Hardware CWE SI Group
Meeting Minutes
June 13, 2025

Meeting Attendance

- Bob Heinemann
- Gananand Kini
- Steve Christey
- Mitchell Poplingher
- Sohrab Aftabjahani
- Justin Forbes
- Keerthi Devraj
- Paul Wortman
- Arun Kanuparthi
- Hareesh Khattri
- Bruce Monroe
- Parbati Manna
- Thomas Ford
- Abraham Fernandez Rubio
- Rachana Maitra
- Rafael Machado
- Mohan Lal
- Jason Oberg
- Jason Fung
- Priya Iyer
- Amitabh Das

Agenda

- General Status of HW CWE Submissions
- Most Important Hardware Weaknesses Refresh Update
- Memory Access Related Weakness: Open Discussion and Working Exercise

Meeting Notes

Pre-Agenda: Bob announced the extension of the poll for the Most Important Hardware Weaknesses Group and reminded everyone about the public content development repository for processing submissions and content updates.

- **Participation in MIHW:** Sohrab inquired about the participation criteria for the MIHW poll, and Bob clarified that it is open to the public, but the most important hardware weaknesses poll is limited to hardware SIG members.
- **Future Topics:** Hareesh suggested scheduling a presentation on mapping CVEs to hardware CWEs and identifying gaps, which was appreciated by the group and noted as a future topic.

General Status of HW CWE Submissions

- **Hardware Submissions Update:** Steve provided an update on the status of hardware submissions, highlighting the progress and challenges faced in reviewing and integrating new submissions into the content development repository.

- **Post-Quantum Crypto:** Steve mentioned that there has been no further progress on the post-quantum crypto submission.
- **Detailed Review:** Steve discussed the detailed review process for a submission on propagating requests for transactions before data validation in multi-manager robust architectures, which is currently under detailed review.
- **New Submissions:** Steve highlighted several new submissions that have been acknowledged but not yet reviewed, including logic transformation discrepancies during RTL synthesis and TLB flush on a context switch.
- **Vulnerability Reports:** Steve noted that some submissions appear to be pure vulnerability reports, which may not be suitable for inclusion as new CWE weaknesses but could serve as observed examples or references.

Most Important Hardware Weaknesses Refresh Update

- Gananand encouraged the group to participate in the Most Important Hardware Weaknesses poll, emphasizing its importance in shaping the future of hardware security and the extended deadline for the first poll.
  - **Extended Deadline:** Gananand announced that the deadline for the first poll has been extended to June 23rd, providing more time for participation.
  - **Expert Opinions:** Gananand highlighted the need for expert opinions in the poll to narrow down the list of weaknesses and ensure the most relevant ones are included.
  - **Second Poll:** Gananand explained that a second poll will follow the first, where participants will rate the weaknesses that made it past the first poll based on a Likert scale.

Memory Access Related Weakness: Open Discussion and Working Exercise:

- Bob summarized the key points from the previous meeting's discussion on memory access-related weaknesses in hardware, including the differences in behavior between simulation and synthesized circuits and the proposal to update existing memory weaknesses within CWE.

    - **Out-of-Bounds Access:** Bob highlighted the differences in how out-of-bounds accesses behave between simulation and synthesized circuits, which may lead to security consequences.
    - **Proposal:** Bob mentioned the proposal to update existing memory weaknesses within CWE to include hardware concerns.
    - **Concerns:** Bob noted concerns about creating hardware-specific variants of existing weaknesses, which could complicate the CWE structure.
- **Simulation vs. Synthesis:** Jason Oberg and Sohrab discussed the differences in behavior between simulation and synthesized circuits, noting that simulation can have multi-valued logic (e.g., X, Z) while synthesized circuits only have binary logic (0, 1).
    - **Out-of-Bounds Access:** Jason emphasized the importance of addressing out-of-bounds access weaknesses in hardware, as they can lead to unexpected behavior and security issues.
    - **Simulation Settings:** Jason mentioned that simulation settings can affect the behavior of out-of-bounds accesses, such as turning off X's to force a real value return.
- **Importance of Bounds Checking:** Arun and Sohrab highlighted the importance of implementing proper bounds checking in hardware design to prevent out-of-bounds access issues, with Arun noting that synthesis is not the root cause of the problem.
    - **Bounds Checking:** Arun and Sohrab emphasized the importance of implementing proper bounds checking in hardware design to prevent out-of-bounds access issues.
    - **Synthesis Role:** Arun noted that synthesis is not the root cause of out-of-bounds access issues, but rather the lack of proper bounds checking in the design.
    - **Verification:** Sohrab mentioned that proper verification and validation processes can help ensure that bounds checking is correctly implemented in the design.

- **Clarifying Hardware Weaknesses:** Hareesh and Jason Oberg emphasized the need to clarify hardware weaknesses related to out-of-bounds access, as it is well understood in software but not as clearly defined in hardware.
    - **Clarification Need:** Hareesh and Jason Oberg emphasized the need to clarify hardware weaknesses related to out-of-bounds access, as it is well understood in software but not as clearly defined in hardware.
    - **Software vs. Hardware:** Hareesh noted that out-of-bounds access is a well-understood concept in software, but it needs to be clearly defined and addressed in hardware as well.
    - **Examples:** Jason Oberg suggested providing hardware-specific examples to illustrate out-of-bounds access weaknesses and their potential impact.
- **Next Steps:** Bob proposed a homework assignment for the group to review and suggest updates to the existing CWE-125 entry to cover hardware concerns, with a Google Doc provided for collaboration.