
RISC-V®
Security HC meeting
Nov 18th, 2021

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 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.

RISC-V

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.

RISC-V®

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

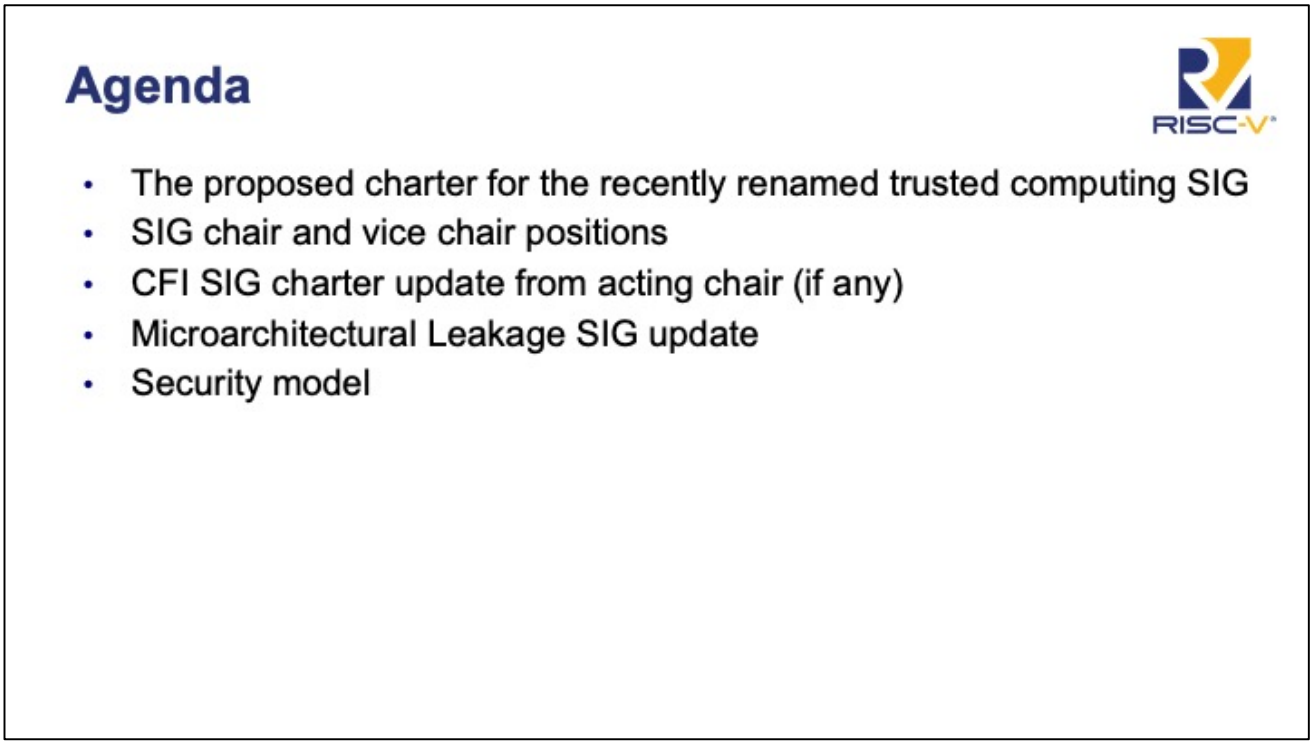
We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

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

RISC-V®

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 unillaterly. 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



- Charter approved (see next slide)
- SIG chairs process
    - Candidate qualifications for open SIG chair and vice chair are assessed by Security HC chair and vice chair (Andy and Manuel)
    - If number of qualified candidates equals number of open positions, then Security HC chair and vice chair will appoint candidates to the open positions.
    - Issue is the case in which number of qualified candidates is greater than number of open positions
        - Group voted on how to select chair and vice chair for SiGs in case there are more candidates than openings (with one vote per company)
            - Option A: Security HC chair and vice chair appoint candidates – received 10 votes
            - Option B: Security HC will select candidates via voting process – received 3 votes
            - Andy and Manuel abstained from vote.
            - Option A carried the vote.
- Decided not to update CFI SIG; good enough for now.
- Will use existing TEE TG meeting slot for SIG discussions as they come up; meeting to be renamed to Security Topics
- Security model: help needed; we don't want to be too prescriptive; need to agree on outline and set expectations about the objectives of the model.

RISC-V Security

RISC-V®

Proposed Trusted Computing SiG Charter

There is a growing need for a zero trust architecture in HW, where a SW application can both examine and attest the environment it is running in, and have guarantees that it is isolated from other, untrusted software. The Trusted Computing SIG will examine the state of the art for hardware-assisted technologies such as Confidential Computing, Remote Attestation, Confidential VM, Hardware TEE, Enclaves, etc., on an ongoing basis, and define the trusted computing strategy for risc-v. It will develop TG Charters as required, that will define the required written documentation, threat models, executable model, prototype implementations including SW PoCs, toolchain support, and compliance suite for RISC-V trusted execution recommendations and extensions.

RISC-V

- No objections to Proposed SIG charter; charter proposal adopted.
- Need to fill vice chair position for this SIG


RISC-V®
Open Action Items

Running list of open AI's

- Identify work ready for charter creation (owner: Andy/Manuel)
  - Ongoing
- What is the Informative/white papers document release process? (owner: Manuel)
  - Request by Blockchain SIG
- Need to define min. Security Targets to integrate into overall spec approval process (owner: TBD)
- Whitepaper on existing RISC-V security mitigations against certain known attacks (owner: Don)
- Rename TEE TG meeting to Security Topics (owner: Nick)
- Call for Trusted Computing SIG vice chair (owner: Andy)

RISC-V