Hardware CWE SI Group
Meeting Minutes
July 11, 2025

Meeting Attendance

- Bob Heinemann
- Gananand Ganesh Kini
- Alec Summers
- Steve Christey
- Mitchell Poplingher
- Parbati Manna
- Abraham Fernandez Rubio
- James Pangburn
- Mohan Lal
- Thomas Ford
- Bruce Monroe
- Sohrab Aftabjahani
- Hareesh Khattri
- Paul Wortman
- Alexander Harner
- Arun Kanuparthi
- Ashrafi Gulam Mohammed
- Soheil Salehi
- Jeremy Lee
- Joe Reisinger
- Amitabh Das
- Keerthi Devraj

Agenda

- Most Important Hardware Weaknesses Refresh Update
- Memory Access Related Weakness: Working Exercise

Meeting Notes

Pre-Agenda: Bob announced that the next meeting is scheduled for August 8th and reminded everyone about the public content development repository. He also mentioned that the second poll for the Most Important Hardware Weaknesses List is closing tonight, July 11, at 11:59 PM Pacific Time.

- **Public Repository:** Bob reminded the group that the content development repository has been public for some time. He encouraged members to check the repository to see submissions currently being processed if interested.
- **Hardware Implants Discussion:** Tom Ford raised a question about hardware implants and their related weaknesses, referencing a Bloomberg story about a Supermicro implant. Bob and Paul discussed the challenges of fitting supply chain issues within CWE and the need for more development around physical access-related CWEs.

Most Important Hardware Weaknesses Refresh Update: Gananand provided an update on the Most Important Hardware Weaknesses (MIHW) effort, mentioning that they have received 19 responses so far to the poll. The poll will close tonight, and data analysis will begin soon. The final list is expected to be published by the end of July. He mentioned that they are finalizing the list this week and will coordinate communications around the list with all members.

- **Methodology for Hardware Weaknesses List:** Gananand explained the methodology used for the hardware weaknesses list, which includes a combination of expert opinion and data-based approaches. The Delphi method was used for the second poll, and the final list will be generated based on weighted scores.
    - **Weighted Scores:** Gananand described how the final list will be generated based on weighted scores. Responses are weighted with +2 for strongly include, +1 for include, 0 for neither include nor exclude, -1 for exclude, and -2 for strongly exclude.
    - **Handling Empty Responses:** Gananand mentioned that some responses were empty because the questions were optional. These empty responses will be replaced with "neither include nor exclude" to ensure they do not affect the scores.
    - **Final Data Analysis:** Gananand stated that the final data analysis will be performed next week, and the new list will be generated based on the analysis. The working group is also working on a write-up to document the process and methodology used.
- **Subjectivity of the Survey:** Sohrab raised a concern about the subjectivity of the survey results, suggesting that different groups of people might produce different results. Gananand assured that limitations and disclaimers will be included in the write-up.
    - **Limitations and Disclaimers:** Gananand assured that the write-up will include a section on the limitations of the methodology and the subjective nature of the expert poll. This will help readers understand the context and limitations of the results.

Memory Access Related Weakness: Working Exercise: Bob led a working exercise to discuss memory access-related weaknesses and how to add hardware concerns to existing entries. The group reviewed CWE-125 (Out-of-bounds Read) and considered potential updates to address hardware concerns. He explained the color-coding scheme used in the document to differentiate between existing text and proposed additions.

- **Challenges Identified:** The group identified challenges in updating the entry, such as ensuring the text captures hardware concerns without fundamentally changing the existing content. They discussed the need for further research and development of hardware-specific text.
- **Common Consequences for Hardware:** The group discussed the common consequences of out-of-bounds reads and whether the existing impacts apply to hardware. They considered adding specific impacts and examples to better capture hardware concerns.
    - **Examples and Context:** Participants suggested including examples and context to illustrate hardware-specific impacts. They discussed the importance of providing clear and precise descriptions to enhance understanding.
    - **Further Review Needed:** The group agreed that further review and development are needed to finalize the updates. They planned to continue working on the document and incorporate additional suggestions and comments.
- **Next Steps for Memory Access Weaknesses:** Bob invited participants to review the document and add their comments and suggestions for hardware concerns. The goal is to develop a model for updating entries to capture hardware concerns.

Action Items

- **Hardware Weaknesses Poll:** Complete the most important hardware weaknesses poll by 11:59 PM Pacific Time. (All Participants)
- **Hardware Weaknesses List:** Coordinate communications around the final list of hardware weaknesses with all members. (Gananand)

- **Hardware Weaknesses Methodology:** Include a section on limitations in the write-up for the hardware weaknesses methodology. (Gananand)
- **Memory Access Weaknesses:** Review and provide additional hardware context for the impacts of out-of-bounds read weaknesses. (All Participants)
- **Memory Access Weaknesses:** Add suggestions for hardware concerns to the Google document for CWE 125 out-of-bounds read. (All Participants)