Risc-V Security

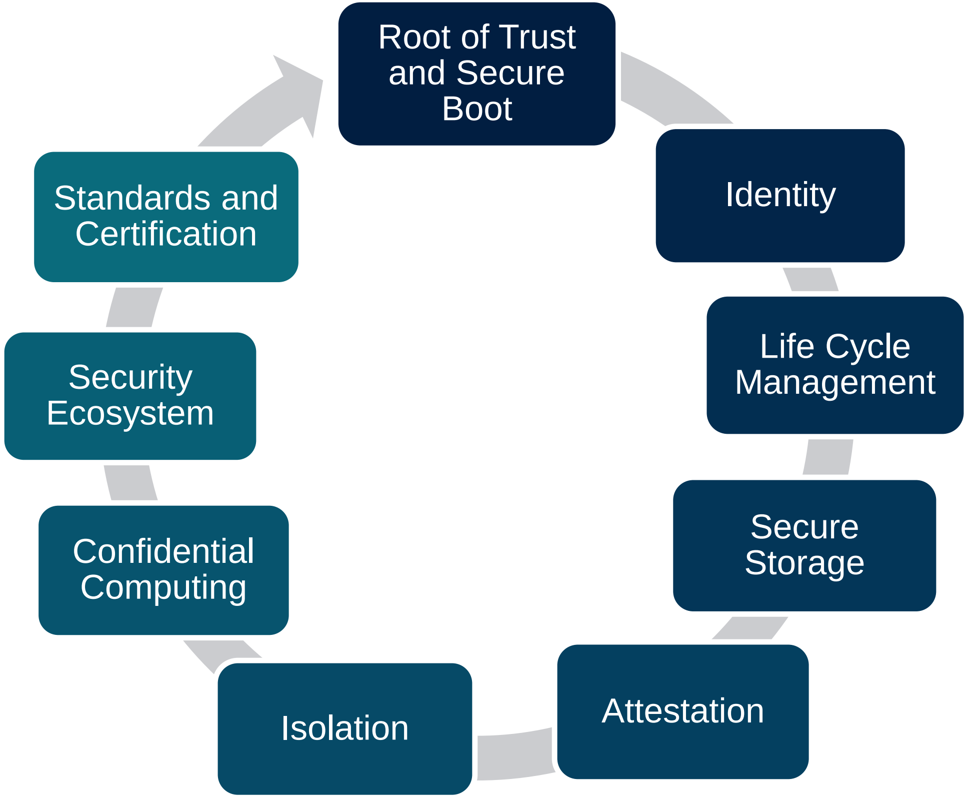
Oct 2021

RISC-V®

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

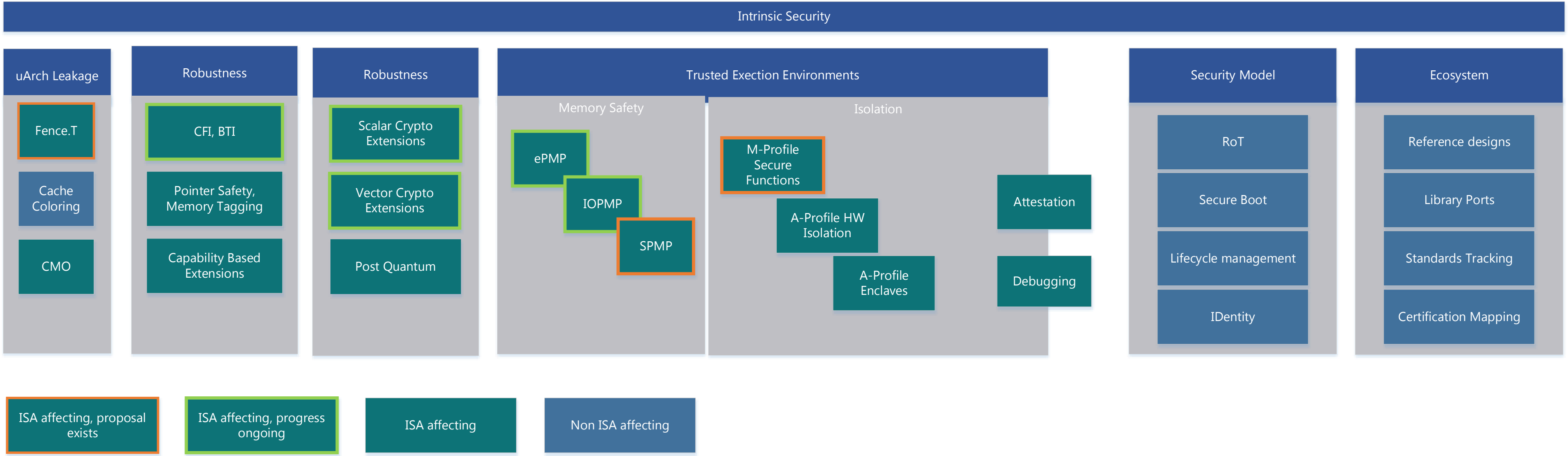
Attestation

Isolation

Confidential Computing

Security Ecosystem

Standards and Certification



Intrinsic Security

uArch Leakage

- 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
- SPMP

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

RISC-V®

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

Robustness

- Control Flow Integrity
  - BTI, PAC etc

- Side Channel Leakage Protection
  - ISA extensions to control uArch ?
    - Fence.t

- Capability Based
  - CHERI JWG
  - Alternatives ?

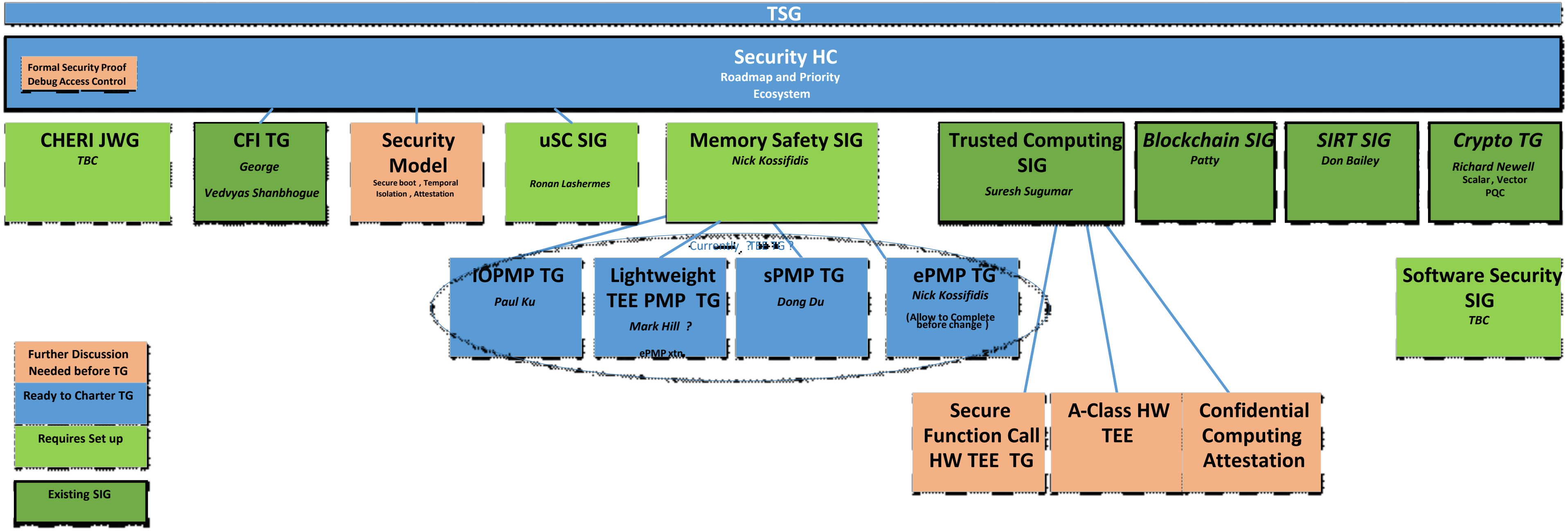
Security Ecosystem

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

- Standards and Certification
  - Formal Security Proofs
  - Certification mapping

- Verticals
  - Any Specific requirements ?

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

uSC SIG
Ronan Lashermes

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

A-Class HW TEE

Confidential Computing Attestation

Further Discussion Needed before TG

Ready to Charter TG

Requires Set up

Existing SIG

Ongoing 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
- Refocused 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 SIG set up
- Uarch Leakage SIG charter for approval
- Still need focus on Security SW and Ecosystem – any volunteers ?