RISC-V®

Security HC meeting

Sept 30th, 2021

Only RISC-V Members May Attend

- Non-members are asked to please leave.
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection
- 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.

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 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

Agenda

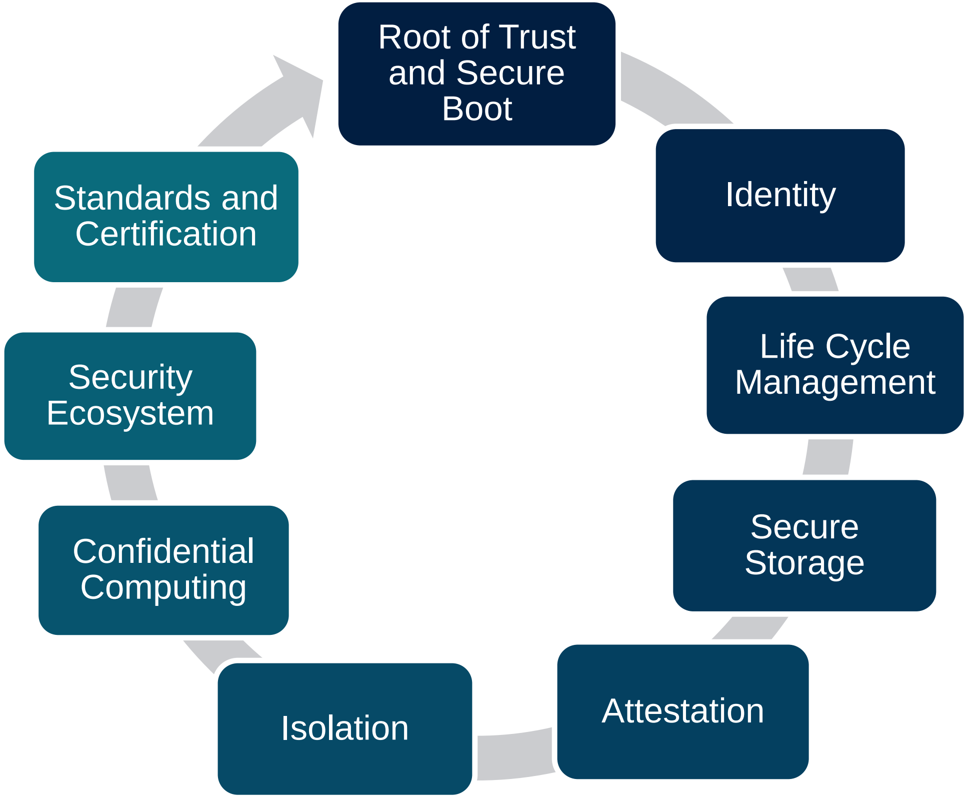
- Specifications out for Public Review
- RISC-V Security Big-Picture discussion
- Proposed organization structure
- Charters

Risc-V Security

Intrinsic Security

Zero Trust Model

- Security as a basic feature of HW, SW Firmware
- Support security through entire lifecycle
- Guidelines matched to profiles



