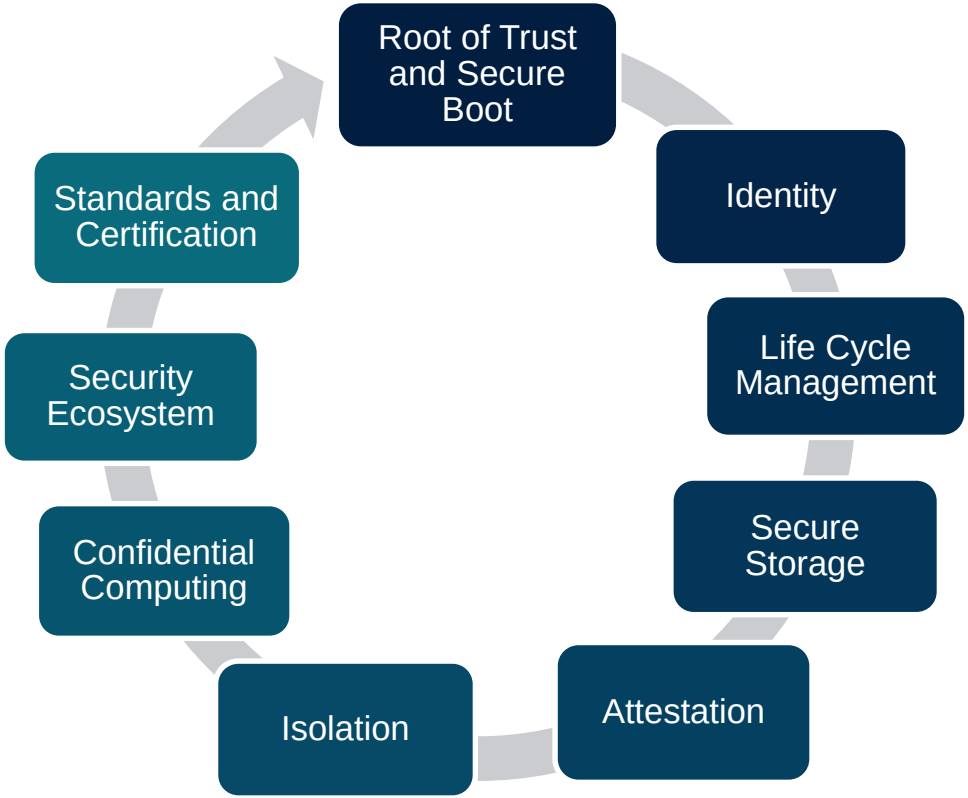
Securing the Future of Open Source Computing

