
RISC-V®
Security HC Meeting
March 16th, 2023

Agenda

- Call for Chair of Trusted Computing SIG, as Suresh has switched to individual member.
- Presentation from Samuel Ortiz (Rivos) on AP-TEE-IO TG proposal
- M-Mode Isolation TG
- Face to Face
- Updates from TGs + SIG

RISC-V

Confidential Computing SIG

- Thankyou to Suresh for his work over the past year (and more)
- Unfortunately due to position change, and individual membership, we need a new Chair.

- SIG charter can be found at https://github.com/riscv-admin/trusted-computing
- Mark confirmed that it is allowed to chair up to three committees
- Proposal is for Suresh and Ravi to switch roles provided –
  - Suresh agrees
  - No one else wishes to come forward to chair the committee.
    - Email before end of the week please if you wish to put yourself forward.

RISC-V

AppTEE-IO

- Proposal for new TG
- Presentation from Samuel Ortiz (Rivos)

- Thanks to Samuel for his presentation.
- This will be made available and the link put on the security mailing list

RISC-V

M-Mode Isolation TG

- https://github.com/riscv-admin/m-mode-isolation/blob/main/CHARTER.md

- Please all review the m-mode isolation TG charter.
- This is in the early stages of set up
- Priv IC will announce, then once running, first job is to close on the charter
- Nick suggested that we add to the charter the fact there are already multiple(at least two) hardware based m-mode isolation custom extensions already implemented, so we should standardise to reduce fragmentation.

RISC-V

F2F, End of April

- Why
- When
- Where
- Ravi to send agenda proposal
- This is requested by the board to make progress quickly with the higher bandwidth of f2f.
- Concerns raised about cost of attendance and short notice.
- Request made to allow on line listening to avoid painful resynchronisation with non attended.
- Propose twice daily (or more?) inclusion of written concerns, contributions etc from on line participants