RISC-V®

RISC-V ISA
The Entropy-Source Standard

Presented at the Cryptarchi Workshop

May 30, 2022 – Porquerolles, France

By G. Richard Newell (Associate Technical Fellow, Microchip Technology, Inc.)

RISC-V Security Rationale

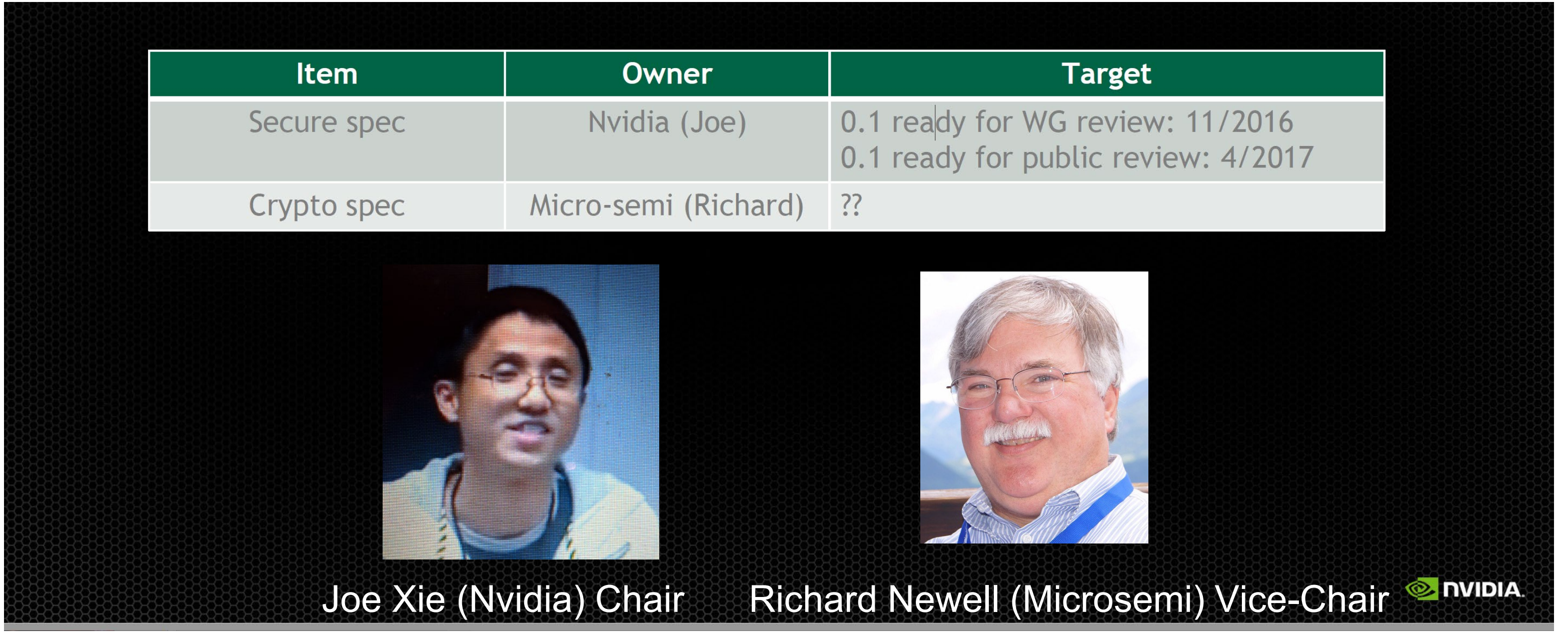
- Clean-slate architecture invites new hardware security solutions
- Open security model accelerates hardware security innovation
- Opportunity to incorporate security industry learnings & best practices
- Open governance facilitates collaboration on best security approach
- Royalty free model enables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

RISC-V International Security Organization

RISC-V®

From the Archives (circa 2015/2016)…

One Security Committee – a Chair and a Vice-Chair (and not much else!)

