Hardware CWE SIG Group
Meeting Minutes
October 11, 2024

Meeting Attendance

- Joerg Bormann
- Steven M Christy
- Jason M Fung
- Bob Heinemann
- Parbati K Manna
- Jason Oberg
- Daniel DiMase
- John Hallman
- Mike Borza
- Bronn Pav
- Thomas Ford
- Keerthi Devraj
- Mohan Lal
- Irena Bojanova
- Gordon Frye
- Sandy Frost
- Alexander Harner
- Mithra Mirhassani
- David Kaplan
- Sherman Brent
- Arun Kanuparthi
- Jeremy Lee
- Amitabh Das
- James Pangburn

Agenda

- Hardware Weakness Discussion
- Security Issues Arising from Hardware Design

Hardware Weakness Discussion

Bob summarized the ongoing discussion about refreshing the most important hardware weakness list, which has not been updated in three years. He mentioned the need for data to support the new list and the possibility of forming an ad hoc committee to define and execute the update.

General Announcements

Bob provided general housekeeping reminders, including the next meeting date (November 8th, 2024) and contact information. He also announced that the CWE 4.16 release has been pushed back to November.

Security Issues Arising from Hardware Design

Joerg Borman introduced himself and his work on formal verification at Siemens EDA. He explained that he would discuss hardware coding rules and their impact on security, highlighting several specific weaknesses.

- Hardware Coding Rules: Joerg highlighted that certain hardware coding rules, although basic, can lead to unexpected behavior on the hardware side and security vulnerabilities if violated. He mentioned specific

weaknesses such as simulation synthesis mismatches, unused logic, and inappropriate clock domain crossings.

- Simulation Synthesis Mismatches: Joerg discussed the issue of simulation synthesis mismatches, where simulators and synthesis tools interpret RTL code differently. He provided examples and proposed a new CWE entry to address this issue.
    - **Examples:** Joerg provided examples of mismatches, such as combinatorial logic blocks and the use of 'X' in RTL, which can lead to different interpretations by simulators and synthesis tools.
    - Proposed CWE: Joerg proposed a new CWE entry to address simulation synthesis mismatches, highlighting the need for better coverage of this issue in CWE.
- Dead Logic in Hardware: Joerg explained the concept of dead logic in hardware, where unused logic can still consume power and potentially create security vulnerabilities. He proposed extending existing CWEs or creating a new one to address these hardware-specific issues.
    - Examples: Joerg provided an example of an if-then-else branch where the else branch is dead but still consumes power, potentially leading to security issues.
    - Proposed CWE: Joerg proposed extending existing CWEs or creating a new one to address the hardware-specific issues related to dead logic, emphasizing the different consequences compared to software dead logic.
    - Discussion: Participants, including Steven and Jason, discussed the implications of dead logic in hardware and the need for better coverage in CWE, considering the unique challenges and security risks it poses.
- Storage Elements Without Reset: Joerg highlighted the problem of storage elements without reset in hardware, which can lead to unpredictable behavior. He suggested either extending an existing CWE or creating a new one to address this issue.
    - Cost Implications: Joerg noted that implementing resets for all state bits is expensive, especially for RAMs, and discussed the trade-offs between cost and security.

    - Verification: Joerg emphasized the importance of verification to cover all potential reset states, suggesting that failure to do so is a weakness that needs to be addressed.
    - Proposed CWE: Joerg proposed either extending an existing CWE or creating a new one to address the issue of storage elements without reset, considering the unique challenges in hardware design.
    - Discussion: Participants, including Steven and Jason, discussed the challenges and potential solutions for verifying and initializing hardware elements, debating the balance between cost and security in implementing resets and verifications.
- Discussion on Verification and Initialization: Joerg and other participants, including Steven and Jason, discussed the challenges and potential solutions for verifying and initializing hardware elements. They debated the balance between cost and security in implementing resets and verifications.
    - Verification Challenges: Joerg and participants discussed the challenges of verifying hardware elements, particularly the difficulty of ensuring all potential reset states are covered.
    - Cost vs. Security: Participants debated the balance between cost and security in implementing resets and verifications, considering the trade-offs and potential risks.
    - Formal Methods: Joerg mentioned the use of formal methods to verify that behavior is consistent regardless of reset states, highlighting the importance of applying these methods hierarchically.
    - Practical Solutions: Participants discussed practical solutions, such as resetting only control logic or using valid signals to manage uninitialized data, to balance cost and security.