
RISC-V®
Security HC meeting
Feb 17, 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 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

Risc-V Security

Agenda

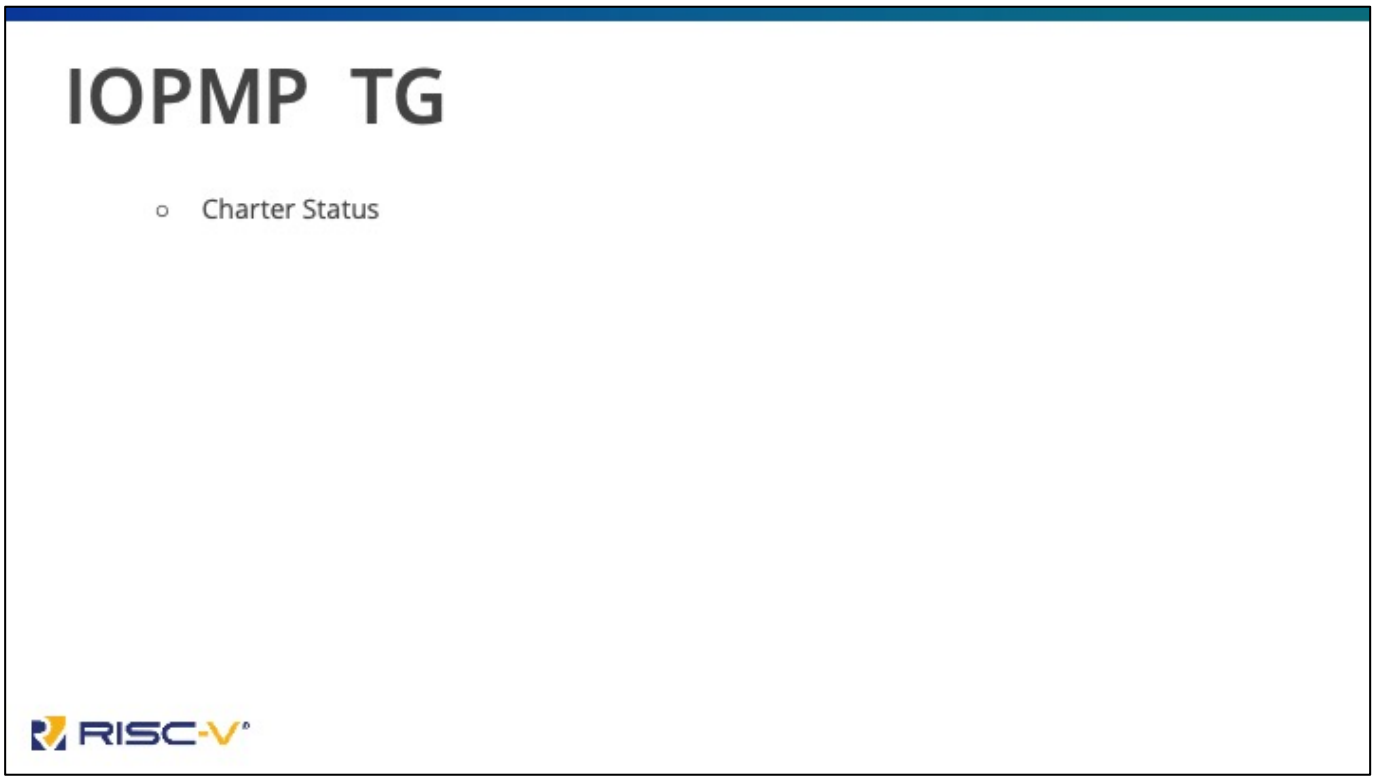
- IOPMP TG - charter status & updates
- TSC Slides
- Security Model – TG, chair/vice chair, status, next steps
- GOST-R TG next steps

RISC-V

Both topics:

- Security Model – TG, chair/vice chair, status, next steps
- GOST-R TG next steps

must move to next meeting; unable to discuss during this meeting due to lack of time



Discussed notes taken during TEE TG meeting on IOPMP charter scope.