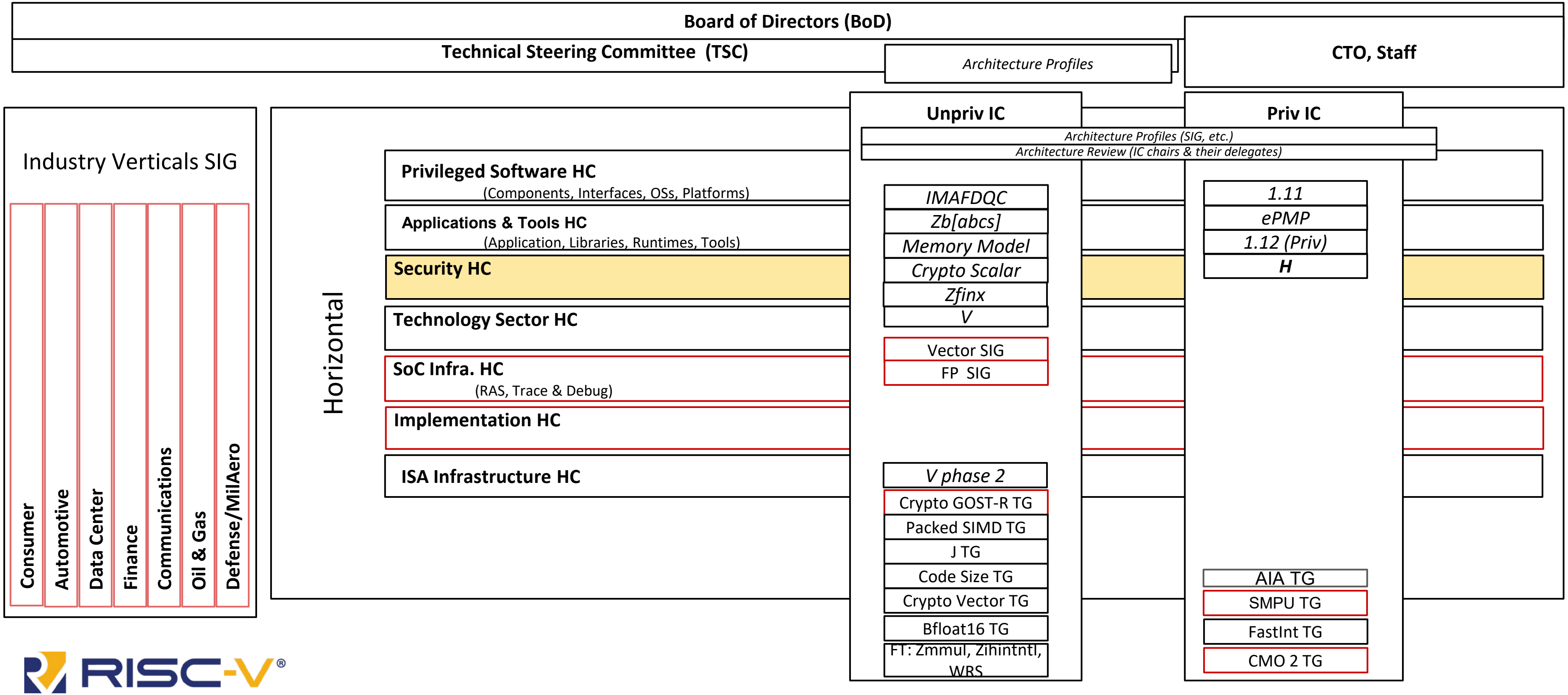


Item	Owner	Target
Secure spec	Nvidia (Joe)	0.1 ready for WG review: 11/2016 0.1 ready for public review: 4/2017
Crypto spec	Micro-semi (Richard)	??

Joe Xie (Nvidia) Chair

Richard Newell (Microsemi) Vice-Chair

RISC-V Technical Organization 2022



Board of Directors (BoD)

Technical Steering Committee (TSC)

Architecture Profiles

CTO, Staff

Industry Verticals SIG

Consumer

Automotive

Data Center

Finance

Communications

Oil & Gas

Defense/MilAero

Horizontal

Privileged Software HC
(Components, Interfaces, OSs, Platforms)

Applications & Tools HC
(Application, Libraries, Runtimes, Tools)

Security HC

Technology Sector HC

SoC Infra. HC
(RAS, Trace & Debug)

Implementation HC

ISA Infrastructure HC

Unpriv IC

Priv IC

Architecture Profiles (SIG, etc.)

Architecture Review (IC chairs & their delegates)

IMAFDQC

Zb[abcs]

Memory Model

Crypto Scalar

Zfinx

V

Vector SIG

FP SIG

V phase 2

Crypto GOST-R TG

Packed SIMD TG

J TG

Code Size TG

Crypto Vector TG

Bfloat16 TG

FT: Zmmul, Zihintntl, WRS

1.11

ePMP

1.12 (Priv)

