Microarchitectural Side Channels (uSC) SIG

April 9, 2024

Agenda

- Disclosures
- Follow up: any remaining questions from Tech Chairs presentation?
- Kick-off for Microarchitecture Security Guide (collaborative drafting)

Collaborative note-taking on Etherpad:
https://tech.riscv.org/etherpad/p/2024-04-09_usc_sig_meeting_notes

Tech Chairs follow up

- Any remaining questions?
- (We'll dedicate a future meeting to fence.t)

Microarchitecture Security Guide

- Help implementers design more secure microarchitectures for RISC-V
- Informational/educational (non-normative) guide
- Focus on microarchitectural side-channel attacks and transient execution vulnerabilities
- Capture known best practices
- Highlight design areas and security concerns that need special attention
- Recommend tools for microarchitecture security verification (pre-silicon and post-silicon)

Discussion

- For implementers: What do you need from a microarchitecture security guide?
- For security experts: What topics should we cover in the guide?
- How frequently to meet?
- Anything you would like to discuss or hear more about in a future meeting?

Further Reading

Lukas Gerlach, Daniel Weber, Ruiyi Zhang, and Michael Schwarz
(2023) *A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs.*
In proceedings of 44th IEEE Symposium on Security and Privacy.
Link: https://publications.cispa.saarland/3924/