HW CWE SIG Board Meeting #6

Friday, April 16 @ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
John Bell - iRobot
John Butterworth – MITRE CWE
Evan Bryers – Aerospace
Steve Carlson – Cadence
Matthew Coles – Dell
Steven Christey – MITRE CWE
Kerry Crouse – MITRE CWE
Amitabh Das – AMD
Iain Deason - CISA
Nusrat Farzana Dipu – University of Florida
Farbod Foomany – Security Compass
Thomas Ford – Dell
Jason Fung – Intel
John Hallman – OneSpin Solutions
Christina L Johns – MITRE CWE
Hareesh Khattri – Intel
Kumar Mangipudi – Lattice Semiconductor
Vikas Kumar – Intel
Gananand G Kini – University of Maryland
Lang Lin – Ansys
Luke W Malinowski – MITRE CWE
Mohan Lal – NVIDIA
Bruce Monroe – Intel
Srinivas Naik – Intel
Jason Oberg – Tortuga Logic
James Pangburn – Cadence Design Systems
Sayee Santhosh Ramesh – Intel
Andreas Schweiger – Airbus
Robert Van Spyk - NVIDIA
Brent Sherman – Intel
Alec J Summers – MITRE HW CWE SIG Moderator
Paul Wortman – Wells Fargo

Housekeeping

The next meeting will take place on May 14 at 12:30 pm EST.

Minutes from previous meetings are available on the Github site: https://github.com/CWE-CAPEC/hw-cwe-sig

HW CWE Usage Models in Security Development Lifecycle

See slides for more information.

The group viewed a presentation from the Intel team regarding how they reference hardware CWEs as part of their product development lifecycle.

Introduction

The first speaker kicked the meeting off by walking through the different steps of the Product Lifecycle (PLC) as they integrate with the Security Development Lifecycle (SDL). He mentioned that sometimes when customers find issues with a product, they will bring them up during the "deployment" phase towards the end of the process. Researchers and architects are engaged early in the process to mitigate any potential threats.

Usage Model #1: How Hardware CWEs Help PSIRT Efforts

The next presenter shared a case study in which a root cause analysis of a target set of issues occurs as the first step in the Product Security Incident Response (PSIRT) process. At this time, mapping to two levels of CWEs for each vulnerability during the triage stage. Since working with the HW CWE's is still a fairly new part of the process, building out the data and looking for patterns is key. Vulnerabilities that aren't covered are shared with the appropriate internal teams. Security training is conducted with individual teams if the patterns reoccur. Automation tools and scripts are developed for test cases that are missed. Once new mitigations are created, they are rolled out to customers.

A member asked the speaker to talk about the ease of selecting CWEs.

The speaker shared that because the hardware CWE is small at the moment, the mapping process is relatively easy. He also said that if one has a good understanding of the bug that they're working with, it can make the process easier.

A CWE team member asked about the specifics of where CWE is helping throughout the PSIRT process.

The speaker talked about how identifying CVEs can lead to a quick connection of CWEs. He said that the biggest piece is driving the CWEs into SDL and that they help with continuous improvement.

Usage Model #2: How Proactive Research Can Leverage CWEs

The speaker discussed the processes of the Internal Security Research team, which covers both internal and external products and maps their findings to the appropriate CWEs. He mentioned that having the processes in place can help improve the quality of the CWEs and helps the group to better prioritize what goes into some of Intel's "Learning Propagation Methods" which include security trainings, automation tools, and mitigations. Previously, the IRS team was categorizing issues internally, however, working with the HW CWEs has accelerated the classification system and understanding of common weaknesses. The speaker also talked about the importance of tagging CVEs properly as this can impact whether/how CWEs are reference in the NVD.

A CWE team member asked for clarification regarding whether the NVD was being used for all hardware items or if the database was just being used for Intel's products. The speakers shared that his team looks for all items using keywords because of the mass volume of CVE entries.

The CWE Team member also brought up the fact that CVE currently only has about 100 CWEs connected (view 1003) but there are no HW CWEs included in that group. He shared that once the HW CWEs reach a certain level of maturity in their usage, that a plan would be developed to get them into NVD.

Usage Model #3: How Security Validation Can Benefit from CWEs

The objectives of SoC Security Assurance are to identify applicability of CWE categories to specific use case scenarios and to develop mapping of next level weakness information to test cases.

The speaker reviewed examples of how the team mapped debug issues to the appropriate CWEs. (see slide)

The moderator discussed how this particular topic ties in with recent work that the CWE team has been researching to determine if everything is being covered correctly in a practical way for users. The moderator also share that the team is exploring physical proximity to a device. He then asked if the current categories are meeting the needs of the SoC assurance team, and the speaker confirmed that they were.

In conclusion the first speaker, encouraged members to contribute additional entries to the CWE as Intel has done in order to enrich the content as various teams rely on the information to understand how issues can be detected, verified, and mitigated.

2021 HW CWE Top N* List

The moderator shared that the CWE team drafted a list of potential questions for the new Top N* survey, which would be distributed to the members for feedback after the call, and briefed the group on the approaches taken in the past to collect information. He explained that the purpose of the top lists is to drive awareness to the broader lists and also to focus on high priority entries. The format of the initial survey was then introduced. The goal would be to publish the formal findings from the public survey at some point during this calendar year.

A member requested that mechanism for collecting feedback from the SIG group allow for anonymous submissions in case there are discrepancies between individual and company perspectives. The moderator agreed to incorporate transition the information from a document to an appropriate tool to support confidentiality.

Feedback is due before May 7th.

Closing

The moderator reminded member of the next meeting date and to email any topics of interest to cwe@mitre.org. There is also an evergreen request out for future presenters to share information on topics such as how members are leveraging HW CWE in their organization and/or operations.