Notes from Oct 28, 2021 meeting

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.

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

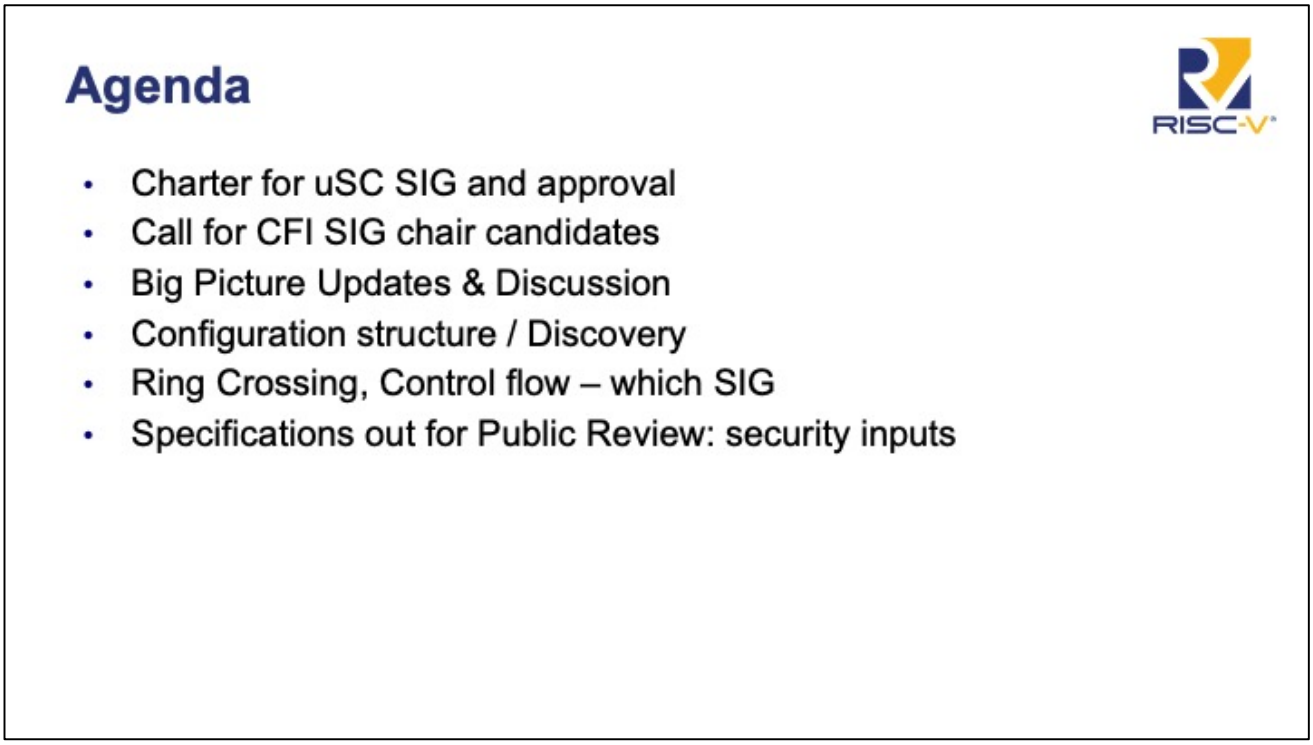
We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

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



- uSC charter approved, SIG creation to move forward
- CFI SIG: formal announcement for Chair Candidates went for CFI SIG out on Oct 26, 2021. Candidates that want to apply should do so within the 2 weeks window.
- Configuration Structure / Discovery: Don volunteered to engage with group defining the Config Structure to ensure security is considered/included.
- Ring Crossing, Control flow: group agreed to move to uSC SIG.
- Big Picture - Security Model:
    - Everyone invited to participate / help with creation of document (located here: https://docs.google.com/document/d/1TRHhsGiB5W4K8M7I4e-f40mOPErTb9sv/edit?usp=sharing&ouid=112955615784799508942&rtpof=true&sd=true)
    - Need a Whitepaper to explain how current RISC-V capabilities prevent some of the well-known attacks (AI)
- Please inform Andy or Manuel which RISC-V specs out for public review you have looked at from a security angle.

RISC-V Security

RISC-V®

uSC SIG

- Proposed charter

The microarchitecture may be vulnerable to information leakage, notably through resource sharing. Via side-channel leakage where the victim application, by modifying any state in the processor, may expose secret information when the attacker can observe state changes. Or via covert-channel leakage where the attacker tries to actively exfiltrate information.

The Microarchitectural Side Channels (uSC) SIG will analyse the literature, identify current gaps, propose and develop the RISC-V strategy to prevent microarchitectural information leakage, with an initial focus on timing side channels. Solutions of interest include microarchitectural purges, microstructure tagging, leakage resilient functionalities, preventing read-only architectural leakage (e.g. performance counters).

The SIG will discuss and propose recommendations on how to evolve the compliance model to include extensions with no functional side effects.

The SIG will develop one or more TG Charters that define one or more of the following items: written documentation, threat models, prototype implementations, toolchain support, and compliance suite for a RISC-V side channel leakage extension(s) or specification(s).

- Proposed to add “on ongoing basis” to stress the lengthy ongoing nature of the SIG
- Acting chairs are Ronan and Gernot
- No objections to adoption of charter with added wording (see next page)

Microarchitectural Side Channel SIG

- Proposed charter (updated after the meeting)

  The microarchitecture may be vulnerable to information leakage, notably through resource sharing. Via side-channel leakage where the victim application, by modifying any state in the processor, may expose secret information when the attacker can observe state changes. Or via covert-channel leakage where the attacker tries to actively exfiltrate information.

  The Microarchitectural Side Channels (uSC) SIG will analyse – on an ongoing basis - the literature, propose and develop the RISC-V strategy to prevent microarchitectural information leakage, with an initial focus on timing side channels. Solutions of interest include microarchitectural purges, microstructure tagging, leakage resilient functionalities, preventing read-only architectural leakage (e.g., performance counters).

  The SIG will discuss and propose recommendations on how to evolve the compliance model to include extensions with no functional side effects.

  The SIG will develop one or more TG Charters that define one or more of the following items: written documentation, threat models, prototype implementations, toolchain support, and compliance suite for a RISC-V side channel leakage extension(s) or specification(s).

- Added text in Red
- This text was approved by the group

Open Action Items

RISC-V®

Running list of open AI's

- Andy/Manuel to identify work ready for charter creation
  - Ongoing
- Andy/Manuel work with Patty and Joe on document release process
- Need to define min. Security Targets to integrate into overall spec approval process
- Don: start whitepaper on existing RISC-V security mitigations against certain known attacks.

RISC-V