H

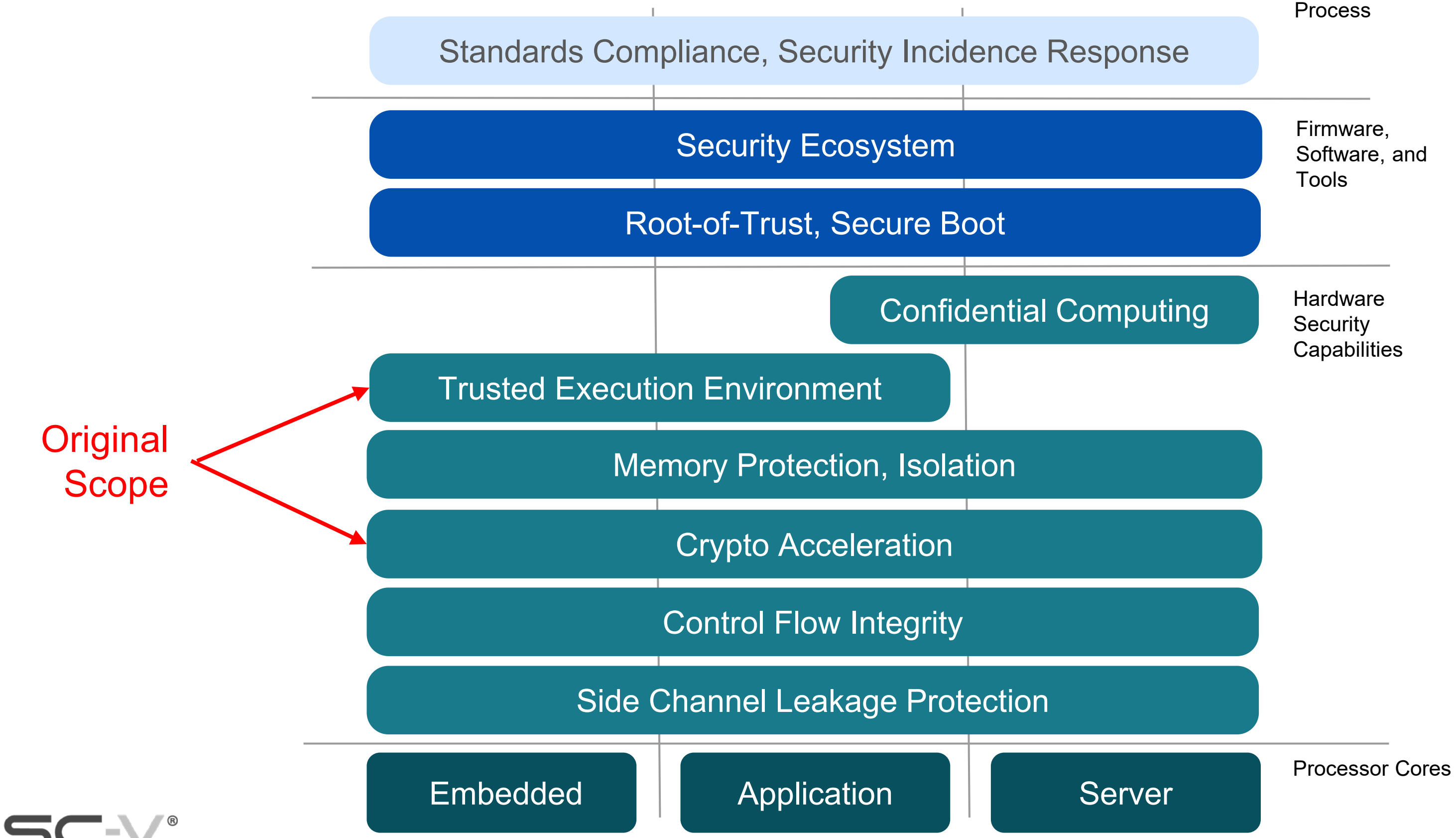
AIA TG

SMPU TG

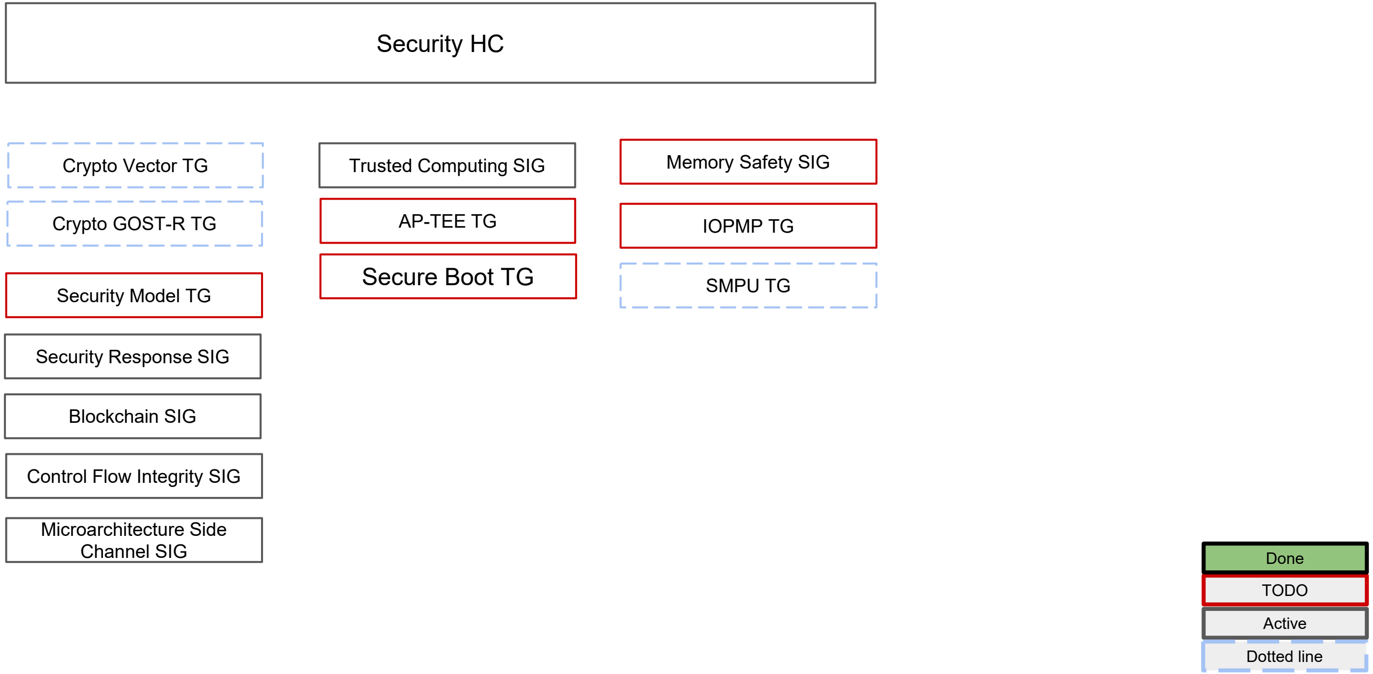
FastInt TG

CMO 2 TG

Security Scope


Process
Standards Compliance, Security Incidence Response
Security Ecosystem
Firmware, Software, and Tools
Root-of-Trust, Secure Boot
Confidential Computing
Hardware Security Capabilities
Trusted Execution Environment
Original Scope
Memory Protection, Isolation
Crypto Acceleration
Control Flow Integrity
Side Channel Leakage Protection
Embedded
Application
Server
Processor Cores

