Hardware CWE SI Group
Meeting Minutes[1]
March 14, 2025

Meeting Attendance

- Sohrab Aftabjahani
- Irena Bojanova
- Steve Christey Coley
- Amitabh Das
- Keerthi Devraj
- Daniel DiMase
- William Ferguson
- Thomas Ford
- Gordon Frye
- Jason Fung
- Alexander Harner
- Bob Heinemann
- Arun Kanuparthi
- Hareesh Khattri
- Gananand Kini
- Rachana Maitra
- Parbati Manna
- Andres Meza (guest)
- Dave Morse (guest)
- James Pangburn
- Mitchell Poplingher
- Jason Oberg
- Amisha Srivastava
- Kathryn Stout
- Alec Summers
- Shivam Swami
- Remy Vanece Stolworthy
- Paul Wortman

Agenda

- Meeting Administration
- General Status of Current HW CWE Submissions
- HW Crypto Leak Submission Review
- Most Important Hardware Weaknesses Refresh Update
- Meeting Conclusion

Meeting Notes

- **Meeting Administration:** Gananand Kini outlined the meeting agenda, and noted that the next CWE HW SIG meeting will take place April 11 from 12:30 pm – 1:30 pm ET.
    - **Announcements:** Gananand announced the release of CWE 4.16, which included the 2024 top 25, and mentioned that CWE 4.17 is scheduled for release on April 3, with a content freeze on March 31. The Content

---

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.

Development Repository (CDR) on GitHub will also be made public with the 4.17 release.

- **Hardware Submissions Update**: Steve Christey Coley provided an update on various hardware-related submissions, including discussions with NIST on quantum-vulnerable cryptographic algorithms (initial consultation – stage 1, phase 4), speculative propagation of requests for transaction before data validation in multi-manager bus architectures (ready for acceptance – stage 1, phase 6), improper protection of intermediate cryptographic state/results (details received – stage 2, phase 8), and a lack of feedback in unexecuted operations across system interfaces for security-critical operations (detailed consultation – stage 2, phase 10).
    - **Amisha's Submission Feedback**: Steve and Amisha Srivastava discussed the feedback received on Amisha's submission, a lack of feedback in unexecuted operations across system interfaces for security-critical operations. The discussion focused on the importance of providing security-critical feedback for unexecuted operations. They also streamlined the discussion of the weakness and discussed the value of using terms like “security critical,” "security relevant," and "security sensitive" instead of "security critical."
    - The community discussed the value of clarifying the names of who receives feedback, with consensus suggesting they should be termed “authorized entities,” as opposed to administrators or operators, to ensure clarity and prevent misunderstandings. Rachana Maitra noted that the use of “critical” demands a metric, so “security sensitive” may be more applicable.
    - Jason Fung asked about the way to share feedback and via which channels, recommending that the design specifications specify the user.
- **Proposed CWE**: Andres Meza presented updates on a proposed CWE, “Driving Intermediate Cryptographic State/Results to Hardware Module Outputs,” that he is developing with Jason Oberg. Andres emphasized the need for zeroing techniques to prevent leakage, showing the effectiveness of these techniques in preventing information leakage. He also provided a case study on the OpenTitan project, demonstrating how intermediate cryptographic states were being leaked to hardware module outputs and the importance of addressing this issue. The submission includes bad vs. good code, which can be used in simulations or formal verification engines. Steve noted that the pull request for a fix to the OpenTitan

project, if accepted, is sufficient to use as an observed example even if it lacks a CVE; however, additional suggestions from the community are welcome.

    - **Community Feedback:** Community members provided feedback on the submission, suggesting more generalized applicability to sensitive information other than intermediate cryptographic operations and emphasizing the importance of preventing leakage to attacker-observable outputs.
    - Steve noted that the latest versions use cryptographic state as an example of sensitive information, but that it is still important to talk about hardware module outputs. There is a separate task that considers more generalized hardware and software independent of that kind of weakness, but this will not be included in the 4.17 release. Steve also noted that the submission is available for review in the CDR.

- **Most Important Hardware Weaknesses Refresh – March 2025 Update:** Gananand provided an update on the most important hardware weaknesses refresh, mentioning that data collection is expected to be completed by the end of next week, or around March 21. Next steps include combining CVE data with expert opinions from the HW CWE SIG, compiling the list by applying methodology, and coordinating communications. Next steps are to identify how to collect.