reasonable for the CWE/CAPE Board.

G) Meeting Schedule
- Questions
    i. How frequent should future board meetings occur?
    ii. When would be a good day/time to set any regularly occurring meeting?
    iii. Board was in previous agreement that event driven meetings be an option when appropriate.

A board member stated the desire to meet before each release to go over what is being included.

The board suggested one last doodle poll to schedule a general day/time.

ACTION – The moderator will conduct a doodle poll to pick a recuring day/time for CWE/CAPEC Board meetings.

H) New Business
- Open floor for discussion.

A board member asked if published works pertaining to, or referencing, CWE/CAPEC were posted on the CWE site. This was clarified to mean links to the works, not the actual work itself. It was stated that the current CWE/CAPEC website has such a list, but that it is a bit out of date. Another board member brought up the challenge with maintaining such a list, someone has to maintain it, needs to vet the works, respond to a lot of requests to add works, and weed out those trying to take advantage of the list.

A board member suggested leveraging social media for this. The community can post what they want and tag CWE so others can find it. One can also search these tags for past works.

A board member mentioned that the CWE Top 25 is domain agnostic. The question was asked if something should be done about this? For example: Embedded, Mobile, Web. These domain lists could help get people be engaged. There was a suggestion for documentation about how the Top 25 should and should not be used.

A board member mentioned that it would be helpful to have good demonstrations on how to use CWE/CAPEC, how to find the correct entry, how to submit a new one, etc.

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	Not Started	Assigned on 2020/08/06.
2020.08.06.07	Research options and establish an online meeting agenda collaboration capability.	Drew Buttner	Not Started	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.
2020.09.14.02	Establish both a private and a public document repository.	Drew Buttner	Not Started	Assigned on 2020/09/14.
2020.09.14.03	Contact AFRL and get more info about what they are trying to do.	Drew Buttner	Not Started	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	Not Started	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	Not Started	Assigned on 2020/09/14.