Hardware CWE™ Special Interest Group (SIG)

Chair: Bob Heinemann (MITRE)

Co-Chair: “Manna” Parbati Kumar Manna (Intel)

MITRE Team: Steve Christey Coley, Alec Summers

MITRE

October 11, 2024

Agenda

REMINDER: This meeting is being recorded.

1	Security Issues Arising from Hardware Design	Joerg Bormann	40 - 60 min
2	Most Important Hardware Weaknesses Discussion	Bob Heinemann	If time allows

Housekeeping

- **Schedule:**
  - **Next Meeting: Nov 8**
    - **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 Content Development Repository (CDR) pilot now on GitHub! Open to anyone by request. Public access in the next few months.**
- **CWE 4.16 release is planned for November.**
- **CWE 5.0 is planned for early 2025.**

Call for Topics

What topics should we cover next time?

- **Anything to share today or topics for consideration for next meeting?**

Security Issues Arising from Hardware Design

Joerg Bormann

Most Important Hardware Weaknesses Refresh

Bob H

Current MIHW

CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

New HW CWEs Since MIHW

- **CWE-1342: Information Exposure through Microarchitectural State after Transient Execution**
- **CWE-1357: Reliance on Insufficiently Trustworthy Component**
- **CWE-1384: Improper Handling of Physical or Environmental Conditions**
- **CWE-1388: Physical Access Issues and Concerns**

Most Important Hardware Weaknesses (MIHW)

- **Is this something worth revisiting?**
- **Part of CWE 4.6 Release, October 28, 2021**
- **Have there been substantial developments since the last release of MIHW?**
- **Would those affect the rankings and inclusions of the list in any meaningful way?**
- **Is there any data available that we could utilize to generate the list? Or should we use the delphi method again?**
- **Are there observational trends that would change the current list in any significant and meaningful way?**

Formation of Ad-Hoc Committee

- **Will be putting a call out of the mailing list for members to join an ad-hoc committee to study.**
- **We will be looking for committee members to study the feasibility of a new list and making a decision to proceed.**
- **Also, members will develop an approach to develop the list with the community.**

Next Meeting (Nov 8)

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.**