
RISC-V®
Security HC meeting
Oct 14th, 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

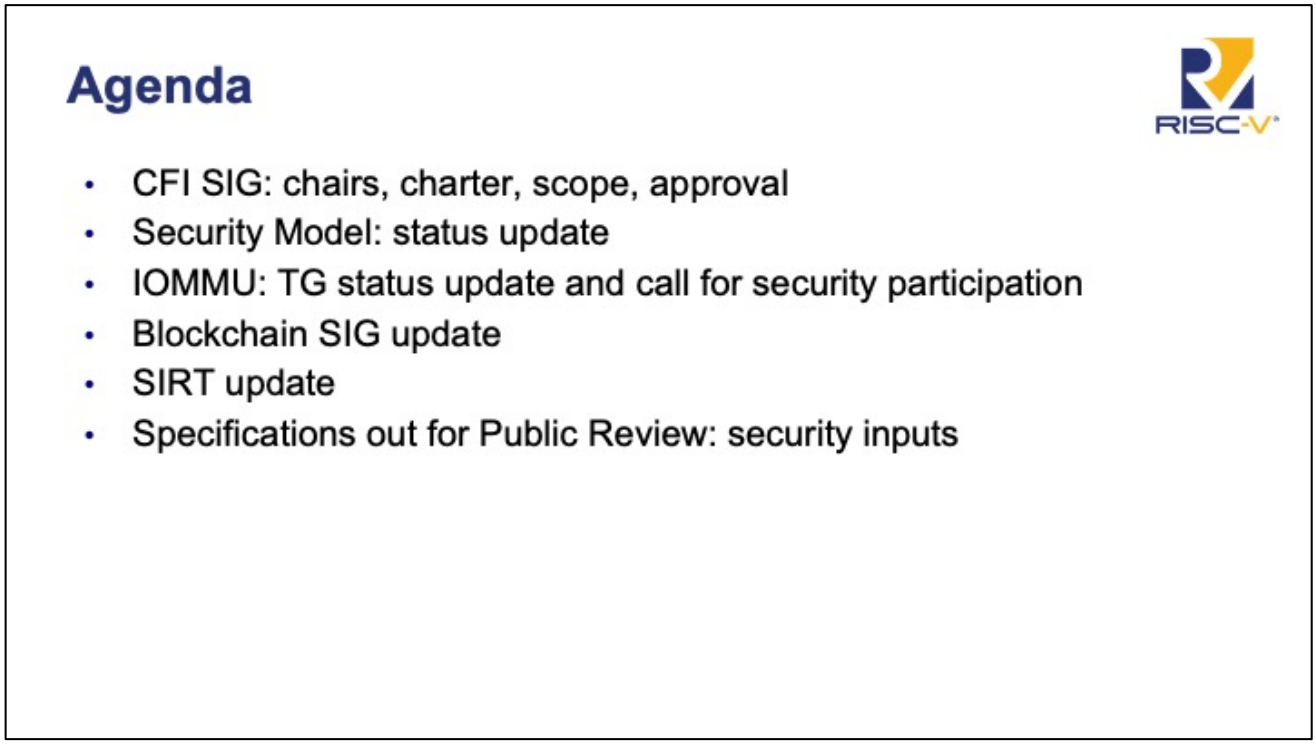
We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

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



- Still Need help reviewing all specifications out for Public Review, see https://wiki.riscv.org/display/TECH/ISA+Extensions+On+Deck+-+Ready+for+Ratification+Milestone

- CFI SIG: see next slide

- Security Status: met with Confidential Compute Consortium; expect follow-ups.

- IOMMU: per last Chairs meeting, charter creation under leadership of Software HC (IOMMU TG will highly likely move under SOC Infrastructure once officially in place).

- Blockchain SIG: Call for help with gap analysis. Developer focused document is in draft stage; need to determine how to officially release as a RISC-V publication.

AI: Andy/Manuel work with Patty and Joe on document release process

- SIRT: Public facing Security page on riscv.org almost done. HackerOne relationship in-place. Don and Alister to circle back to all technical groups within RISC-V for process integration.

Risc-V Security

RISC-V®

CFI SIG

- Proposed charter wording
  - Advanced exploitation techniques based on code reuse, commonly known as Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP), do not introduce new code in vulnerable programs. Code reuse attacks are based on diverting the control flow of an application by, amongst other things, overwriting function pointers (JOP) and return addresses (ROP). The CFI SIG will analyze the state of the art and develop the risc-V strategy to mitigate or prevent CFI attacks. It will select the preferred potential solutions including ISA extensions that can be used by privileged and unprivileged programs to protect the integrity of their control-flow. The SIG will develop a CFI TG Charter that will define the required written documentation, threat models, executable model, prototype implementations including SW PoCs , toolchain support, and compliance suite for a RISC-V CFI extension.

- George to forward summary of past CFI discussions within TEE TG.
- Suggested to remove references of ROP and JOP from charter (too specific)
- Suggested to include broader language such as “by overwriting critical flow variables” and “prevent code reuse attacks”
- Charter to be updated with suggested changes (see below)
- George and Vlad are acting Chair and Vice Chair.
- Group agreed to continue with next steps in creation of CFI SIG.
- Next steps: update charter and send out formal request for chair and vice-chair candidates.

- Final text - Advanced exploitation techniques based on code reuse, do not introduce new code in vulnerable programs. Code reuse attacks are based on diverting the control flow of an application by overwriting critical flow control variables. The CFI SIG will analyze the state of the art and develop the RISC-V strategy to mitigate or prevent code re-use attacks. It will select the preferred potential solutions including ISA extensions that can be used by privileged and unprivileged programs to protect the integrity of their control-flow. The SIG will develop a CFI TG Charter that will define the required written documentation, threat models, executable model, prototype implementations including SW PoCs , toolchain support, and compliance suite for a RISC-V CFI extension.


RISC-V®
Open Action Items

Running list of open AI's

- Andy/Manuel to identify work ready for charter creation
  - CFI -> create SIG
- Andy/Manuel work with Patty and Joe on document release process

RISC-V