Hardware CWE SI Group
Meeting Minutes
October 10, 2025

Meeting Attendance

Bob Heinemann
Alec Summers
Steve Christey
Francesco Restuccia
Thomas Ford
Priya Iyer
Joe Reisinger
Ashrafi Gulam Mohammed
James Pangburn
Jason Fung
Jeremy Lee
Mohan Lal
Vinod Viswanath
Kepa, Krzysztof
Rachana Maitra
William Ferguson
Das, Amitabh
Hareesh Khattri
Jason Oberg
Arun Kanuparthi
Shafqat Ullah
Sohrab Aftabjahani
Abraham Fernandez Rubio

Agenda

- HW Submission Review: Improper Request Propagation before Data Reception in Write Transactions in a Bus Architecture

Meeting Notes

Introduction and Administrative Announcements

The meeting was opened by Bob Heinemann, who welcomed a notably large group of participants and reminded everyone that the session was being recorded. Bob emphasized the collaborative nature of the SIG, inviting attendees to propose topics for future meetings and reminding them of the next scheduled session on November 14th. He also referenced recent publications on hardware weaknesses and the availability of the CDR for those interested in further resources.

Hardware Submission Presentation: Improper Request Propagation before Data Reception in Write Transactions in a Bus Architecture

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.

Francesco Restuccia, a researcher at UC San Diego, delivered the main presentation, focusing on a hardware weakness related to improper request propagation in bus architectures.

Francesco explained that in multi-manager shared bus systems, the on-chip interconnect may speculatively write requests before the corresponding data is available.

This speculative forwarding, while intended to optimize performance, can inadvertently reserve shared resources for incomplete transactions, resulting in blocking conditions that affect the entire system.

He noted that the widely used AXI protocol does not specify a timeout or abort mechanism for such transactions, instead assuming that all controllers will behave cooperatively and provide data promptly.

When this assumption fails, due to either malicious or faulty controllers, the system can experience indefinite stalls and denial of service.

Demonstration and Technical Details

To illustrate the problem, Francesco described a series of experiments using FPGA platforms and custom hardware accelerators. He showed how a single misbehaving controller could monopolize access to shared memory, effectively locking out other controllers and causing a denial of service. The demonstration included waveform tracking results, which visually confirmed the blocking conditions and the resulting system-wide impact. Francesco stressed that this weakness is particularly relevant in mission-critical domains such as automotive, avionics, medical devices, robotics, and data centers, where availability failures can lead to missed deadlines, system resets, or even safety hazards.

Impact and Mitigation Strategies

Francesco outlined several mitigation approaches. The store-and-forward method buffers the entire transaction before forwarding it, which can prevent stalls but introduces significant latency and hardware overhead. The cut-and-forward technique, developed by Francesco's team, splits transactions into smaller chunks and forwards them only when the data is ready, striking a balance between latency, area, and system availability. Another approach, monitor recovery, uses logic to detect stalls and complete stalled transactions with dummy data, thereby restoring the interconnect to a functional state. Each method

involves trade-offs, and Francesco emphasized the importance of considering both performance and security when selecting a mitigation strategy.

Discussion and Participant Questions

The presentation sparked a robust discussion among attendees. Hareesh asked about the lack of timeout mechanisms in AXI, and Francesco clarified that the protocol's design relies on cooperative behavior, leaving systems vulnerable to indefinite delays. Rachana raised concerns about the severity of denial of service, especially in critical systems, and both Francesco and Steven agreed that such availability issues are serious enough to warrant inclusion as a weakness.

Ashrafi inquired about detection and correction mechanisms, such as timeouts, and Francesco explained that monitor recovery involves watchdog timers but must also ensure compliance with the AXI standard.

Jason brought up CWE-1264, which deals with race conditions in data communication channels, and suggested reviewing it for overlap with Francesco's submission. Francesco responded that while CWE-1264 focuses on security checks, his submission addresses operational issues in bus communication.

Sohrab questioned the use of cut-through switching given the cooperative assumptions, and Francesco explained that while store-and-forward is safer, it is often impractical due to area and latency costs, making cut-through a common but riskier choice.