IOPMP expectation:

- Blacklist policy -> we add what we want to protect, not what we want to allow
- Static partitioning
- Array of registers
- Finite set of rules
- No memory translation
- Initialize it during boot
- Locked rules
- Priority matching
- Simple implementation
- Recommend / standardize who is responsible for programming it, define TBD

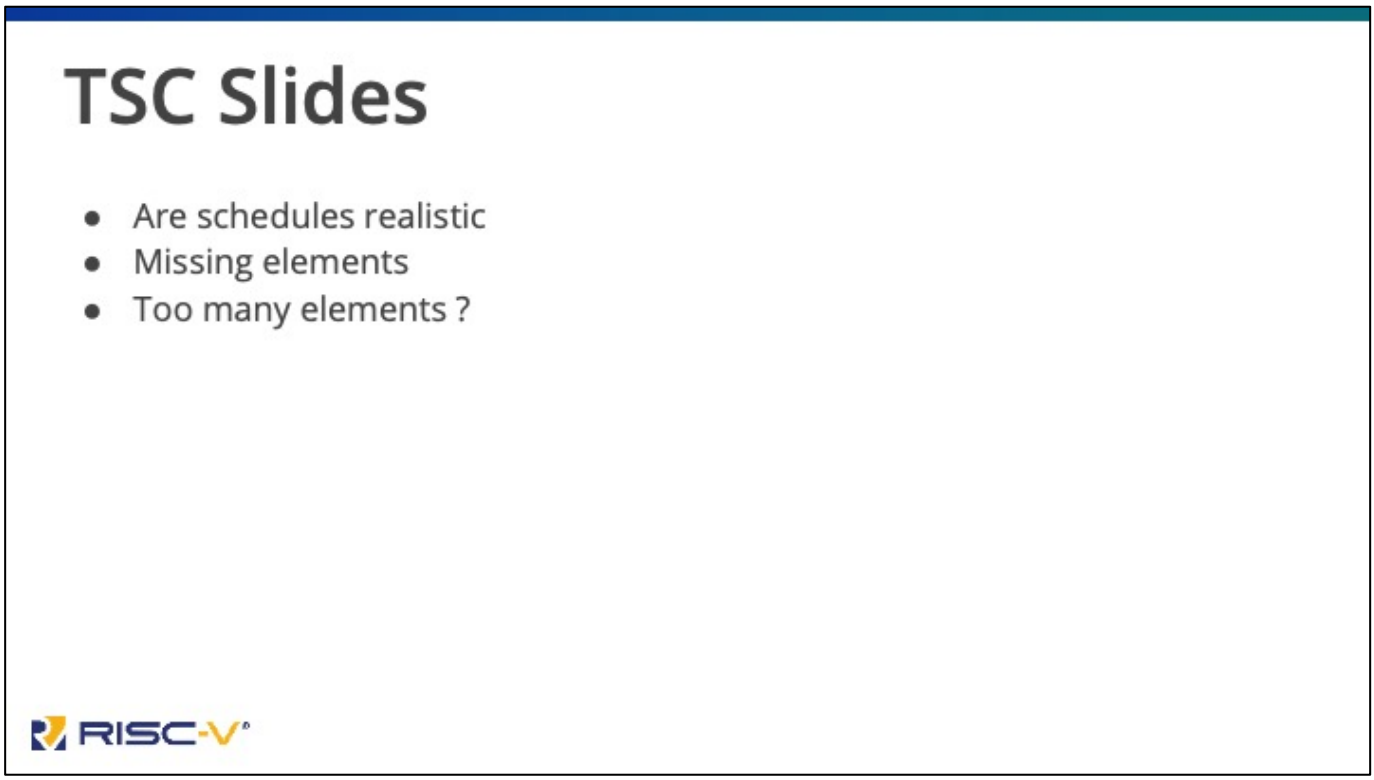
IOMMU expectations:

- Whitelist policy -> we add what we want to allow, if there is not a
- mapping, deny access
- Or passthrough / disabled
- Dynamic allocations
- Page tables
- Infinite set of rules
- Memory translation
- Complex implementation
- Recommend / standardize who is responsible for programming it, define TBD

