HW CWE SIG Board Meeting #11

Friday October 29@ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
Mike Borza - Synopsys
John Butterworth – MITRE CWE
Matthew Coles – Dell
Steve Christey Coley – MITRE CWE
Amitabh Das – AMD
Daniel DiMase - Aerocyonics
Nicole Fern - Riscure
Thomas Ford – Dell
Jason Fung – Intel
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Victor Ibe - Aero
Joe Jarzombek – Synoposys
Gananand Kini – MITRE CWE
Lang Lin – Ansys
Chris Lathrop – MITRE CWE
Arun Kanuparthi – Intel
Milind Kulkarni – NVIDA
Mohan Lal – NVIDIA
Bruce Monroe – Intel
Luke Malinowski – MITRE CWE
Kumar Mangipudi – Lattice Semiconductor
Srivinas Naik – Intel
Jason Oberg – Tortuga Logic
Vivek Ponnada - GE
Sayee Santhosh Ramesh – Intel
Naveen Sanaka - Dell
Alec Summers – MITRE (HW CWE SIG Moderator)
Chris Timko – Red Hat
Steven Walters – Aerocyonics
Paul Wortman – Wells Fargo

General/initial Discussion

- Next meeting will take place in November or December 2021 (exact date TBD)
- G32 Efforts
  - Security risk articles from G32 publicly available (see last section for more information). A process is needed to convert the items into CVEs/CWEs.
  - Looking into quantified assurance model. There are two chess projects: risk modeling and quantification. This is an opportunity for some of the SMEs who are members of the HW CWE SIG to contribute

CWE 4.6 & the 2021 CWE MIHM List

- List published on October 28
- Press coverage has already come from Dark Reading and Semiconductor
- Request for SIG members: Amplify List promotion

Work Behind the Scenes
CWE/CAPEC Technical Lead: Steve Christey Coley

- The speaker gave a brief on how CWE 4.6 was developed. Originally, there weren't many detection methods. 10 different elements were considered for the entries.
- 72% of the required entry elements were originally filled out and the update brought that up to 99%
- Usability description still needs to be updated so that people aren't discouraged from tackling the issue
- Names and descriptions of demonstratives examples were improved upon across the board
- No changes to the attack patterns were made during this release. There may be a minor release that pushed to address this in the coming weeks.
- The SIG and CWE Hardware team played a primary role in these improvements coming to fruition

A member shared that some of the entries seemed misplaced and may need to be moved for the next release. The speaker acknowledged that the original email request was received but didn't come in time to be included for 4.6.

Expanding HW CWE Content
Proposal from SAW G32 CPSS to Add HW CWEs

- The speaker provided some background on the proposal about incorporating new hardware CWEs to address relevant supply chain concerns. Discord comes from the fact that the issues don't map well with CWEs currently.
- CWE team is thinking more abstractly about the definition of a HW weakness

A member mentioned that the current weaknesses available are not related to supply chain weaknesses.

Another member provided clarification between the scope of the G-19 (dealing with counterfeits) and G-32 groups. G-32 is currently looking to analyze gaps between the CWEs and CVEs. Looking at inputs from NDIA, CWE produced by this SIG group, and 5200.xx recently addresses to ensure all areas are covered. This is an opportunity to converge and ensure we have alignment. It's easier to point to the predefined processes than to create something brand new.

A third member shared that everything that G-32 had identified at counterfeit or tainted in considered testable. He also discussed the connection between quality and security flaws.

A fourth member shared that he felt that there was a more natural fit into CAPEC than in CWE because the audience for the latter is more focused on design, where as CAPEC may have more for the manufacturing group.

A CWE team member emphasized that there will be a vetting process before creating any new entries that create a big scope change.

The third member responded by saying that the attack patterns explore the weakness so there is extensive correlation, thus there is more relevancy beyond design.

A member asked if MITRE ATT&CK might be another avenue to consider. The moderator acknowledged that this hadn't been discussed but was in the realm of possibilities for the future and proposed having someone from the team join an upcoming call.

Follow Up on Security Articles of Interest from G-32

- A weekly security resource that is widely distributed (audience=ISACs, government agencies, NDIA electronics and more)
- The moderator discussed opportunities for mining the resource for new CWE entries
- Daniel DiMase is the contact. Reach out if you have questions or would like to subscribe to receive

A member brought about the topic of increasing and gauging CWE usage as a topic for a future meeting.

Another member wanted to know about how other SIG members were using HW CWEs throughout their product lifecycle.