Root of Trust and Secure Boot

Identity

Life Cycle Management

Secure Storage

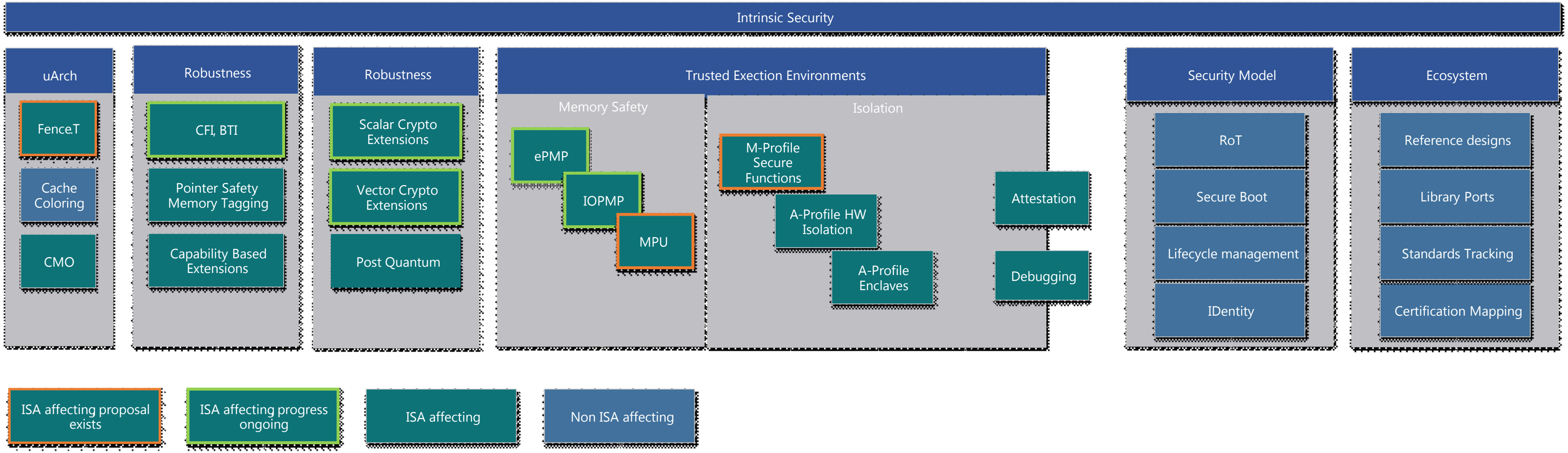
Attestation

Isolation

Confidential Computing

Security Ecosystem

Standards and Certification



Intrinsic Security

uArch
- Fence.T
- Cache Coloring
- CMO

Robustness
- CFI, BTI
- Pointer Safety Memory Tagging
- Capability Based Extensions

Robustness
- Scalar Crypto Extensions
- Vector Crypto Extensions
- Post Quantum

Trusted Exection Environments

Memory Safety
- ePMP
- IOPMP
- MPU

Isolation
- M-Profile Secure Functions
- A-Profile HW Isolation
- A-Profile Enclaves
- Attestation
- Debugging

Security Model
- RoT
- Secure Boot
- Lifecycle management
- IDentity

Ecosystem
- Reference designs
- Library Ports
- Standards Tracking
- Certification Mapping

ISA affecting proposal exists

ISA affecting progress ongoing

ISA affecting

Non ISA affecting

Security Model

- State Goals of Security and Rationale
- Abstracted from implementation specifics
- Platform specifications can reference appropriate sections
    - By Profile, By Vertical
- Reuse Existing standards when appropriate

Security Model

Secure Boot

- Immutable Root of Trust
- Secure Boot Chain
- Mutable Root of Trust
- Attestation through every stage
- Temporal Isolation
- *Certificate Format*
- *Binary Format*
- ....

LifeCycle Management

- Development and Debug
- Provisioning
- IDentity
- Update
- Anti Roll back
- Decommisioning

- Intention is to reference from Platform Specifications
    - Shall - Should - May in platform spec
    - Security Model itself is Non-ISA affecting

Trusted Execution

- Memory Safety
  - PMP based TEEs
- Hardware based Isolation
  - M-Class secure functions
  - A-Class Maintaining privilege levels in TEE
- Confidential Compute
  - Mutually untrusted applications
  - Isolated Application Enclaves
  - Encrypted Enclaves
- Attestation of entire software chain from initial boot
- Security aware Debugging

Maybe ISA affecting / **ISA Affecting**

Robustness

- Control Flow Integrity
  - BTI, PAC etc
- Side Channel Leakage Protection
  - ISA extensions to control uArch ?
    - Fence.t
- Capability Based
  - CHERI JWG
  - Alternatives ?

