HW CWE SIG Board Meeting #10

Friday August 6 @ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
John Butterworth – MITRE CWE
Matthew Coles – Dell
Kerry Crouse – MITRE CWE
Steve Christey – MITRE (HW CWE SIG Moderator)
Daniel DiMase - Aerocyconics
Thomas Ford – Dell
Jason Fung – Intel
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Joe Jarzombek – Synoposys
Vikas Kumar – Intel
Bruce Monroe – Intel
Luke Malinowski – MITRE CWE
Jason Oberg – Tortuga Logic
James Pangburn – Cadence Design Systems
Naveen Sanaka - Dell
Robert Van Spyk - NVIDIA
Paul Wortman – Wells Fargo

Housekeeping

Next Meeting – *Friday, September 3 @ 12:30 pm EST* (may be moved pending survey)

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

Discussion

New CAPEC 3.5 Release – June

The CAPEC team is focused on including more content on supply chain in the coming months. There are 7 new entries related to the topic that are now available.

A member expressed concern with using the word “maliciously” because it implies intent versus something inadvertently being done. Another member countered this idea because this was specifically created for an “attack patterns” list. In response, the first member mentioned that an attack can also come from another computer.

New CWE 4.5 Release – July

One hardware CWE was added (CWE-1351). An update was made to CWE-1256 via Tortuga Logic.

Images are now supported on entries via tags. An interest in seeing architectural configurations was the impetus for the change.

Thinking through any practical concerns about how the images are packaged via XML and whether or not this new feature impacts organizations displaying CWEs on their own sites is something that the team is exploring further.

A member asked if there was an entry similar to CWE-1351 that addressed humid conditions. Another member and the moderator referenced one that relates to radiation exposure. The group also discussed the distinction between functional and security issues.

Top N-List: Timeline to Publications

A CWE team member discussed plans for compiling data in September and releasing a top-N list in October. Options for gathering the necessary information include a MITRE-facilitated discussion/exercise or having members of the SIG deploy a survey. The group generally preferred the MITRE-led activity.

A member requested seeing a candidate list prior to the conversation taking place and shrinking the number of options from the approximately 100 related hardware entries. They also discussed differences in ranking methodologies such as consequence versus ease of exploitation. The idea of having a discussion in addition to any sort of individual ranking was emphasized.

Another member suggested working off of the initial list of CWEs presented in the recent Google survey as a starting point. The moderator brought up the fact that only 13 SIG member participated in the survey as a consideration. The CWE team member agreed that using the top entries ranked in this survey along with others that were selected to a lesser extent may be a good next step.

Additionally, a member asked for clarification on the challenges of deploying a survey. The moderator briefed the group on considerations that were shared during a meeting with MITRE's survey experts (e.g. data privacy, internal processes and regulations).

Submissions from Paul Wortman
See slides for more information.

- HCWE102: Untrusted Manufacturing of Intellectual Property (IP)

A member asked for more information on the intention behind this proposed entry as it would relate to a weakness and expressed that there was a lack of clarity in the connection with CWE-684. The proposer explained that the intention was tied to the fact that because manufacturing isn't always done in house anymore, the development is being sent to a third-party, which may be untrusted.

A second member questioned the use of the word untrusted in this case.

Another member also stated that the phrasing could be different (e.g. "leakage of IP in a third-party environment," use of the word "integrity," etc.) The same member also asked if provisioning would be part of the entry.

The proposer acknowledged that a decision would have to be made about whether or not key provisioning can be attached in this instance or if it needs to be a separate entry. They said it was a question of how detailed the CWEs could get.

- HCWE201: Verifiable Integration Testing

A member shared that they were in agreement with adding this proposed entry to CWE-684.

- HCWE105: Hardware Trojans
- HCWE106: Lack of Hardware Design Verification Against a Golden Standard
- HCWE104: Missing protective measures for preventing or hindering reverse engineering of IP or other sensitive data
    - The moderator expressed the need for MITRE and the SIG to make a decision on whether or not reverse engineering should be included (more info to come via email)

Additional Items

Counterfeit/Anti-Tamper - MITRE is still reviewing SAE G32 CPSS proposal (via Joe Jarzombek, Synopsys); a new subset of this data will be sent to the SIG. Dr. Nguyen from Auburn may also have some additional insight.