HW CWE SIG Meeting
Friday, August 18, 2023

Members in Attendance

Bob Heinemann	Amitabh Das	Shafqat Ullah
Luke Malinowski	Krzysztof Kepa	Nicole Fern
Andreas Schweiger	Rich Piazza	Bruce Monroe
Gage Hackford	Mohan Lal	Abraham Fernandez Rubio
Steve Christey Coley	Dale Donchin	Scott Constable
Faheem Ahmed	Ian Land	Allen Krell
Jason Oberg	Rafael dos Santos	John Hallman
James Pangburn	Andy Meza	Kris Britton
Parbati K Manna	David Kaplan	Sohrab Aftabjahani
Alric Althoff	Thomas Ford	Jiang Fu

Agenda

- Housekeeping and Announcements
- CWE Nit Bits (Bob Heinemann)
- Discussion: Covert Channels and CWE (Bob Heinemann)
- Discussion: Most Important Hardware Weaknesses Refresh (Bob Heinemann)
- AOB (Any Other Business)

Housekeeping

- Next meeting: September 8, 12:30 – 1:30 PM EDT (16:30 – 17:30 UTC) on MS Teams.
- Contact: cwe@mitre.org
- Mailing list: hw-cwe-special-interest-group-sig-list@mitre.org
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements

- Talking with CISA to see if they are willing to present their Secure by Design/Secure by Default strategy. May happen at the next HW SIG meeting.

CWE Nit Bits: Vulnerability Mapping Notes (Bob Heinemann)

- A new section in CWEs that provides guidance for when or whether to map an issue (vulnerability) to a particular CWE entry or to suggest alternatives. Mapping notes may include usage, reason, rationale, comment, and suggestions (see meeting slides).
- Mapping Notes are required, per the CWE schema.

- Great way to capture CWE team institutional knowledge. Primarily intended for internal use to improve mapping to CVEs.
- Provides a way to identify prohibited mappings, e.g., don't map to a particular category or view, don't map to a deprecated CWE.
- Example CWEs were shown that use Vulnerability Mapping Notes: CWE-20: Improper Input Validation, CWE-514: Covert Channel, and CWE-1277: Firmware Not Updateable (see meeting slides).
- Comment: users may not have the time to identify the most precise CWE, so they may decide to not map to anything. Response: program recognizes the need for better tools to make it easier for users to navigate and drill down to the most appropriate CWE.

Covert Channels and CWE (Bob Heinemann)

- Specifically looking at covert coverage and hardware CWEs.
- Came out of research by a team from an Israel university that developed and demonstrated a data exfiltration technique for air gap systems. They refer to the technique as COVID bit (see meeting slides).
- Covert channels are different from side channels (like CWE-1300: Improper Protection of Physical Side Channels).
- Comment: Need to be clear about the distinction between side and covert channels.
- Questions for the SIG:
    - Do we have adequate coverage of covert channels in CWE, and specifically for HW CWEs? The closest we have is CWE-514: Covert Channels.
    - Should we include covert coverage in the hardware view, which we currently do not have?
    - Do we need to modify CWE-514 so it covers both software and hardware, or create a base of CWE-514 that's more specific to electromagnetic covert channels?
    - Does the group think there should be covert channel coverage in the hardware view? Responses: Yes. We also need a side timing channel view, suggest using the observable timing discrepancy which is CWE 208 to help avoid mis categorization of side channels as covert channels. The CWE internal team will meet to continue work on this topic, and report out to the SIG.