Hardware CWE SI Group
Meeting Minutes[1]
April 11, 2025

Meeting Attendance

Arun Kanuparthi	Jason Fung	Rachana Maitra
Bob Heinemann	Krzysztof Kepa	Shawn Siah
Bruce Monroe	Milind Kulkarni	Sohrab Aftabjahani
Gananand Kini	Mitchell Poplingher	Steve Christey
Hareesh Khattri	Mohan Lal	Thomas Ford
Irena Bojanova	Parbati Manna	William Ferguson
James Pangburn	Pieter Van Wassenaer	

Agenda

- Meeting Administration
- CWE 4.17 Release
- Status of Submissions
- Most Important Hardware Weaknesses (MIHW) WG Updates

Meeting Notes

- **Meeting Administration:** Bob outlined the meeting agenda, which includes discussing the status of submissions, commentary on the recent release CWE 4.17, and receiving updates on the subgroup compiling the Most Important Hardware Weaknesses list for 2025.

---

[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.*

    - **Long CWE Titles:** Bruce raised a concern before the next topic about the length of CWE titles, suggesting that they could be shortened using AI and including the CWE number in brackets for easier reference.
        - Bob acknowledged the concern and suggested that they could discuss it further at the end of the meeting. He expressed interest in understanding the challenges Bruce mentioned.

- **CWE 4.17 Release:** Bob announced the release of CWE 4.17, which includes three new weaknesses, usability improvements, and the creation of diagrams to demonstrate weaknesses. He encouraged the team to review the entries and provide feedback.
    - **Usability Improvements:** Bob highlighted several usability improvements, including streamlining descriptions and moving impact type language to appropriate sections like consequences and mitigations.
    - **Diagrams Creation:** Bob mentioned the creation of diagrams to pictorially demonstrate weaknesses, which are oriented along with the descriptions. This effort has been ongoing for the past three releases, with updates made to 40 or 50 entries.
    - **Feedback Encouraged:** Bob encouraged the team to review the updated entries and provide feedback, especially for hardware entries that might benefit from these usability improvements.
    - **Content Development Repository (CDR):** Bob shared that the content development project is now fully public, allowing the broader community to view submissions, make comments, and contribute to entry development. Steve added that submissions are manually reviewed before being uploaded to the CDR.
- **Status of Submissions:** Bob and Steve provided updates on two hardware submissions in progress: the use of quantum vulnerable cryptographic algorithms and speculative propagation of requests for transactions for data validation in multi-manager bus architectures.
    - **Quantum Vulnerable Cryptography:** Bob mentioned that the submission on the use of quantum vulnerable cryptographic algorithms is still in the early phase, with clarifying questions sent to the submitter. Steve added that they are considering whether to update existing submissions or create new ones to address quantum vulnerabilities.

    - **Speculative Propagation:** Bob provided an update on the submission from Francesco regarding speculative propagation of requests for transactions for data validation in multi-manager bus architectures. He noted that significant progress has been made, and they are now in the full submission request phase, awaiting additional details from the submitter.
    - **Consultation Phase:** Steve explained that the quantum vulnerable cryptography submission is still in the consultation phase as they determine whether to create new entries or update existing ones. He mentioned that they had a meeting with NIST staff to discuss this issue.
    - **Next Steps:** Bob and Steve outlined the next steps for both submissions, including further consultation and gathering additional details from the submitters to finalize the entries.
- **New Hardware Entries:** Bob introduced two new hardware entries: CWE-1429, submitted by Amisha Srivastava (*CWE-1429: Missing Security-Relevant Feedback for Unexecuted Operations in Hardware Interface*), and CWE-1431 (*CWE-1431: Driving Intermediate Cryptographic State/Results to Hardware Module Outputs*), submitted by Andres Meza. Both entries received valuable input from the community and are now part of the hardware view.
    - **CWE-1429:** Bob introduced CWE-1429, submitted by Amisha Srivastava, which addresses hardware interfaces that silently discard operations in situations where feedback is security relevant. He thanked Amisha and the community for their valuable input in shaping this entry.
    - **CWE-1431:** Bob introduced CWE-1431, submitted by Andy Meza, which deals with hardware modules implementing cryptographic algorithms that write sensitive information about intermediate states or results to output wires. He noted that this issue is commonly observed in the community's analysis.
    - **Community Input:** Bob emphasized the importance of community input in developing these entries and acknowledged the contributions that helped shape them.
    - **Placement in Hardware View:** Steve mentioned that the placement of these entries in the hardware view was a last-minute decision and invited further discussion if anyone disagreed with their current placement.

- **Most Important Hardware Weaknesses (MIHW) WG Updates**: Gananand, Arun, and Hareesh provided updates on the progress of the most important hardware weaknesses project, including the completion of vulnerability data collection and the upcoming expert opinion survey.
    - **Expert Opinion Survey:** Gananand outlined the tentative schedule for the expert opinion survey, which will be conducted in two parts. The first part will collect opinions on which CWEs should be included in the list, and the second part will involve rating the importance of these CWEs.
    - **Survey Methodology:** Gananand explained that the survey methodology would follow the same approach as the first round, combining vulnerability data and expert opinions to create the final list of important hardware weaknesses.
    - **Community Involvement:** Arun and Hareesh emphasized the importance of community involvement in reviewing the collected data and providing feedback to ensure accuracy and completeness. They encouraged members to cross-check the data and provide additional insights.

Action Items

- **CWE Title Length Issue:** Review the current process for handling long CWE names and explore operational solutions to address the issue. This potentially would be a CWE 5.0 item. The release date for CWE 5.0 has not been set yet. (Bob, Steve)