Hardware CWE™ Special Interest Group (SIG)

Gananand Kini, Bob Heinemann, Luke Malinowski, Gage Hackford, Chris Lathrop, Steve Christey Coley, Alec Summers

MITRE

February 10, 2023

Agenda

REMINDER: This meeting is being recorded.

- **Housekeeping and Announcements**
- **Working Items for this meeting:**

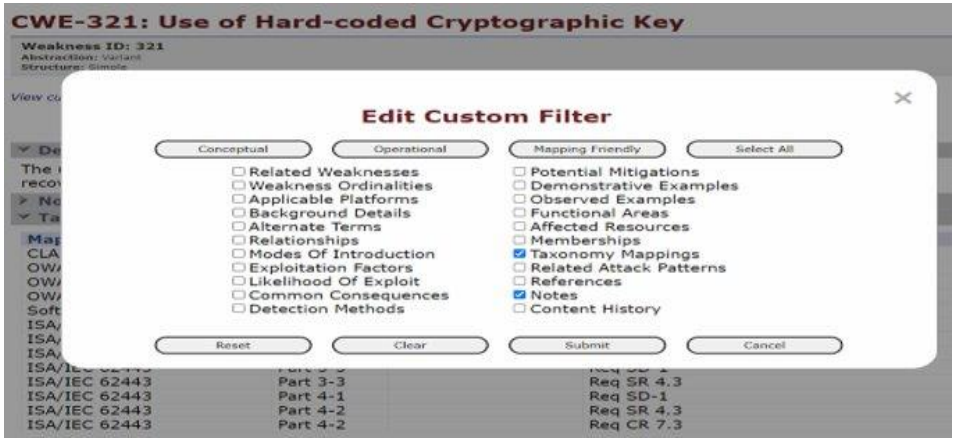
1	Changes made in CWE 4.10 / Looking forward to 4.11	Steve C/Bob H	15 min
2	Transient Execution Weaknesses Update	Ganu K	5 min
3	HW Description Language discussion	Ganu K	30 min
4	Other Mailing List Discussions (if time allows) Addition of Semiconductor defects to category. Use of the language "Security Guarantees".	Bob H	As time permits

Housekeeping

- **Schedule:**
  - **Next Meeting:**
    - **Rescheduled for March 10**
    - **12:30 – 1:30 PM EST (16:30 – 17:30 UTC)**
    - **Microsoft Teams**
- **Contact: cwe@mitre.org**
- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
- **Minutes from previous meetings available on our Github site:**
  - **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
  - Any interest in a demo for this group?



CWE 4.10 Updates

- **Revamped CWE-1357: Reliance on Insufficiently Trustworthy Component to emphasize dependency on “insufficiently trustworthy” components. In cross-cutting problems category.**
- **Changed over 400 CWE descriptions to replace “software” with “product” to better allow the scope of those CWEs to include hardware, driven by experience with the ICS/OT SIG and the CWE Hardware SIG.**
- **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.**

CWE 4.11 Items

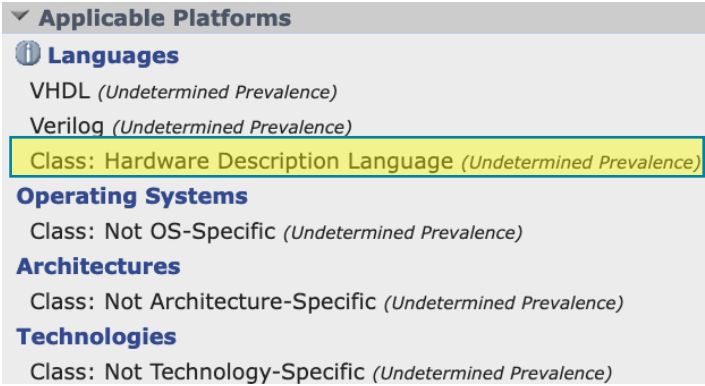
- **GitHub Items**
  - https://github.com/CWE-CAPEC/hw-cwe-sig/issues
  - Community initiated items dealing with discussions and existing CWE updates.
  - Place to submit agenda topics for SIG Meetings
  - Vision is that community will drive discussion topics and MITRE team will implement.
  - Send us your GitHub username and we'll add you as a member to the repo
- **Research Items**
  - There are some internal research items that we would like to work and create initial CWEs for community discussion. Stay tuned.
- **Submissions**
  - No change on submitting proposals for new CWEs.

