HW CWE SIG Meeting
Friday, February 10, 2023

Members in Attendance

Aftabjahani, Sohrab
AHMED, FAHEEM
Alec J Summers
Bob Heinemann
Bormann, Joerg
Bronn Pav
Carlos Moreno
Chris Coffin
Constable, Scott D
Daniel DiMase
Das, Amitabh
Evan Bryers
Ford, Thomas
Fung, Jason M
Gage Hackford
Gananand G Kini
Iyer, Priya B
James Pangburn
Jason Oberg
Kanuparthi, Arun
Kaplan, David
Khattri, Hareesh
Lang Lin
Luke W Malinowski
Manna, Parbati K
Mike Borza
Milind Kulkarni
Mohan Lal
Monroe, Bruce
Nicole Fern
Pav, Bronn
Rich Piazza
Sanaka, Naveen
Shafqat Ullah
Wortman, Paul

Agenda

- Housekeeping and Announcements
- Working Items for this Meeting
  - Changes made in CWE 4.10 / Looking forward to 4.11
  - Transient Execution Weaknesses Update
  - HW Description Language Discussion
  - Other Mailing List Discussions (if time allows)
    - Addition of Semiconductor defects to category
    - Use of the language "Security Guarantees"

Housekeeping

- Next meeting: March 10, 2023, 12:30 – 1:30 PM EST (16:30 – 17:30 UTC). Virtual meeting using 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

- CWE 4.11 targeted for release sometime in May 2023.
- Custom presentation filters

  - Demonstrated to User Experience Working Group (UEWG) on February 8, 2023
  - ETA CWE 4.11 at the latest, maybe earlier
  - Email if there is interest in a demo for this group.

Changes Made in CWE 4.10 (Bob Heinemann)

- Revamped CWE-1357 having to deal with the dependency of insufficiently trustworthy components.
- Updated over 400 CWE records to replace the word “software” with “product.” This better allows the scope of those CWEs to include hardware.
- Deprecated CWE-1324: Sensitive Information Accessible by Physical Probing of JTAG Interface. All relevant content has been integrated into CWE-319.
- Changed categories and relationships in the Hardware View (CWE-1194).
- Improved names, descriptions, and/or demonstrative examples of multiple hardware weaknesses.

Looking Forward to CWE 4.11 (Bob Heinemann)

- Now is the time for HW SIG members to submit any items or updates they would like to see in 4.11. They will be rolled into 4.11 prioritization and planning.
- Updates and change requests can come from the HW SIG or the broader community. The program encourages the use of GitHub for all suggestions/requests for CWE issues and updates: https://github.com/CWE-CAPEC/hw-cwe-sig/issues. If not already a member, send your GitHub username to the program to be added to the repo.
- There are some internal research items the program would like to work (create initial CWEs) and make available for community discussion. Stay tuned.
- No change to the process for submitting new CWE proposals.

Transient Execution Weaknesses Update

- The document with the four submissions and MITRE team questions/suggestions was shared with the group via Box.
- A comment was made that Box is good for file sharing and not so good for collaboration. GitHub may be better for collaboration. It was agreed to create a top level folder at GitHub called working-docs.
- Let the program know if you’re interested in supporting the transient execution work.

HW Description Language Discussion

- New class created last year under Languages called Hardware Description Language.
- Presented the CWE HW entries that mention VHDL (in Languages) but are missing Language Class = Hardware Description Language.
- Presented CWE-1299
- Presented the CWE HW entries that mention VHDL (in Description) but are missing in Languages and Language Class = Hardware Description Language.
- Members were asked: “Should any of these CWE entries include the hardware description language as the class?”

- The suggestion was made to develop formal definitions. What does it mean for not language specific versus it is part of the language category class, HDL, VHDL, Verilog and then compile?
- Provide further input using the tracker: https://github.com/CWE-CAPEC/hw-cwe-sig/issues/3

Other Mailing List Discussions (hw-cwe-special-interest-group-sig-list@mitre.org)

- Category Name Update
    - A SIG member suggested that the CWE-1206 name be changed from "Power, Clock, Thermal, Reset Concerns" to "Power, Clock, Thermal, Reset Concerns, or Semiconductor Defects."
    - No objections to not making the change since semiconductor defects are covered elsewhere.
- CWE-1248 – Issue with phrase "Security Guarantees"
    - CWE Description includes the text "If such faults occur in security-sensitive hardware modules, security guarantees offered by the device will be compromised." Inanimate objects cannot offer guarantees.
    - Two proposed rewording options:
        - "If such faults occur in security-sensitive hardware modules, security guarantees offered by the device vendors/ manufacturers will be compromised.
        - "If such faults occur in security-sensitive hardware modules, the security objectives of the hardware module may be compromised."
        - The second option is recommended, and if there are any objections or concerns, use the GitHub tracker to communicate.