Security Horizontal Committee
and sub-committees



Security HC

Crypto Vector TG

Crypto GOST-R TG

Security Model TG

Security Response SIG

Blockchain SIG

Control Flow Integrity SIG

Microarchitecture Side Channel SIG

Trusted Computing SIG

AP-TEE TG

Secure Boot TG

Memory Safety SIG

IOPMP TG

SMPU TG

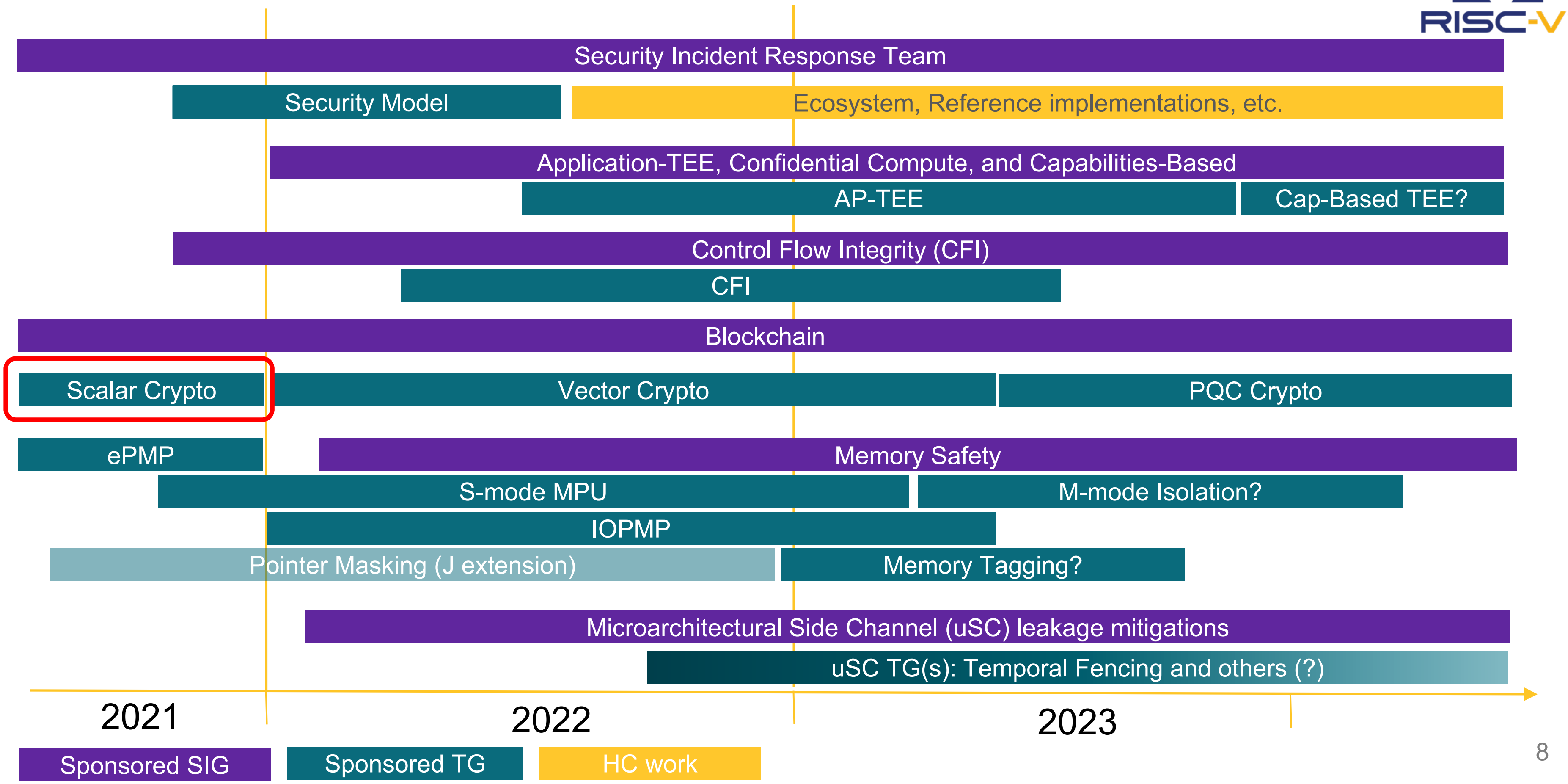
Done

TODO

Active

Dotted line

Security HC - Roadmap



Security Incident Response Team

Security Model

Ecosystem, Reference implementations, etc.

Application-TEE, Confidential Compute, and Capabilities-Based

AP-TEE

Cap-Based TEE?