TASER'22 Sept 2022

Andrew Dellow - Huawei UK

Intrinsic Security

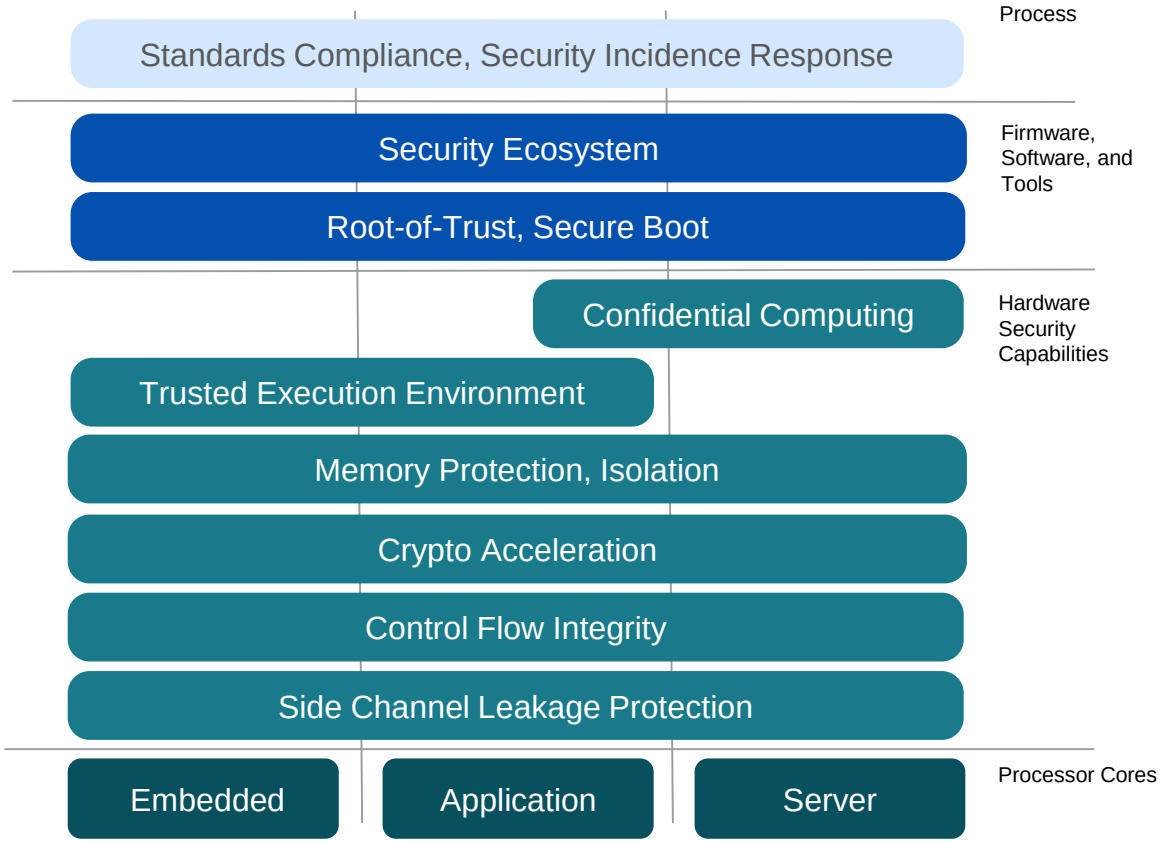
- Security as a basic feature of HW, SW Firmware
- Support security through entire lifecycle
- Published Guidelines matched to usage profiles



RISC-V Security Rationale

- Clean-slate architecture invites new hardware security solutions
- Open security model accelerates hardware security innovation
- Opportunity to incorporate security industry learnings & best practices
- Open governance facilitates collaboration on best security approach
- Royalty free model enables new open-source hardware security solutions

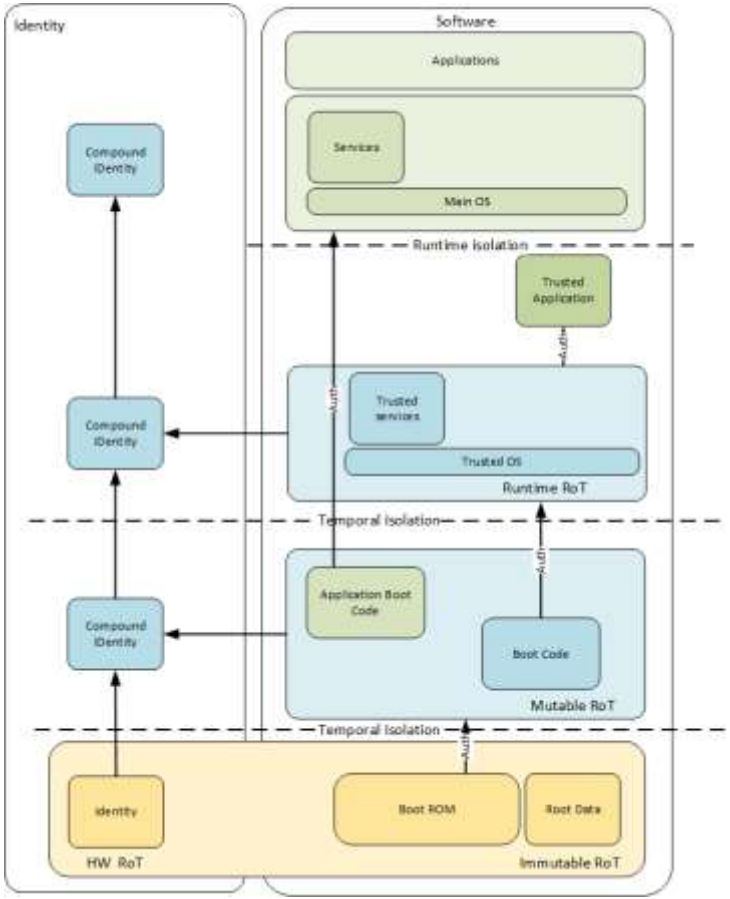
Security Scope



Security Model

- State Goals & Rationale for RISC-V Security
- Defines Scope
- Defines Threat Model
- Derives Security Requirements

