



# Security HC

26<sup>th</sup> October 2023

[Video link](#)

# Agenda

- RVI Summit / CCM security strategy and plan - updates
  - ALL TG, SIG, please send summary of status and plans for the CCM update next week, and the summit.
- World guard TG proposal from SiFive and Lightweight TEE - progress, organisation, consensus
  - Gurney progressing on starting the lightweight isolation TG. Andy D will assist as acting Vice chair if needed. Initial question to answer is world guard use cases and how it relates to lightweight isolation . i.e. is more than one world needed a m-mode. Then plan is to fast track the WG ISA aspects. IOMP is already looking at the non ISA checker side.
- Security model ..... Paul reports progress (great ! Thanks to the contributors). Please do make contributions edits etc. This is critical.
  - Platform security services workgroup – to define the server platform profile security requirements. Request contributions - please send email to volunteer
- Members Day discussion topics - please send mail. There are still slots at members day for TGs and SIG if required
- AOB
  - Smmtt call for candidates - deadline Nov 3<sup>rd</sup>
  - High Assurance Crypto TG call for candidates – deadline Nov 7th
  - CHERI Charter, TG formation – Simon to request slot at chairs meeting to begin discussion and help understanding (and contact priv, unpriv chairs)

# 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