Control Flow Integrity (CFI)

CFI

Blockchain

Scalar Crypto

Vector Crypto

PQC Crypto

ePMP

Memory Safety

S-mode MPU

M-mode Isolation?

IOPMP

Pointer Masking (J extension)

Memory Tagging?

Microarchitectural Side Channel (uSC) leakage mitigations

uSC TG(s): Temporal Fencing and others (?)

2021

2022

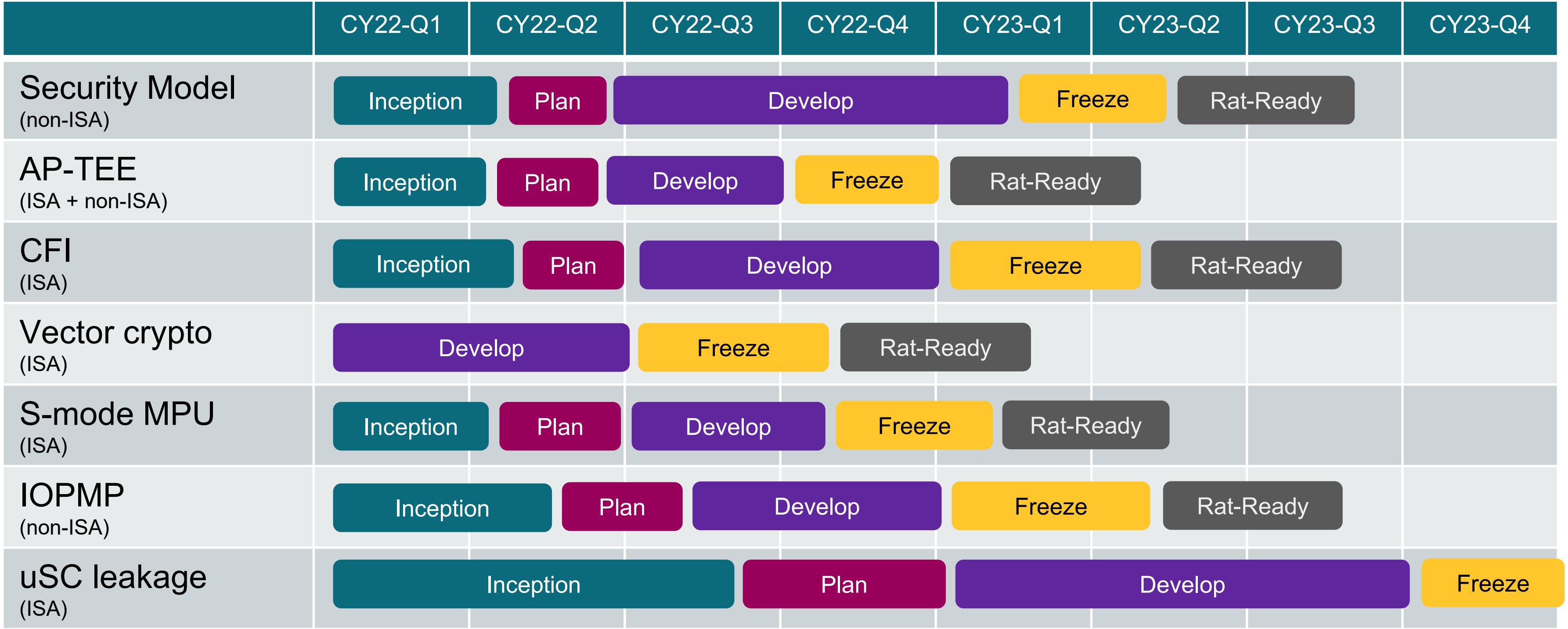
2023

Sponsored SIG

Sponsored TG

HC work

Specification Plan



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

RISC-V Cryptographic Extensions

Scalar Crypto
Vector Crypto

RISC-V®

Overview: Scalar Crypto (a.k.a. “K” for “Krypto”)

