



Security HC meeting

August 4th, 2022

Only RISC-V Members May Attend

- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. [Joint working groups](#) (JWG) agree that any IP discussed or worked on is fully open source and unencumbered as per the policy.
- It is easy to become a member. Check out riscv.org/membership
- If you need work done between non-members or other orgs and RISC-V, please use a joint working group (JWG).
 - used to allow non-members in SIGs but the SIGs purpose has changed.
- Please put your name and company (in parens after your name) as your zoom name. If you are an individual member just use the word "individual" instead of company name.
- Non-member guests may present to the group but should only stay for the presentation. Guests should leave for any follow on discussions.



Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: <https://riscv.org/regulations/>

If you have questions about these matters, please contact your company counsel.



Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

<https://riscv.org/community/community-code-of-conduct/>



Conventions



- Unless it is a scheduled agenda topic, we don't solve problems or detailed topics in most meetings unless specified in the agenda because we don't often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unilaterally. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, ...
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Risc-V Security



Agenda

- Summit Tutorials reminder
- Krste email on memory security incl. SMPU (suggests rename to SPMP), IOPMP, etc
- AP-TEE status update
- Any Updates from TGs + SIG



- Summit Security tutorial: 90 min, topics are CFI and microarchitectural side channels. Ved and Allison are signed up as presenters.
- TG creation requests for IOPMP, SMPU, Security Model, and Shadow Stack & Landing Pads are in front of TSC for approval vote.
 - Active reflector traffic around proposed name change for SMPU. Andy to take the discussion off-line.
 - Discussion in TSC about Security Model: is it a non-ISA spec, white paper, or something else (called Architecture Overview for now). Manuel to work on an initial proposal for Architecture Overview. It may take a little longer for formal approval of Security Model TG given the discussion on Architecture Overview. Meanwhile, TG work on Security Model should continue.
- AP-TEE TG status: still need to interview one more chair candidate. Vacation and scheduling conflicts have delayed this final interview. Candidate expected to be back in office this week.
- No other SIG or TG updates.

Any Other Status Updates



Open Action Items

Running list of open AI's