Hardware CWE SI Group
Meeting Minutes[1]
December 13, 2024

Meeting Attendance

- Abraham Fernandez Rubio
- Amisha Srivastiva
- Amitabh Das
- Arun Kanuparthi
- Ashrafi Gulam Mohammed
- Bob Heinemann
- Daniel DiMase
- Gananand Kini
- Hareesh Khattri
- Irena Bojaneva
- James Pangburn
- Jason Oberg
- Jeremy Lee
- John Hallman
- Keerthi Devraj
- Krzystof Kepa
- Mike Borza
- Milind Kulkarni
- Mitchell Poplingher
- Mohan Lal
- Parbati Manna
- Paul Wortman
- Rafael dos Santos
- Rafael Machado
- Steven Christey Coley
- Thomas Ford

Agenda

- Meeting Administration
- CDR Hardware Submissions
- Use Cases for Hardware Weaknesses List
- Meeting Conclusion

Meeting Notes

- **Meeting Administration:** Bob introduced the agenda for the meeting, which focused on refreshing the list of the most important hardware weaknesses. He mentioned the need to revisit the list due to internal and community interest and outlined the plan to form a working group for this task.
    - **Working Group Formation:** Bob announced the formation of a working group to work on the new list of hardware weaknesses, with Gananand leading the effort. Volunteers were called to join this group to help define the

[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.*

methodology, set timelines, collect feedback, and prepare the final list for publication.

    - **Meeting Series for 2025:** Bob announced that a new meeting series for 2025 would be scheduled, maintaining the same frequency and time as the current year's meetings.

- **CDR Hardware Submissions:** Steven provided an update on the status of hardware submissions in the Content Development Repository (CDR), discussing specific submissions related to cryptographic state protection, speculative propagation of requests, and quantum-vulnerable cryptographic algorithms.
    - **Speculative Propagation:** Steven mentioned another submission focused on speculative propagation of requests for transactions in multi-manager bus architectures. The team has received replies from the submitter and needs to decide on the next steps.
    - **Quantum-Vulnerable Algorithms:** Steven highlighted a submission related to quantum-vulnerable cryptographic algorithms, noting NIST's interest in seeing CWE coverage of this topic. The discussion has focused on attacks against quantum-vulnerable algorithms rather than underlying weaknesses, making it a complex issue to address.
    - **Initial Consultation Phase:** Steven explained that all three submissions are in the initial consultation phase, where the team figures out the name, scope, and fit of the weakness within the broader CWE hierarchical organization.
        - **Quantum Vulnerable Cryptography:** Steven and Parbati discussed the growing interest in quantum-vulnerable cryptographic algorithms, mentioning recent advancements and the need to include quantum considerations in CWE coverage, especially Google’s new Willow chip. NIST has shown direct interest in the status of related submissions.
        - **Quantum Considerations:** Steven emphasized the importance of including quantum considerations in modernizing CWE coverage, despite the challenges in fitting new quantum-related weaknesses into the existing hierarchical organization.
    - **Practical Attacks:** Steven noted that practical quantum-based attacks seem to be far off, but it remains a security preference for some product owners to address quantum vulnerabilities proactively.

- **Use Cases for Hardware Weaknesses List:** Gananand led a discussion on how members use the most important hardware weaknesses list, with participants like Jason, Parbati, Ashrafi, and Thomas sharing their use cases, including guiding customers, creating review checklists, and justifying testing.
    - **Internal Awareness:** Parbati mentioned using the list within their semiconductor company to raise awareness among security architects and designers about prevalent weaknesses and to ensure these are mitigated in their products.
    - **Review Checklists:** Ashrafi explained that the list is used to create review checklists for design reviews, ensuring that the most important weaknesses are mandatorily checked and mitigated in their designs.
    - **Justifying Testing:** Thomas highlighted that the list is used to justify testing and to look for particular issues in new designs, ensuring that potential weaknesses are identified and addressed early in the design process.
  - **Previous Methodology:** Gananand explained the methodology used for the previous hardware weaknesses list, which involved polling members and using the Delphi method to identify the top weaknesses.
    - **Delphi Method:** Gananand explained that the previous list was created using the Delphi method, where members were polled to identify the top 10 hardware weaknesses based on nine significance questions. The responses were then combined and weighted to form the final list.
    - **Polling Process:** Members were asked to assign the identified weaknesses into different support buckets during a live poll, and the results were used to create a primary group of 12 most important weaknesses and a secondary group of weaknesses on the cusp.
    - **Significance Questions:** The nine significance questions used in the polling process included factors like weakness detection, mitigations, phases of introduction, and whether physical access was required to exploit the weakness.
  - **Changes in Hardware CWE:** Gananand highlighted the changes in hardware CWE since version 4.6, including new weaknesses and categories, and the need to consider these in the new list.

Action Items

- **Forming Ad Hoc Group:** Form an ad hoc group to define the methodology for updating the most important hardware weaknesses list and set timelines for the activity. (Gananand)