Scalar Cryptographic Extension:

- Adds Functionality required for cryptography to Unprivileged Spec.
    - Cryptographic algorithms acceleration
    - Cryptographic-quality Random bits
- True random bits generation
    - Entropy source
- Performance-driven proposals:
    - New dedicated instructions:
        - NIST: AES / SHA2
        - ShangMi: SM3 / SM4
    - Fine-grained options for highly-constrained systems
    - Some required instructions *shared* with Bitmanip:
        - Rotations / Permutations
        - Carryless Multiply
    - Data-independent timing guarantees

- This combination of **K**rypto and **B**it-manip. commands can also accelerate:
    - Asymmetric crypto (e.g., ECC, RSA)
    - GMAC (needed for AES-GCM)
    - SHA3 (needed for post-quantum crypto)
    - Many lightweight algorithms like PRESENT
    - Bit-slice implementations
        - One possible approach for DPA resistance
- “**Firsts**” – First ISA to do this for Cryptography:
    - Lightweight crypto. instructions using GP X-registers (vs. round-based using vector/SIMD registers)
        - Algorithms still done largely in software, but accelerated with lightweight instructions
    - Entropy source (vs. full random number generator)
        - supports any security strength in software
        - Compatible with modern view of TRNGs
    - Timing guarantees on a subset of the full RISC-V ISA

Overview: Vector Crypto

Vector Cryptographic Extension:

- Built on top of the base vector extension
  - RISC-V -style variable-length vector support for crypto using vector registers
  - Extremely broad range of implementations possible from narrow to wide data-paths
- Low-latency limited-rounds instructions for AES, SHA2 (i.e., SHA-256, SHA-512)
- Full-rounds instructions for AES
- Round-based for SM3, SM4 (2022, time permitting)
- AES modes (e.g., AES-CBC) and SHA2 variations (e.g., SHA-384) done in software taking advantage of the commands above

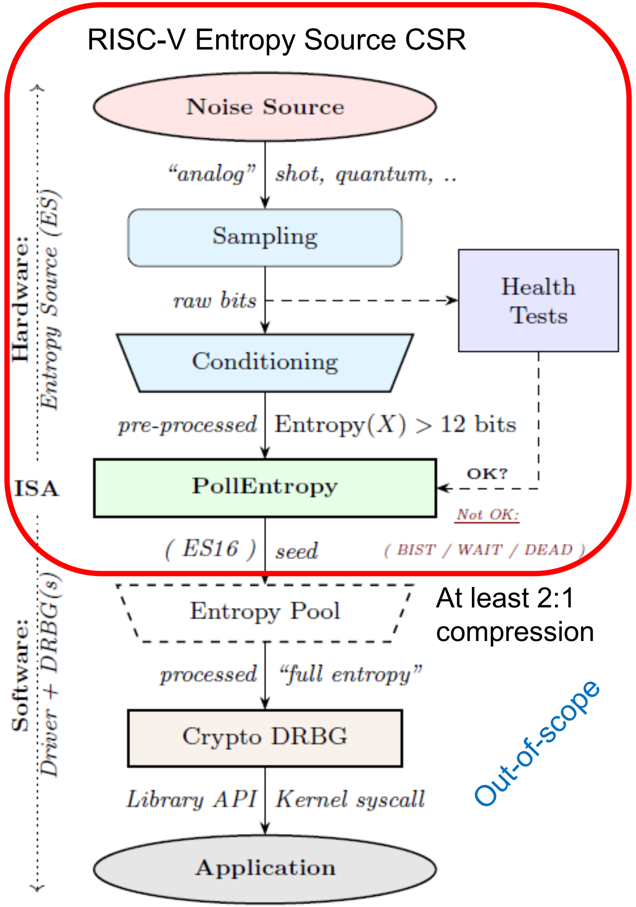
- Adds a few vector bit-manipulation -type instructions needed for cryptography:
  - Rotations & Permutations not already in the base vector extension
  - Vector Carry-less Multiply
- In total, these commands can also accelerate:
  - SHA3
  - Asymmetric algorithms (ECC, RSA)
  - GMAC (needed for AES-GCM)
- "**Firsts**" – First ISA to do this for Cryptography:
  - Full-round instructions that facilitate building side-channel-resistant micro-architectures (if desired)