- Task Group under consideration



Generic Device Model

Security Ecosystem

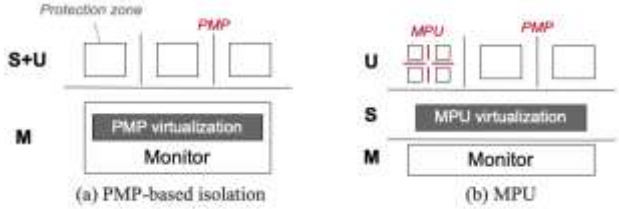
- Enablement of RISC-V security services & software
- Identify and list key open-source security software and libraries
- Develop RISC-V security reference implementation(s)
- Identify, monitor, and influence applicable standards
- Identify and liaison with applicable Security Certification entities

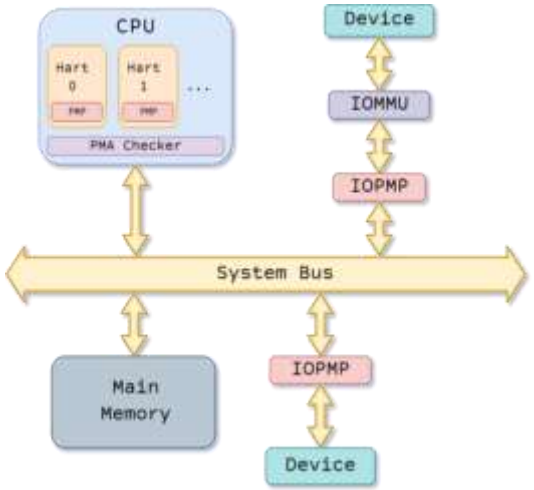
Memory Safety

- PMP
  - Basic isolation between M-mode and S/U-modes.
- ePMP
  - Enhanced PMP for increased executable protection, additional use cases
- Virtual Memory
  - Isolation between S and U mode
  - Guest-Guest Isolation (VS-VS)
  - Host –Guest Isolation (HS-VS)

under development, task groups active:

- sPMP
  - An S-mode PMP, sometimes called MPU
- IOPMP
  - System Level PMP
  - Protects memory from other masters





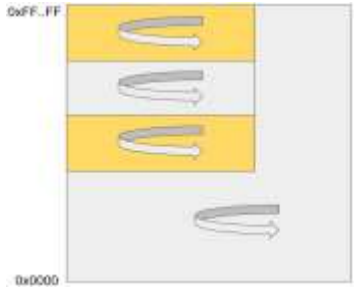
Robustness

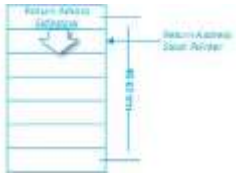
- Pointer Masking
  - actual_address = (requested_address & ~mpmmask) | mpmbase
  - Software based memory tagging
  - Memory bounding

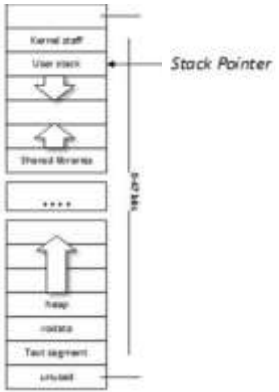
- Control Flow Integrity
  - Shadow Stack
  - Labelled Landing Pad

Active TG :

- MicroArchitectural Side Channel Leakage
  - An anomaly for an ISA standard
  - Speculation Barriers – fence.t