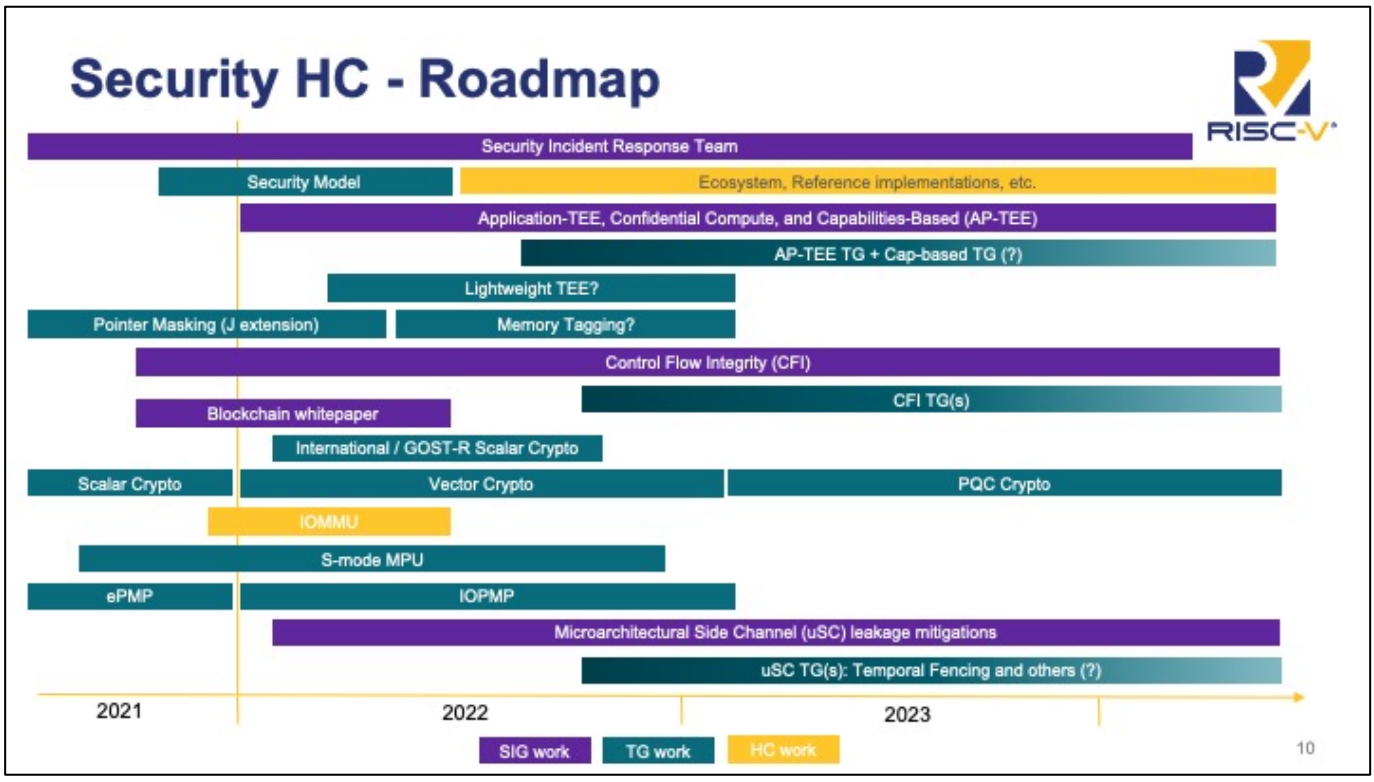
- Can be used as an IOMPU if using physical addresses on the page tables
- Supports only first stage, only second stage, nested or no translation modes -> It can also cover embedded cases

No conflict / dependencies between what's in the hart (PMP/ePMP/MMU/MPU) and IOMMU/IOPMP

- Paul to update IOPMP draft charter.