The RISC-V Entropy Source

Ratified Dec. 2021

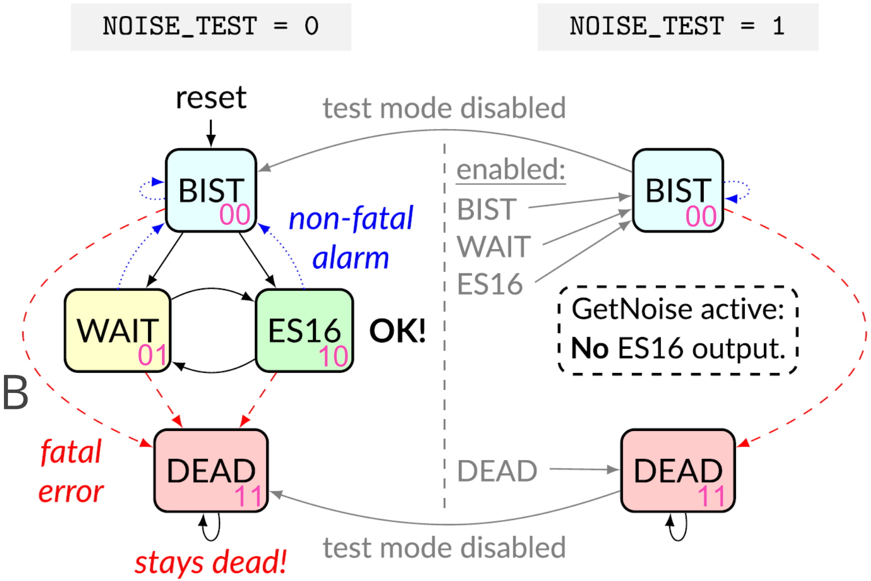
Overview: Entropy Source

- Provides standardized polling interface to a modern Entropy Source
- DRBG/PRNG post processing is out-of-scope
  - Done on software side
- Minimum Entropy guarantee:
  - 128 bits “full entropy” per 256 bits, plus one or more of:
    - 0.75 min-entropy rate per SP800-99B/C (192 bits per 256)
    - 0.997 Shannon entropy rate (per AIS-31 PTG.2)
    - Post-Quantum level 5 security
- 2:1 compression required of user on output
  - 512 bits → (e.g.) 2:1 SHA → 256-bit DRBG “seed”
- No limit on security strength… just draw more bits out
  - If an implementation *does* limit security strength (discouraged, or for virtual sources), it must support 256-bit security strength, minimum

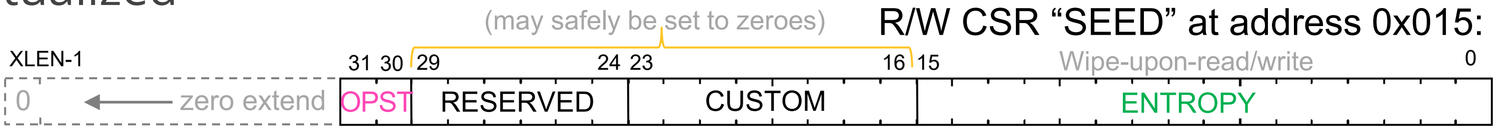


Overview: Entropy Source (cont.)

- **SEED** CSR available in M-mode. Also available in S- & U-Modes
  - If M-mode allows it
- Optional standardized raw noise interface **GetNoise** (in M-mode only), for qualification testing
- Designed to work with NIST SP800-90B & BSI AIS31
- Works with RISC-V hypervisor spec.
- Can be virtualized



R/W CSR “SEED” at address 0x015:



We need your help:

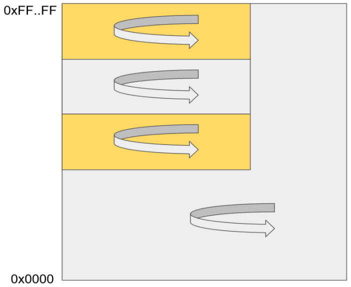
Security@lists.riscv.org

RISC-V®

Backup Slides

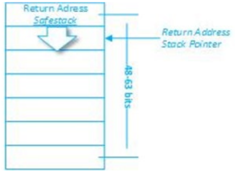
Robustness

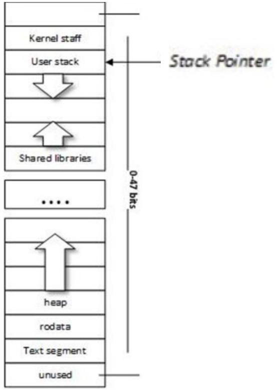
- Pointer Masking
  - actual_address = (requested_address & ~mpmmask) | mpmbase
  - Software based memory tagging
  - Memory bounding



under development:

- Control Flow Integrity
  - Shadow Stack
  - Labelled Landing Pad
- MicroArchitectural Side Channel Leakage
  - An anomaly
  - Speculation Barriers – fence.t