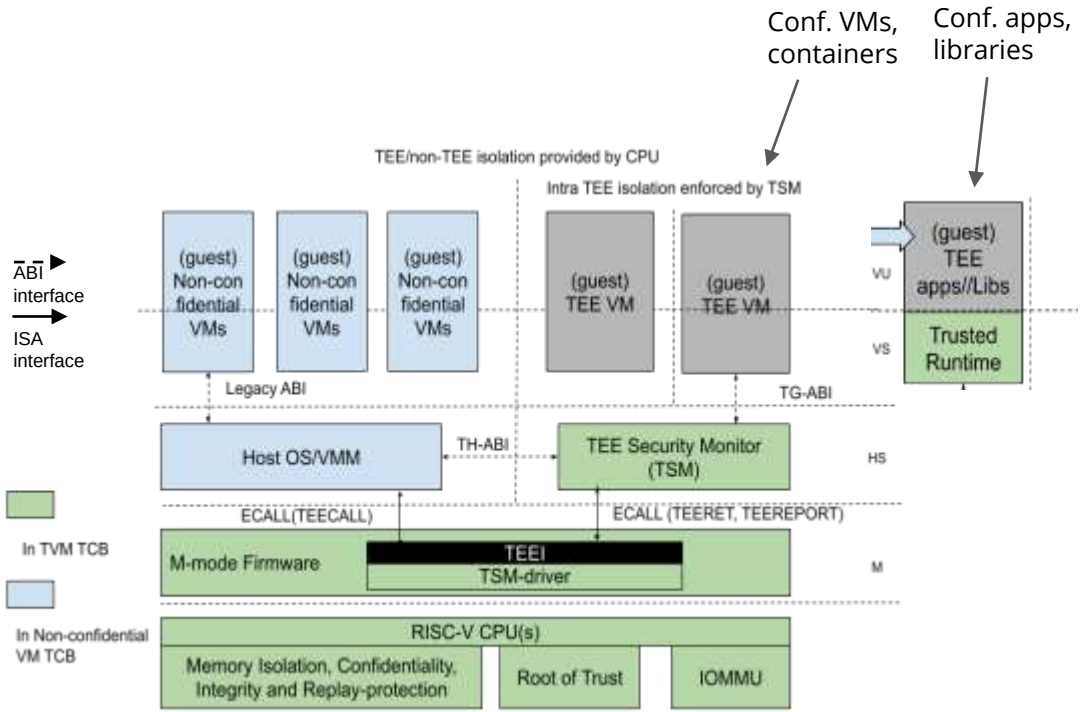
Cryptography

- Scalar Extension Ratified
- Vector Extension – 2022
- Post Quantum – under discussion

Trusted Computing

Active AP-TEE TG:

- Trusted Execution Environment for application class and above
- AP TEE ABI to allow support on current ratified ISA
- ISA Extensions to improve performance, shrink TCB, allow attestation, improve security

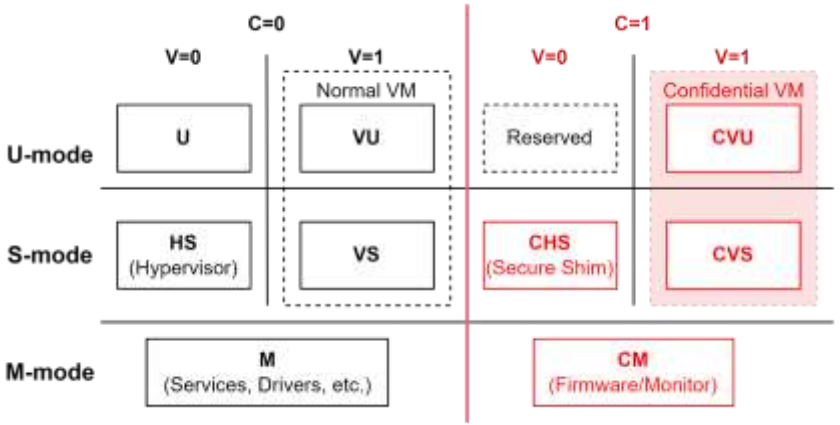


Maybe ISA affecting / **ISA Affecting**

Trusted Computing (2)

Active AP-TEE TG :

- Extend APP TEE to include Confidential Computing
- Isolated, attestable TCB
- Support for Confidential VMs



Trusted Computing (3)

IoT-TEE TG under consideration:

- Lightweight TEE for constrained devices and MCUs
- Isolated, attestable TCB
- Additional M-Mode context ? Other ?
- Trusted functions
- Lower PPA costs than ePMP ?

