HW CWE SIG Board Meeting #8

Friday June 11 @ 1230-1330 EST

Members in Attendance

John Bell – iRobot
James Bellay – Batelle
Mike Borza – Synopsys
Evan Bryers - Aerospace
John Butterworth – MITRE CWE
Dave Clinton – Microchip
Matthew Coles – Dell
Kerry Crouse – MITRE CWE
Steve Christey – MITRE CWE
Amitabh Das – AMD
Daniel DiMase - Aerocyconics
Nusrat Dipu – University of Florida
Thomas Ford – Dell
Farbod Foomany – Security Compass
Domenic Forte – University of Florida
Jason Fung – Intel
John Hallman – OneSpin Solutions
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Joe Jarzombek – Synoposys
Arun Kanuparthi - Intel
Gananand G Kini – MITRE CWE
Milind Kulkarni – NVIDIA
Vikas Kumar – Intel
Mohan Lal – NVIDIA
Lang Lin – Ansys
Luke Malinowski – MITRE CWE
Bruce Monroe – Intel
Jason Oberg – Tortuga Logic
James Pangburn – Cadence Design Systems
Naveen Sanaka - Dell
Sayee Santhosh Ramesh – Intel
Robert Van Spyk – NVIDIA
Alec Summers – MITRE (HW CWE SIG Moderator)
Jim Wesselkamper – XiLinx
Paul Wortman – Wells Fargo

Housekeeping

- Next Meeting is Friday, July 9
  12:30 to 1:30 pm EST

Handling Overlapping HW Entries
(HCWE's sharing a common thematic similarity)
See proposal and slides for additional information

The CWE Hardware team discussed two options for potentially addressing this challenge and hoped to walk away with a couple of principals for the future.

A member spoke in favor of proposal 2 saying that the level of precision for CVEs and child CWEs will be better.

Another member agreed because ROM and firmware are dependent on different technologies. CPU Microkorg was shared as an example. The member also shared another example where PLCs could be part of a different class.

A third member called out the distinct processes for mitigating the issues between CWE-1277 (more software centric) and CWE-1310 (physical interaction required for patching). Another member later reiterated this by acknowledging that there were similarities at a high level but the mechanisms and implementations vary greatly.

A member of the hardware team acknowledged that mitigations were not an area that the team had not factored in as reasons to keep or not keep separate entries in the past.

A fourth member supported proposal 2 because CWE-1329 because of its status as the sole CWE covering software updates as opposed to firmware or ROM updates. The member asked if the CWE would potentially be split into a class and base weakness and saw this as an opportunity to bridge the gap between software and hardware weaknesses.

The hardware team member explained that the intention of CWE-1329 is to include both software and hardware aspects. They acknowledged that in CWE this was referenced as a base but should really be a class. A solution of having a lower-level class or base level children (one for software and one for hardware) was mentioned. This may result in some of the hierarchical relationships becoming deeper and risks them becoming too complex once again (work was done to shrink the levels down to about 5 from 7).

The general consensus at the end of the conversation was that proposal 2 would be the best fit for moving forward.

Enumerating Indicators That Serve as Markers for Non-Confirming, Counterfeit and Tempered Hardware Components
Proposal from SAE G32 CPSS to Add Hardware CWEs
See slides for more information

The speaker shared that the hardware CWEs currently only cover design defects and that other attributes that could be or have been exploited, such as coding covered on the software side, has not been addressed previously. He then presented some categories, including a "tampered" category that is

still evolving, for addressing supply chain challenges. At a high level, the proposal consisted of aligning HW CWE's with SAE G 19A categories for counterfeit defects.

A member expressed their support of the effort and discussed one of the free tools on SAE's website that helps determine what kind of testing would be most appropriate for detecting counterfeit defects.

Another member asked if the taxonomy was intended for unintentional defects.

The speaker stated that the focus was on intentional counterfeiting and that proving malicious intent could be difficult. There was also a point made about nonconforming components from a contracts perspective.

Another consideration mentioned by the speaker was aligning names between G19A and the CWEs.

A member brought up their concern with the fact that the taxonomy might not be sufficient because it is component centric. He concluded that the structure would need to be extended and additional categories should be added.

A second member noted that the taxonomy was likely not meant to mirror CWE but focus on counterfeits while evolving. The member emphasized that this was an important resource because counterfeiting is the most prevalent occurrence within hardware assurance.

Another member brought up several points including reiterating exploring the entire supply chain ecosystem (impacts of software and hardware issues), the possibility of counterfeit types having greater relevancy to weaknesses (versus defects) and the idea that monetization involved (with cloning, for example) should be a consideration.

The speaker responded by reference the ISO's reliability issues and their potential transition to security issues and reminded the group that CWE doesn't just cover security but also other weaknesses that deal with other quality attributes.

A member brought up CWSS as being a relevant tool as well.

After the speaker asked for a general consensus on the proposal, the members spoke up in agreement.

One member requested a formal proposal and said that mapping would be worth further conversation. Another member mentioned that many of the counterfeit types could fit under CWE-1195, which addresses manufacturing.

The moderator concluded by sharing an interest in having the members be involved in the process of writing some of the content and revisions that would come out of this effort.