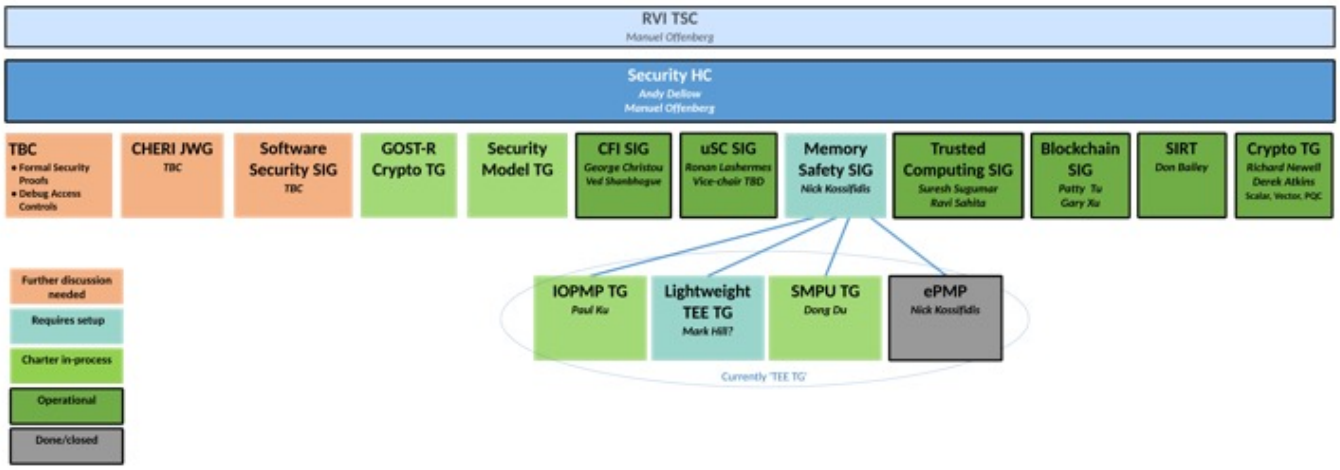
- All feedback to be incorporated into next revision of the TSC slides



Slide needs updates:

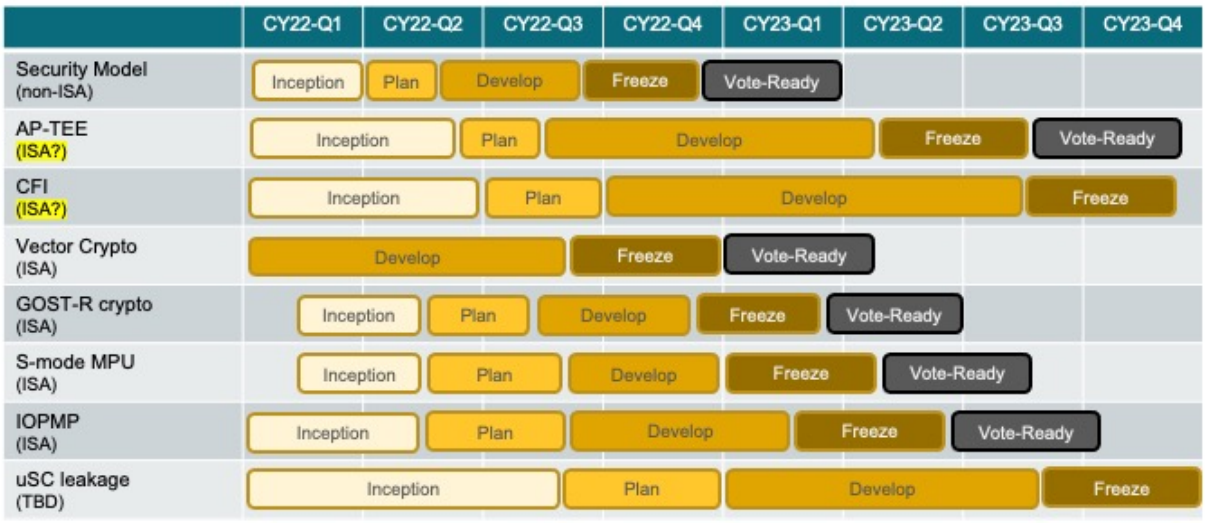
- Need to add Memory Safety SIG
- Once sMPU and IOPMP TG are up-and-running TEE TG stops to exist and will become Memory Safety SIG
- Change Lightweight TEE to “M-mode Isolation”: multiple real-world use cases identified; need for spec/TG still TBD

Security HC - Organization



Planned Specifications

TBD:
- Lightweight TEE
- Memory Tagging



- Multiple updates to spec timelines
- AP-TEE may need to become ISA + non-SA (or Hybrid Spec)
- uSC will likely be ISA
- IOPMP is non-ISA
- CFI is ISA


RISC-V®
Open Action Items

Running list of open AI's

RISC-V®