Hardware CWE SI Group
Meeting Minutes[1]
May 9, 2025

Meeting Attendance

Bob Heinemann
Steve Christey Coley
Ganu Kini
Mitchell Poplingher
James Pangburn
Parbati Manna
Jason Oberg
Abraham Fernandez Rubio
Andreas Schweiger
Rachana Maitra
William Ferguson
Paul Wortman
Milind Kulkarni
Thomas Ford
Jason Fung
Hareesh Khattri
Mohan Lal
Remy Stolworthy
Jeremy Lee
Bruce Monroe
Ashrafi Mohammed
Sohrab Aftabjahani
Irena Bojanova
Arun Kanuparthi
Joerg Bormann

Agenda

- Meeting Administration
- Hardware Submissions in Progress
- Memory Access Related Weaknesses, Presentation by Jason Oberg
- Most Important Hardware Weaknesses (MIHW) WG Updates

Meeting Notes

Meeting Administration: Bob initiated the meeting by discussing the general status of hardware submissions and introduced Jason Oberg's presentation on memory access

[1] *This document includes content generated with the assistance of Microsoft Teams Copilot, a generative AI tool. Microsoft Teams Copilot was used to generate the initial draft of the meeting minutes and provide suggestions for summarizing key discussion points. All AI-generated content has been reviewed and edited by the CWE Team to ensure accuracy and completeness.*

related weaknesses in hardware. He also mentioned the next meeting date (June 13) and some general housekeeping announcements, including information about the mailing list, where minutes and meeting recordings are kept, and the public status of the content development repository (CDR).

Hardware Submissions in Progress: Steve provided an update on the current hardware submissions, including discussions with NIST on post-quantum cryptography, a detailed submission from Francesco Restuccia on data validation in multi-manager bus architecture, and a new submission from Fanyun Shu on CPU control bits. He also mentioned some submissions that were just vulnerability reports.

- **Post-Quantum Cryptography:** Steve discussed the submission related to post-quantum cryptography, originally submitted by NIST. He mentioned that several NIST staff members involved in this area have left, and he plans to follow up with NIST to determine the next steps.
- **Data Validation:** Steve provided an update on Francesco Restuccia's submission on data validation in multi-manager bus architectures. Francesco has provided a detailed submission, and the next step is for the CWE team to review the details and potentially have Francesco present to the hardware team.
- **CPU Control Bits:** Steve mentioned a new submission regarding CPU control bits being trusted or modified when they shouldn't be. This submission has been uploaded to CDR, and the team is awaiting further details from the submitter.

Memory Access-Related Weaknesses in Hardware: Jason Oberg presented his thoughts on memory access-related weaknesses in hardware, highlighting the differences between software and hardware in terms of out-of-bounds access. He provided examples and discussed the potential impacts and consequences of these weaknesses in hardware.

- **Context and Examples:** Jason Oberg provided context for the discussion, explaining that while out-of-bounds access weaknesses are well-defined in software, they are not as clearly defined in hardware. He presented examples to illustrate the differences and potential impacts in hardware.
- **Out-of-Bounds Read:** Jason explained that in hardware, an out-of-bounds read might return an undefined value (X) in simulation, but in a synthesized circuit, it could return data from an unexpected location within the same buffer, potentially leading to data leakage or other unintended consequences.
- **Out-of-Bounds Write:** Jason discussed out-of-bounds write weaknesses, noting that in simulation, such writes might be treated as no-ops, but in synthesized

hardware, they could modify unexpected locations within the buffer, leading to data corruption or other issues.

- **Hardware-Specific Consequences:** Jason emphasized the need to consider hardware-specific consequences and mitigations for these weaknesses, suggesting that existing CWEs could be updated to include hardware-specific details rather than creating new hardware-specific CWEs.
- **Discussion on Hardware View of CWEs:** The group discussed the inclusion of memory-related CWEs in the hardware view. Steve suggested updating existing CWEs to include hardware-specific consequences and testing suggestions, rather than creating new hardware-specific CWEs. The group agreed on the need for memory-related weaknesses in the hardware view but decided to continue the discussion in the next meeting.
- **Further Discussion:** The group decided to continue the discussion in the next meeting, acknowledging that more consideration and input are needed to determine the best approach for incorporating hardware-specific details into existing CWEs.
- **Most Important Hardware Weaknesses (MIHW) WG Updates**: Ganu and Arun provided an update on the most important hardware weaknesses, outlining the plan for a two-part survey to collect expert opinions. The first part of the survey will ask for inclusion or exclusion of specific CWEs, and the second part will involve rating the importance of these CWEs. They discussed the timeline for the survey (May 16 – May 23) and the publication of the most important hardware weaknesses list in July
    - **Optional Metadata:** Gananand mentioned the inclusion of optional metadata questions in the survey to help understand the data better, such as name, email, role, and industry.
    - **Purpose and Use:** The purpose of the list was discussed, emphasizing its use for educating designers and validation teams about common hardware weaknesses and ensuring these are considered in design and validation processes.

Action Items

- **Hardware Weaknesses Discussion:** Follow up with the team via email to continue the discussion on memory-related weaknesses in the hardware view and schedule time for the next SIG meeting to work through this topic. (Bob)

- **Survey Time Frame:** Consider extending the survey response time from one week to two weeks to allow members sufficient time to complete the survey. (Gananand)
- **Survey Metadata Questions:** Send an email to the mailing list to gather feedback on the inclusion of optional metadata questions in the survey. (Gananand)