HW CWE SIG Board Meeting #9

Friday July 9 @ 1230-1330 EST

Members in Attendance

John Bell – iRobot
James Bellay – Batelle
Mike Borza – Synopsys
John Butterworth – MITRE CWE
Matthew Coles – Dell
Kerry Crouse – MITRE CWE
Steve Christey – MITRE CWE
Amitabh Das – AMD
Iain Deason – DHS
Daniel DiMase - Aerocyconics
Farbod Foomany – Security Compass
Domenic Forte – University of Florida
Jason Fung – Intel
John Hallman – OneSpin Solutions
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Victor Ibe - Aerospace
Joe Jarzombek – Synoposys
Christina Johns – MITRE CWE
Peter Kertner – MITRE CWE
Gananand G Kini – MITRE CWE
Milind Kulkarni – NVIDIA
Mohan Lal – NVIDIA
Chris Lathrop – MITRE CWE
Lang Lin – Ansys
Bruce Monroe – Intel
Srinivas Naik – MITRE CWE
Jason Oberg – Tortuga Logic
James Pangburn – Cadence Design Systems
Naveen Sanaka - Dell
Andreas Schweiger
Alec Summers – MITRE (HW CWE SIG Moderator)
Paul Wortman – Wells Fargo

Announcements

Next meeting – Friday, August 6 at 12:30 pm EST

Minutes from previous meetings available at: https://github.com/CWE-CAPEC/hw-cwe-sig

Discussion

Inaugural 2021 CWE Top-10 Most Dangerous Hardware Weaknesses
See slides for more information

General information was presented regarding who participated in the initial HW CWE SIG survey. Results for the top questions to ask about a CWE entry for weight were also reviewed. Many of the selections focused on frequency of detection and remediation. A follow-up survey focused on the top questions is being developed. The Hardware team is considering whether to ask questions about severity/impact of a weakness.

Top 5 from survey distributed to SIG (ranked):

1. CWE-1300
2. CWE-1191
3. CWE-1189
4. CWE-1277
5. CWE-1240

Following the top entries, this group was ranked equally:

CWE-1247
CWE-1332
CWE-1242
CWE-1260
CWE-1233
CWE-1295
CWE-1324

A member agreed with the notion of analyzing severity/impact and looking at the "consequences." Another member pointed out the differences in severity and how that has been a challenge in other forums but concluded that classifying a weakness with a broader descriptor such as "complete data loss" may be a solution.

Next, there was a conversation about the application of the CWSS to a Top N list and whether there was a consistent way to use it as a resource.

Several members voiced an interest in creating product segment lists. Another member expressed that depending on the system being used, a weakness may or may not have a significant impact across users.

A member asked what the significance of incorporating severity would be (example, for an individual user's ranking). A member of the CWE Hardware team mentioned that this could help to better capture risk within a Top 10.

A member mentioned that the title could veer away from 'Top 10' to make the list more unique and to avoid branding conflicts with other resources in the space. Another member brought up the fact that in the past severity and prevalence were the strongest factors for ranking. A CWE HW team member acknowledged that this occurred between 2009 and 2011 and is still partially present in the modern methodology. The lack of previous data was brought up as a challenge as well as the possibility of not using ranking the list.

A member stated that they didn't see the need to rank at this early stage in part because there would be a period where educating designers would be necessary and that the expectation should be that they pay attention to the list more generally rather than focusing on a few items at the top and moving on.

A CWE HW member brought up the idea that ranking could be correlated with adoption. Another CWE HW member mentioned focusing on awareness for the list's first year. *In response, a member proposed clearly explaining the methodology behind why and how the final entries made the list over others.*

A member shared that they would like to talk more about how to address the overlapping entries that the HW team brought up during the presentation, potentially during the next meeting.

The moderator concluded by providing a timeline to publication.

Continued Discussion: Expanding HW CWE Content
See slides for more information.

The presenter provided a recap on last month's conversation which consisted of consensus on the proposal "Enumerating Weaknesses Related to Non-Conforming, Counterfeit, and Tampered Hardware components as well as the agreement that many entries could expand category CWE-1195.

Next, the presenter proposed forming sub-committees focusing on different interest areas (e.g. supply chain, Top 10).

A member expressed an interest in the idea but also wanted to see the incorporation of CAPEC. They also proposed not always enumerating new additions and having a smaller group provide further analysis.

A member proposed having subcommittees by CWE category (example, supply chain can fit into multiple categories). Another member thought that the categories should be more narrowly focused. A third member agreed with the idea.

Next, the presenter brought up the topic of Submission Review Questions and shared that the new CWE/CAPEC User Experience Working Group will help to determine which questions are appropriate by audience. The goal is to modernize the corpus. Another focus is to ensure that proposed entries are within the scope of CWE.

In response to the questions posed, a member emphasized that having the ability to describe attack potential would be useful in the event that a physical product isn't accessible. The presenter shared that this is present in other areas of the form outside of the summary.

A member mentioned that the original goal of the SIG was to make sure that the focus was to ensure designers had what else they need to secure vulnerable products. Another member mentioned that after reviewing CVEs, CWEs, and CAPECs as part of the G32 committee efforts, it seems that some of the content extends past the design scope. A third member stated that we should be including information for how a weakness can detected. The presented acknowledged that detection methods are an area that the team would need to further develop.