Transient Execution Weaknesses Update

- **Document with the four submissions and add the MITRE team questions/suggestions has been shared with the group.**
- **Gotten some feedback and additional questions from the group. Waiting on others to provide more feedback/answers.**
- **What does the group think of the Box platform?**

Languages Class: Hardware Description Language

- **Started with CWE-1272: Sensitive Information Uncleared before Debug/Power State Transition updated the Applicable Platforms section in Oct 2022:**
- **This indicates the weakness is applicable to a class of Hardware Description Languages including VHDL and Verilog.**



CWE HW entries mention VHDL (in Languages) but missing Language Class = Hardware Description Language

- **CWE-1269: Product released in Non-Release Configuration. (Compiled)**
- **CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT vendors. (Not Language Specific)**
- **CWE-1273: Device Unlock Credential Sharing. (Compiled)**
- **CWE-1223: Race Condition for Write-Once Attributes. (Empty)**
- **CWE-1221: Incorrect Register Defaults or Module Parameters. (Empty)**
- **CWE-1298: Hardware Logic Contains Race Conditions. (Empty)**
- **CWE-1311: Improper Translation of Security Attributes by Fabric Bridge. (Empty)**
- **CWE-1280: Access Control Check Implemented After Asset is Accessed. (Not Language Specific)**
- **CWE-1296: Incorrect Chaining or Granularity of Debug Components. (Not Language Specific)**
- **CWE-1224: Improper Restriction of Write-Once Bit Fields. (Empty)**
- **CWE-1251: Mirrored Regions with Different Values. (Empty)**
- **CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready. (Not Language Specific)**

CWE HW entries mention VHDL (in desc.) but missing in Languages and missing Language Class = Hardware Description Language

- **CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface. (Not Language Specific)**

Hardware Language Class discussion

- **Questions:**
  - Should any of these have the Hardware Language Class updated to include ‘Hardware Description Language.’
  - If so, which ones?
  - Does the HW SIG Community have an understanding of Language Class?
- **Please join the discussion on the issue tracker on GitHub.**

Mailing List Items

Mailing List: *hw-cwe-special-interest-group-sig-list@mitre.org*

- *NOTE: All mailing list items are archived publicly at:*
  - *https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/*

Active Discussions – Category Name Update

- **A sig member has suggested that the category CWE-1206 name should be changed from "Power, Clock, Thermal, Reset Concerns" to**
- **"Power, Clock, Thermal, Reset Concerns, or Semiconductor Defects."**
- **The rationale is this: The current title does not discuss hardware deterioration.**
- **Manufacturing and Life Cycle Management Concerns (1195) covers "defects that arise in the semiconductor-manufacturing…"**
- **Recommendation is not to make this change.**

https://github.com/CWE-CAPEC/hw-cwe-sig/issues/1

Active Discussion: CWE-1248 - Issue with phrase "Security Guarantees"

- **The SIG Community is having issue with the phrase "security guarantees" in the extended description.**
- **Some have issue with semantics of products are incapable of making claims and others have issue with the language as their may be specific legal consequences of the term.**
- **The sentence under scrutiny is**
  - "If such faults occur in security-sensitive hardware modules, ***security guarantees*** offered by the device will be compromised."
- **There are two proposals at the moment:**
- **Hareesh proposes, "If such faults occur in security-sensitive hardware modules, security guarantees offered by the device vendors/ manufacturers will be compromised."**
- **Jim Wesselkamper proposed: "If such faults occur in security-sensitive hardware modules, the security objectives of the hardware module may be compromised."**
  - Jason O and Joe J endorse this proposal.

https://github.com/CWE-CAPEC/hw-cwe-sig/issues/2

Next Meeting (March 10)

CWE@MITRE.ORG

- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
  - ***NOTE: All mailing list items are archived publicly at:***
    - *https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/*
- **What would members of this body like to see for the next HW SIG agenda?**
- **Questions, Requests to present? Please let us know.**