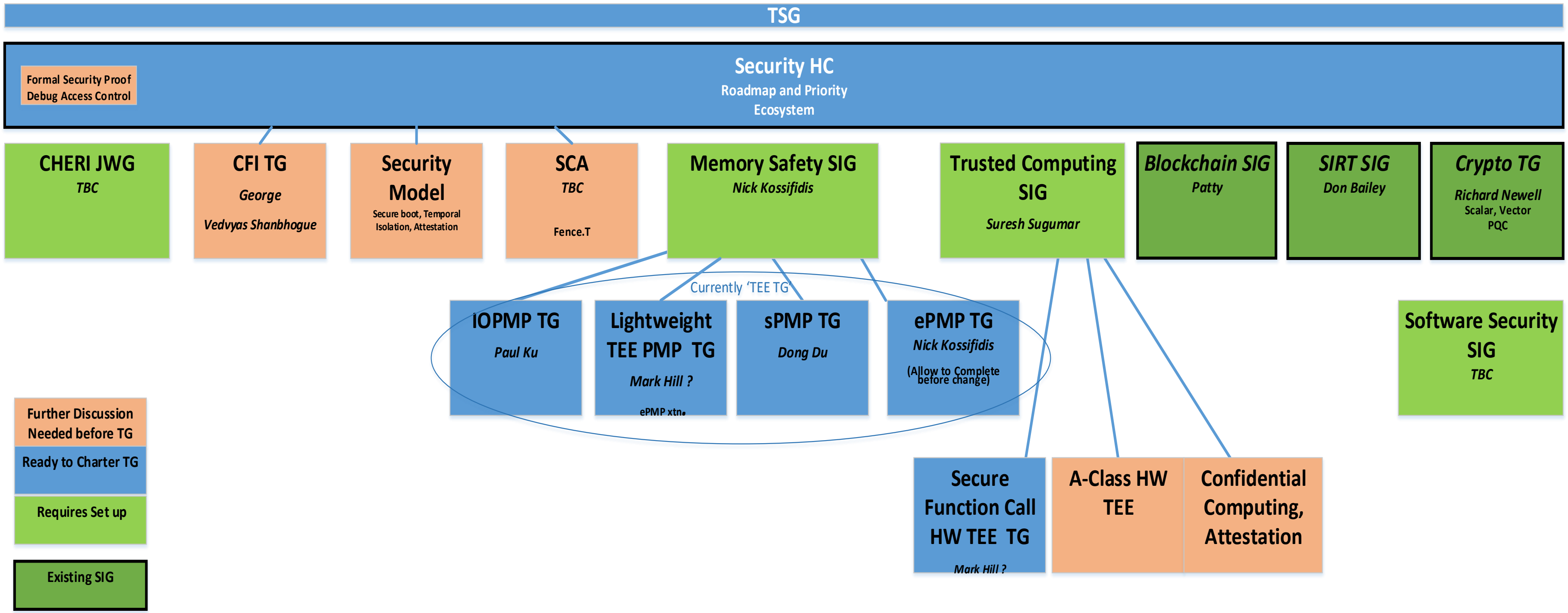
Security Ecosystem

- Security Services
  - Reference implementations
    - Secure Boot
    - Attestation
    - …
  - Optimised library ports
    - OpenSSL
    - mbed Crypto
  - OS ports
  - APIs

- Standards and Certification
  - Formal Security Proofs
  - Certification mapping

- Verticals
  - Any Specific requirements ?

Proposed Reorganisation of Security in Risc-V



TSG

Security HC
Roadmap and Priority
Ecosystem

Formal Security Proof
Debug Access Control

CHERI JWG
TBC

CFI TG
George
Vedvyas Shanbhogue

Security Model
Secure boot, Temporal Isolation, Attestation

SCA
TBC
Fence.T

Memory Safety SIG
Nick Kossifidis

Trusted Computing SIG
Suresh Sugumar

Blockchain SIG
Patty

SIRT SIG
Don Bailey

Crypto TG
Richard Newell
Scalar, Vector
PQC

Currently 'TEE TG'

IOPMP TG
Paul Ku

Lightweight TEE PMP TG
Mark Hill ?
ePMP xtn.

sPMP TG
Dong Du

ePMP TG
Nick Kossifidis
(Allow to Complete before change)

Software Security SIG
TBC

Secure Function Call HW TEE TG
Mark Hill ?

A-Class HW TEE

Confidential Computing, Attestation

🟧 Further Discussion Needed before TG

🟦 Ready to Charter TG

🟩 Requires Set up

🟩 Existing SIG

Proposed Reorganisation of Security in Risc-V

- Start *Security Model* team under HC to create high level recommendations around RoT, secure boot, attestation chain, temporal isolation, updateability, identity, and the rationale.
- Move most of the Current TEE TG work to a new SIG ‘Memory Safety SIG’ -
  - Meetings structure unchanged, chair remains Nick
  - Create individual TGs for each task with specific charter
- Refocus the Security Tech SIG
  - Suresh remains chair
  - Trusted Execution and Confidential Computing
  - Initial work is to define the requirements, aim to charter TG(s)
- Create Joint Working Group (JWG) for CHERI discussion
- CFI ready to charter TG
- Restart SCA discussion on fence.T and other proposals
- Also need focus on Security SW and Ecosystem – any volunteers ?

Open Action Items

Running list of open AI’s

- Manuel/Andy confirm that Discovery is actively worked
- Suresh to find candidate to lead Side-Channel activities
- Andy/Manuel to identify work ready for charter creation