Hardware CWE SI Group
Meeting Minutes
September 12, 2025

Meeting Attendance

Bob Heinemann

Gananand Kini

Steve Christey

Vinod Viswanath

Mitchell Poplingher

Parbati Manna

Hareesh Khattri

Paul Wortman

James Pangburn

Thomas Ford

Amitabh Das

Jeremy Lee

Sohrab Aftabjahani

Arun Kanuparthi

Joe Reisinger

Rafael Machado

Soheil Salehi

Suresh Palaniappan

Rachana Maitra

Ashrafi Gulam Mohammed

Joerg Bormann

Agenda

- CWE Gaps Based on the Most Important Hardware Weakness Data

Meeting Notes

Pre-Agenda: Bob outlined the meeting agenda, which includes a quick review of the most important hardware weaknesses and a presentation by Hareesh and Arun from Intel on potential gaps within the corpus.

- **October Meeting Reminder:** Bob reminded everyone about the next meeting scheduled for October 10th at 12:30 PM Eastern Time.
- **CWE Release Announcement:** Bob announced the recent release of CWE 4.18, which includes a new view for the 2025 most important hardware weaknesses.
    - **New View:** Bob explained that the new view, numbered 1432, was introduced as part of the release and is specifically for the 2025 most important hardware weaknesses. The new view also includes a category called expert insights, which highlights items that ranked high in polling but lacked weakness data to back them up.

- **Content Development Repository:** Bob highlighted the content development repository as a public and transparent way to process submissions for updating existing entries or proposing new weaknesses.
    - **Repository Overview:** Bob described the content development repository as a public and transparent platform for processing submissions, including updates to existing entries and proposals for new weaknesses.

Most Important Hardware Weaknesses Overview: Bob provided an overview of the most important hardware weaknesses, explaining the methodology used to compile the list and the new view created for the 2025 list.

- **Methodology:** Bob detailed the methodology used to compile the list, including data collection, filtering, and combining expert opinions with weakness data.
- **Accessing the List:** Bob demonstrated how to access the list on the website, highlighting the new view created for the 2025 list and its advantages for programmatic access.
- **White Paper Version:** Bob mentioned that a white paper version of the list is available for download, providing an offline reading option.

Hardware Fabric Issues: Hareesh Khattri discussed hardware fabric issues, including silent transaction drops and memory corruption, and emphasized the need for more detailed weaknesses in this area.

Protocol Violations: Hareesh highlighted issues with protocol violations in AXI fabric implementations and PCIe handling, noting the need for better handling of malformed or unexpected packets.

Security Implications: Hareesh explained that these weaknesses could have significant security implications, especially in the context of confidential computing, where secure paths are critical.

Community Input: Hareesh encouraged the community to provide input and share similar experiences to help identify and propose new CWEs or update existing ones.

Address Translation and Range Checking: Hareesh Khattri highlighted the importance of address translation and range checking in hardware security, noting that there are gaps in the current CWE coverage for these issues.

    - **Importance:** Hareesh Khattri emphasized the critical role of address translation and range checking in hardware security, noting that these mechanisms are essential for access control and memory protection.

    - **Current Gaps:** Hareesh pointed out that there are gaps in the current CWE coverage for address translation and range checking issues, suggesting the need for new or updated CWEs to address these weaknesses.

    - **Examples:** Hareesh provided examples of potential weaknesses, such as incorrect implementation of translation tables, synchronization issues, and concurrency problems, which could compromise hardware security.

    - **Community Feedback:** Hareesh invited feedback from the community on how they handle these issues within their organizations and encouraged proposals for new CWEs or updates to existing ones.

- **Processor Instruction Issues:** Hareesh Khattri raised the topic of processor instruction issues, questioning whether specific examples should be detailed or if a high-level CWE is sufficient.

    - **Instruction Issues:** Hareesh Khattri discussed processor instruction issues, such as the improper handling of partially completed instructions due to hardware interrupts and questioned whether specific examples should be detailed or if a high-level CWE is sufficient.

    - **Security Consequences:** Hareesh noted that these issues could have significant security consequences, such as data exposure or denial of service, and emphasized the need to address them in CWEs.

    - **Community Input:** Hareesh sought input from the community on whether to create specific CWEs for these issues or to bundle them under a high-level CWE, highlighting the importance of community feedback in this decision.

    - **Research and Examples:** Hareesh mentioned ongoing research in hardware security that focuses on microarchitectural state exposure and data leakage, suggesting that these findings could inform the creation of new CWEs.

- **Side Channel and Physical Attacks:** Hareesh Khattri mentioned new papers on side channel and physical attacks, noting that the group had previously decided not to enumerate all possible side channel leakage methods in CWE.

    - **New Papers:** Hareesh Khattri mentioned new papers on side channel and physical attacks, including infrared, acoustic, magnetic, and laser-based attacks, highlighting the ongoing research in this area.
    - **Previous Decision:** Hareesh noted that the group had previously decided not to enumerate all possible side channel leakage methods in CWE, suggesting that this approach should continue.
- **Call for Proposals:** Hareesh Khattri encouraged participants to analyze the gaps discussed and propose new or updated CWEs based on their findings.
    - **Encouragement:** Hareesh Khattri encouraged participants to analyze the gaps discussed during the meeting and propose new or updated CWEs based on their findings and experiences.
    - **Community Involvement:** Hareesh emphasized the importance of community involvement in identifying and addressing weaknesses, inviting participants to share their insights and contribute to the development of CWEs.

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.