RISC-V®

Security HC

2024/02/20

Agenda – and notes

- Disclosures, opens, and updates
- Architectural comparison table
- Memory safety
- Lightweight Isolation TG

ongoing/done, In plan, gap

Use cases, Scenarios, Threat mitigation gaps

Feature	RISC-V
Arbitrary Code Execution	**RWX permissions, SUM, disallow supervisor execution from user memory (unconditional on RISC-V), CHERI SIG**
Control Flow Integrity (prevent ROP/JOP…)	**Zisslpcfi (Shadow Stack Landing Pads TG), speculative gadget execution (see uSC SIG below), CHERI SIG**
Cryptography	**AES, SHA2, SM3, SM4, entropy, Data Independent Execution Latency , PQC TG, HAC TG**
Confidential Compute (A-class TEE)	**RISC-V CoVE ABI (AP-TEE TG); Smmtt TG (ISA); CoVE-IO TG**
Intra-address space isolation (M-class)	**ePMP, SPMP, IOPMP; Lightweight isolation TG (discussion in SIG), CHERI SIG**
Intra-address space isolation	**Compartmentalization, HFI (requirements discussion in RI SIG), CHERI SIG**
Virtualization-based Security	**Hypervisor extension, IOMMU, Guest translation protection**
Memory Safety	**Pointer Masking (HW-ASAN), Memory Safety, Compart (RI SIG), CHERI SIG**
Microarch. Side Channels	**uSC SIG (IS TG), fence.T, speculation barriers -- (SOK paper: https://arxiv.org/pdf/2309.03376.pdf) - need sep. fault injection discussion?** **uSC SIG should address TEA** **Potential deliverable for recommendations from this SIG for sub-cases (TEA) - AI** **[HAC addresses power/emissions side channels]**
Crypto libraries	**Gap ? are vendor performance libraries needed? How are optimizations made available?** **link to available RISC-V crypto open source libraries (openssl as e.g.), boring SSL**
Ecosystem (APIs, reference implementations, profiles, certification, protocols)	**Security Model (TG); SBI definition (Open SBI); Standard Security ABIs; Reference Implementations?**

notes

Discussed the use case, scenario, threat mitigation slide. Updated the table on Google Docs. Latest snapshot as of 21st Feb included here.

Meltdown – not mentioned. Alison to look into uarch sig writing white paper to be referenced from the security model. Should cover all uarch side channel; state of the art recommendations or links to papers. Both the fault injection component and the leakage vector (if not direct leakage).

Crypto Libs etc – need to update with supported libraries. Follow up with SW HC, tools RISE etc

Several other updates and additions reflected in the table.

Other work items

- **Memory Safety**
- **Lightweight Isolation TG (assignee RI SIG)**
  - Charter revision ?
  - Need to answer the WG question ASAP