



# Security HC

12<sup>th</sup> October 2023

[Video link](#)

# Agenda

- Security model .....
  - Recovery plan – Paul to restart meetings, chase volunteers and form new timeline
- World guard TG proposal from SiFive - organisation, consensus
  - General consensus to split iopmp (non isa) and ISA parts.
  - Dean to work with IOPMP to ensure it has enough compatibility with world guard. Fast track a simple world ID ISA proposal via the privilege committee.(ideally include some reserved capability to allow use by potential future lightweight domain isolation mechanisms at m-mode)
  - Dean to confirm the above
- CHERI charter
  - Simon showed the proposed CHERI charter. Nick requested to add requirement to look at compatibility (fwd and bkwd) to the charter. ALL – please review the charter and comment.
  - Simon to socialise with greg and andrew (privilege committee) and get early comments.
- RVI Summit updates
  - ALL TG, SIG, please send summary of status and plans for summit.
- ZiCon conditional move
  - Awaiting new spec release, Markku indicated this solves the issue . Andy to approve once the spec update is announced, released and checked

# RVI Summit NA 2023 - Members day & Security track

Members day 6th Nov (Monday)

Morning session - 30 mins for security TGs

Afternoon session: 1pm onwards

- **1pm Crypto ext**
- **2pm Security HC - TG updates**  
- need 1 slide from all TGs
- **Priv, Unpriv ISA**
- **Priv SW**
- **ACT, SAIL**
- **SOC Infra, DC SIG**
- **Other updates**

<https://events.linuxfoundation.org/riscv-summit/program/schedule/>

Wednesday, November 8

11:30am PST

CPU Security in the Context of RISC-V - Sylvain Guilley, Secure-IC  
GRAND BALLROOM H

11:50am PST

Benchmarking RISC-V Post-Quantum - Markku-Juhani Saarinen, PQShield  
GRAND BALLROOM H

12:10pm PST

Towards Scalable Confidential Computing on RISC-V - Ravi Sahita, Rivos inc.  
GRAND BALLROOM H

1:55pm PST

The RISC-V Vector Cryptographic Extensions in the Real World - Ken Dockser, Tenstorrent  
GRAND BALLROOM H

2:15pm PST

Introduction to Project CHERIoT - Kunyan Liu, Microsoft  
GRAND BALLROOM H

2:35pm PST

Designing High-Performance RISC-V Core Resilient to Branch Prediction Timing Side Channels - Cyril Bresch, SiFive  
GRAND BALLROOM H

2:55pm PST

Recent Developments in Oreboot, a Pure-Rust Firmware and SBI Stack - Ronald Minnich, samsung  
GRAND BALLROOM H



# Thank You

