Hardware CWE SI Group
Meeting Minutes[1]
November 8, 2024

Meeting Attendance

- Bob Heinemann
- David Rodriguez
- Robert Roberge
- Jiang Fu
- Irena Bojaneva
- Alexander Harner
- Alec Summers
- Steve Walters
- Shivam Swami
- Gananand Kini
- Soheil Salehi
- Paul Wortman
- Gage Hackford
- Arvind Sharma
- Priya Iyer
- Rafael dos Santos
- Steve Christey Coley
- Krzysztof Kepa
- Alan Sorensen
- Gus Serino
- Shawn Siah
- Amisha Srivastava
- Milind Kulkarni
- Marisa Harriston
- Rafael Machado
- Mitchell Poplingher
- Pieter Gerard Van Wassenaer
- Amitabh Das
- Arun Kanuparthi
- Banafsheh Saber Latibari
- Parbati Manna
- Joerg Bormann

Agenda

- Meeting Administration
- Release 4.16 Update
- Presentation on Security Issues in Hardware Design by Joerg Bormann
- Presentation on Lack of Feedback for Unexecuted Operations Across System Interfaces by Amisa Srivastava
- Meeting Conclusion

Meeting Notes

- **Meeting Administration:** Bob introduced the November SIG meeting, mentioning two presenters: Joerg Bormann, who will continue his presentation from 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.*

October meeting, and Amisha Srivastava, who provided updates on a CWE entry in development.

    - **December Meeting:** Bob announced the next meeting scheduled for 13-Dec-2024, noting that December meetings often get canceled due to people's lack of availability due to Holidays.

- **Release CWE 4.16 Update:** Steve confirmed that the release date for version 4.16 has been delayed to 19-Nov-2024. Bob mentioned a planned release for early 2025, which could be a major or minor release.
- **Presentation on Security Issues in Hardware Design by Joerg Bormann:** Joerg continued his presentation from 11-Oct-2024, on security issues in hardware design, focusing on the relationship between physical processes and digital descriptions, and the importance of abstraction in understanding chip behavior.
    - **Digital Abstraction:** Joerg explained the digital abstraction, introducing thresholds to define signal values as either 0 or 1, and discussed the concept of metastability.
    - **Synchronous Abstraction:** Joerg described the synchronous abstraction, defining small windows around each rising edge of the clock and the importance of propagation delay in ensuring proper chip functionality.
    - **Propagation Delay Requirement:** Joerg explained the concept of propagation delay and its importance in ensuring that combinatorial logic settles on new values within the clock cycle time, highlighting potential attack vectors that could exploit propagation delay issues.
    - **Combinatorial Logic and Feedback Loops:** Joerg discussed the risks associated with complex combinatorial logic and combinatorial feedback loops, proposing 2 new CWE entries to address issues.
    - **Inappropriate Clock Domain Crossings:** Joerg highlighted the importance of properly implemented clock domain crossings to prevent unpredictable behavior and data integrity issues, proposing a new CWE entry for this weakness.
    - **Discussion on Security Implications:** Arun and Steve raised questions about the security implications of the issues Joerg presented, discussing the potential for these weaknesses to be exploited in security-critical parts of the design.

        - **Metastability:** Arun questioned how metastability could cause security impacts, to which Joerg responded that metastability makes the circuit behave differently than specified, potentially allowing attackers to exploit this for fault insertion attacks.
        - **Combinatorial Feedback Loops:** Arun asked if combinatorial feedback loops would be caught by synthesis tools. Joerg explained that while synthesis tools may find these loops, warnings need to be taken seriously, and loops can still be created during physical design.
        - **Security Context:** Steve asked for specific examples of how combinatorial feedback loops could introduce vulnerabilities. Joerg responded that poorly written RTL or Trojans could introduce these loops, affecting security-critical parts of the design.
- **Presentation on Lack of Feedback for Unexecuted Operations Across System Interfaces by Amisa Srivastava:** Amisha presented updates on a new CWE entry, providing examples and potential mitigations for this weakness.
    - **Introduction:** Amisha presented a detailed review of a new CWE entry for lack of feedback for unexpected operations across system interfaces, explaining how this weakness can lead to data loss, security vulnerabilities, and system instability.
    - **Examples:** Amisha provided examples of where this weakness can be found, including systems on chips like OpenTitan, microcontroller interrupt systems, and network interface controllers.
    - **Mitigations:** Amisha recommended incorporating structured logging and feedback mechanisms during the architecture and design phase, using implementation phase checks, and employing automated static analysis and manual code reviews to detect this weakness.
    - **Discussion on Lack of Feedback:** HW SIG Members discussed the intentional design choices related to lack of feedback, debating whether it constitutes a security issue or a functional issue.
        - **Intentional Design:** Arun and Joerg argued that lack of feedback is often an intentional design choice to avoid wasteful traffic, prevent information weakness, and brute force attacks, questioning whether it constitutes a security issue.

    - **Security vs. Functionality:** Steve highlighted the importance of logging for forensics and incident response, suggesting that lack of feedback could still be a security issue if it prevents actionable information from reaching admins or operators.
    - **Real-World Scenarios:** Steve emphasized the need to consider real-world scenarios where lack of feedback could lead to security vulnerabilities, even if the design choice is intentional.
    - **Boundary that Separates a Functional Problem from a Security Problem:** Manna emphasized that we need to be careful not to treat every functional issue as a security problem or we'll get lost.
- **Meeting Conclusion:** Bob suggested having Joerg return for an open discussion on the material presented in the next SIG meeting and reminded everyone of the next planned meeting on December 13th.

Action Items

- **Feedback on CWE Entry:** Provide feedback on new CWE entries proposed by Joerg. Please refer to his presentation. (All participants)
- **Follow-up Discussion on Hardware Security Issues:** Coordinate with Joerg to schedule a follow-up discussion on the hardware security issues presented, ensuring ample time for open discussion. (Bob)