HW CWE SIG Board Meeting #7

Friday May 14 @ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
John Bell – iRobot
James Bellay – Batelle
John Butterworth – MITRE CWE
Steve Carlson – Cadence
Matthew Coles – Dell
Kerry Crouse – MITRE CWE
Steve Christey – MITRE CWE
Amitabh Das – AMD
Thomas Ford – Dell
Farbod Foomany – Security Compass
Jason Fung – Intel
Kathy Herring Hayashi – Qualcomm
John Hallman – OneSpin Solutions
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Christina Johns – MITRE CWE
Gananand G Kini – MITRE CWE
Vikas Kumar – Intel
Mohan Lal – NVIDIA
Lang Lin – Ansys
Luke Malinowski – MITRE CWE
Parbati Manna – Intel
Bruce Monroe – Intel
Kirrill Motil – Microsoft
James Pangburn – Cadence Design Systems
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 – Friday, June 11, 12:30 to 1:30 PM EST

Minutes from previous meetings available at:

https://github.com/CWE-CAPEC/hw-cwe-sig

SIG Survey Results – 2021 HW CWE Top N* List
See slides for more information

The moderator described the CWE team's motivation behind developing a survey which includes the fact that there aren't as many resources covering the topic of hardware. Eleven responses were received with the following entries gaining the most votes (in order of highest number of votes):

- CWE-1191: Exposed Chip Debug and Test Interface With Insufficient or Missing Authorization
- CWE-1300: Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
- CWE-1189: Improper Protection Against Physical Side Channels
- CWE-1277: Firmware Not Updateable

6 others received 3 votes each.

A CWE team member shared his interest in exploring the findings after combining similar HW CWEs together based on various views and analyzing how distinct the individual CWEs are.

A SIG member asked for clarification on whether the initial survey asked for a ranked order of CWEs and it was confirmed that this was not the case. Another member recommended collecting additional data for more accurate insight.

Next, a summary of how general questions that could be used for a broader survey was shared. Questions like: "Associated cost of equipment?, Can the weakness be detected by physical proximity?, Can the weakness be detected by software?" were the least popular. Questions covered a variety of areas including prevalence, detection, and exploitability. The CWE presenter asked for feedback and expressed interest in including some of the questions as part of the HW entry submission process.

A member shared that he thought the adding the questions to the submission process would be a good way to drive severity scores.

Another member said that the impact was not as important because things depends on the implementation, use case model, etc. and can be hard to gauge based on the weakness. He said that he didn't think of the top responses as the most dangerous but as common mistakes that readers of the survey can use to assess the strength of their tools/resources. He also drew attention to question 18 (whether a weakness requires hardware modifications to mitigate) as it makes the key distinction between hardware and software weaknesses.

The moderator acknowledged that there is a certain level of flexibility when it comes to how the survey summary information ends up being presented. Examples include the title and number of entries featured (e.g. Top 10).

A member discussed the design-centric nature of hardware development and how it may have impacted the number of upvoted received on Question 1 (weakness detection during design). Questions 2,3, 18, and 23 were mentioned as items that could be affected after a cost benefit analysis is conducted. Another mentioned hardware trojans as an example of something that may not be detected during the design phase. A third member agreed and said that manufacturers have to look at different points of potential injection for where these issues could arise.

The moderator thanked everyone for participating in the discussion and reminded people to complete the survey if they had not already. He then asked how long it took those who had submitted feedback.

One member said it took 30 minutes but that it might take as little as five minutes. Another member shared that it took about 20 minutes.

The moderator also asked members to provide their thoughts on how HW CWE information is presented.

A member asked if it would be helpful to know what challenges companies face when trying to adopt CWEs in addition to how far they are in their adoption.

The moderator shared that developing a survey to gather this sort of information would be useful in CWE's goal of providing value and enhancing the way information is presented to the community.