Cryptography

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

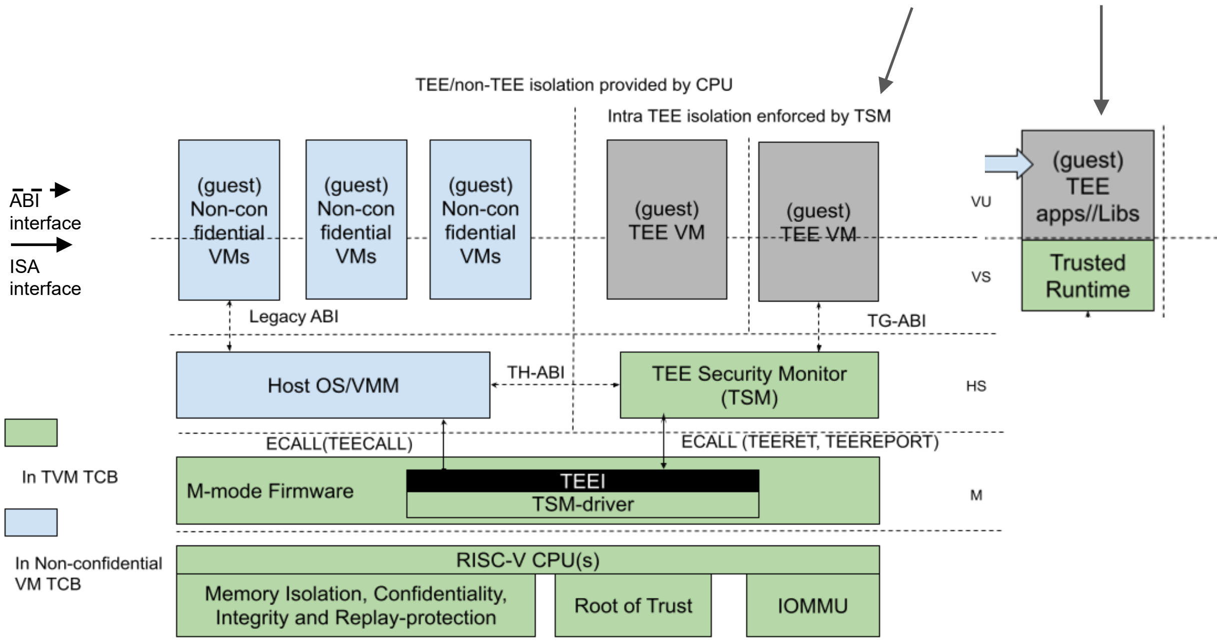
Trusted Computing

Under Development:

- Trusted Execution Environment
- APT TEE i/f to allow support on current ratified ISA
- Extensions possible to improve performance, security etc

Conf. VMs, containers

Conf. apps, libraries



TEE/non-TEE isolation provided by CPU
Intra TEE isolation enforced by TSM
ABI interface
ISA interface
(guest) Non-confidential VMs
(guest) Non-confidential VMs
(guest) Non-confidential VMs
(guest) TEE VM
(guest) TEE VM
(guest) TEE apps//Libs
Trusted Runtime
VU
VS
Legacy ABI
TG-ABI
Host OS/VMM
TH-ABI
TEE Security Monitor (TSM)
HS
ECALL(TEECALL)
ECALL (TEERET, TEEREPORT)
M-mode Firmware
TEEI
TSM-driver
M
In TVM TCB
In Non-confidential VM TCB
RISC-V CPU(s)
Memory Isolation, Confidentiality, Integrity and Replay-protection
Root of Trust
IOMMU

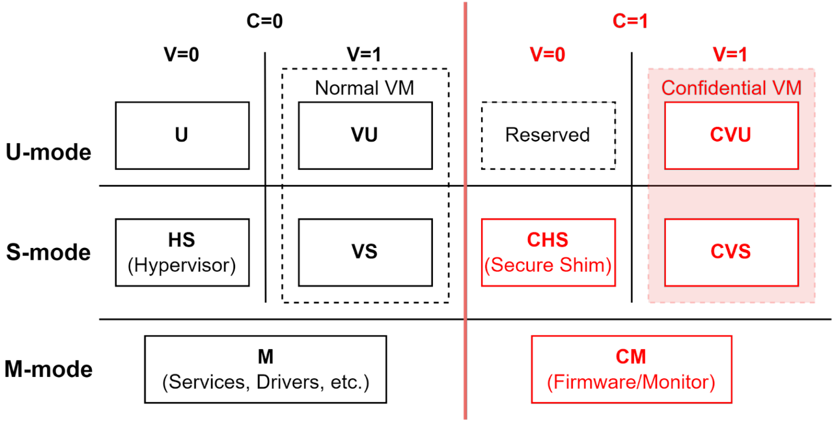
Maybe ISA affecting / **ISA Affecting**

Trusted Computing (2)

Under Development:

- Confidential Computing
  - Confidential VMs

- Extension of APP TEE
- Incorporate attestation standards



Maybe ISA affecting / **ISA Affecting**

Future Potential

Requirement Under discussion

- Lightweight TEE
  - Potential Memory isolation scheme for small M/U systems.
  - Additional context to M mode

- Capability Based Security
  - 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