Capability Based Security

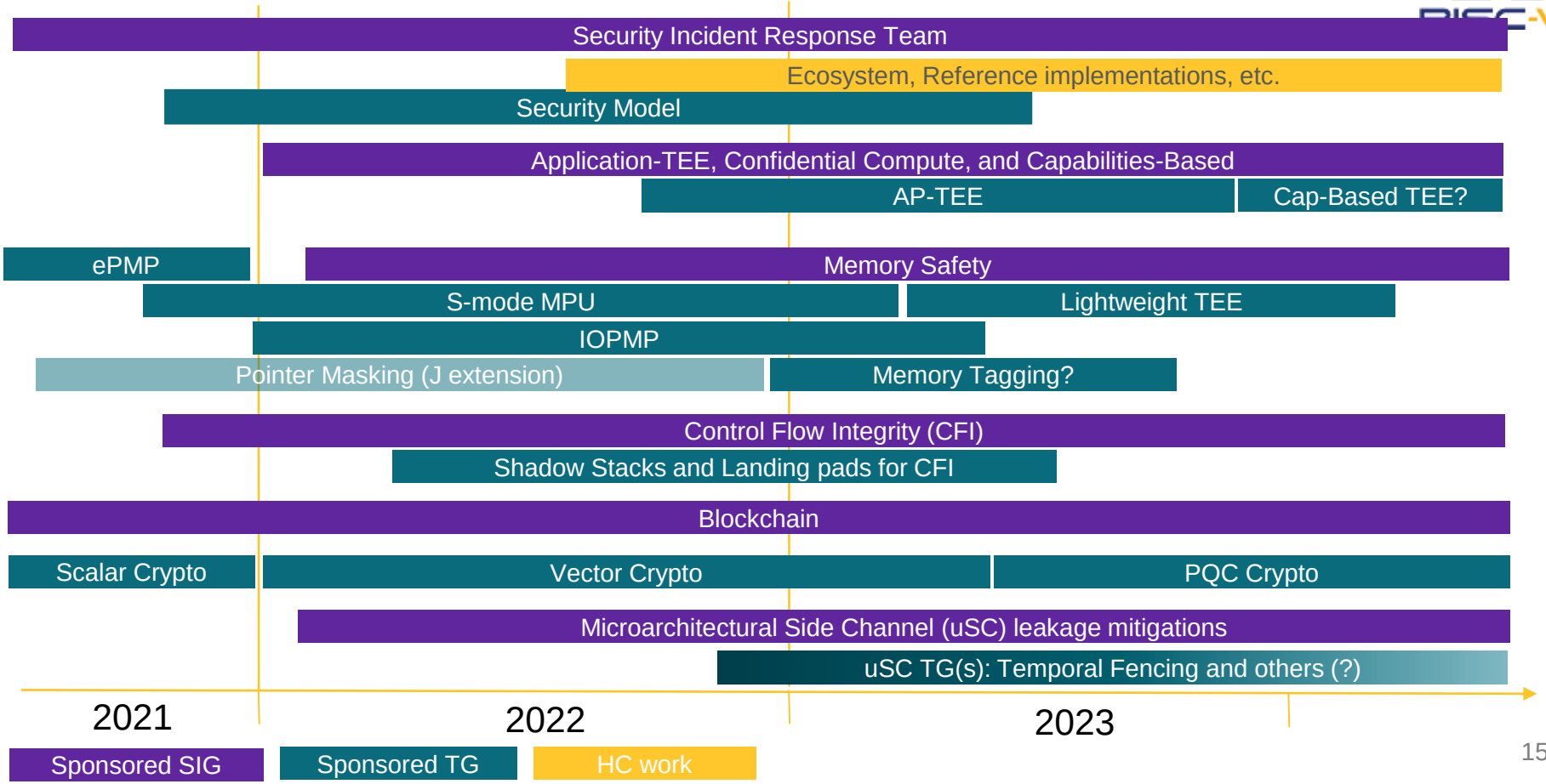
- CHERI
- Unfortunately little progress
- Seemingly a lot of interest
- Lightweight TEE based on CHERI ?

SIRT

- Ensure continuity of the RISC-V Security Incident Response Team (SIRT)
- Institute and manage a responsible disclosure process
- Triage incoming security disclosures
- Maintain a catalogue of security issues

Status & Roadmap

Security HC - Roadmap



RISC-V Security 5 year horizon

- Platform Security Model outlining RISC-V security capacities and system's integration
- Tools and Software support for RISC-V security capabilities
- Protection against side-channel information leakage at the hardware level
- Robustness capabilities to prevent malicious manipulation of e.g., code execution flows
- Cryptography support for small to large devices, including Post-Quantum Crypto
- Memory isolation and Trusted Execution Environments to securely separate applications from each other
- Support for Confidential Compute and Capability based models to enhance application and data privacy
- Blockchain technology on RISC-V based systems

We need your help:

Security@lists.riscv.org