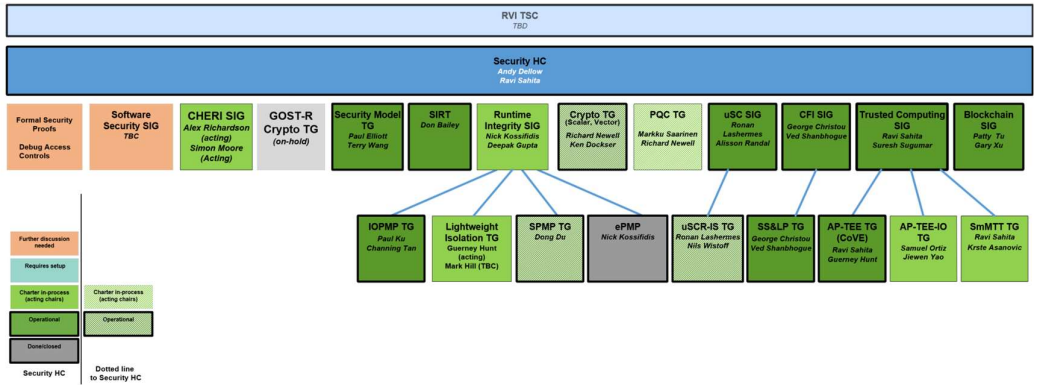
Security in Risc-V International



The Security Horizontal Committee (HC) is responsible for the overall Security organisation within Risc-V. It's charter (https://github.com/riscv-admin/security/blob/main/CHARTER.md) includes promoting Risc-V as a vehicle within the security community, as well as identifying security challenges, requirements and trends for the RVI security community to address. It proposes security committees, both Special Interest Groups and Task Groups to tackle specific security topics and ensures coordination with other Risc-V committees and external bodies. In accordance with the policies and practices of Risc-V international, all ISA affecting specifications are sponsored by either the Privileged or Non-Privileged Instruction Committees

In common with other HCs, it doesn't create ISA or non-ISA specifications. A detailed authoritative view of the structure and policies of RVI can be found at https://wiki.riscv.org/

Under the Security HC are currently six Special Interest Groups. These are formed to focus discussion on specific areas of interest and concern, and they themselves propose the formation of Task Groups that create specifications to address individual aspects of security.

1. The Trusted Computing SIG is tasked with examining zero trust architectures in HW, where a software application can both examine and attest to the environment it is running in, and have guarantees that it is isolated from other software. It will examine the state of the art for hardware-assisted technologies such as Confidential Computing, Remote Attestation, Confidential VM, Hardware TEE, Enclaves etc. and has sponsored the AP-TEE (a.k.a CoVE), SmMTT and AP-TEE-IO task groups. The Charter is at https://github.com/riscv-admin/trusted-computing/blob/main/CHARTER.md

2. The Runtime Integrity SIG's goal is to discuss strategy and gaps in ISA and non-ISA mechanisms for program safety and execution integrity for software running on RISC-V platforms. This has included forming task groups for the Physical Memory Protection units and Lightweight Isolation, formerly known as m-mode isolation. The charter is at https://github.com/riscv-admin/runtime-integrity/blob/main/CHARTER.md
3. Control Flow Integrity SIG is concerned with advanced exploitation techniques based on code reuse. Initially sponsoring the Shadow Stacks and Landing Pads Task Group, it will analyse the state of the art in code reuse attacks on an ongoing basis. Charter is https://github.com/riscv-admin/control-flow-integrity/blob/main/CHARTER.md
4. Microarchitectural Side Channel leakage SIG will analyse the state of the art and literature and develop the Risc-V strategy to prevent information leakage via microarchitectural side channels. Initially the focus is on timing side channels and the microarchitectural side channel resistant instruction spans task group. The charter is at https://github.com/riscv-admin/uarch-side-channels/blob/main/CHARTER.md
5. The Blockchain SIG's main goal is to ensure that Risc-V can meet or exceed the security and performance expectations for Blockchain technology and solutions. The charter is at https://github.com/riscv-admin/blockchain/blob/main/CHARTER.md
6. The CHERI SIG is tasked with developing a strategy for adding capability enhanced risc instructions to the Risc-V ISA. CHERI is a technology to enable fine grained memory protection and scaleable software compartmentalisation. The charter can be found at https://github.com/riscv-admin/cheri/blob/main/CHARTER.md

In addition to the SIGs, there are three task group directly sponsored by the security HC.

1. Cryptographic extensions TG adding scalar and vector cryto extensions
2. Post Quantum cryptographic extensions TG adding the quantum safe algorithm support
3. Security Model TG

The Security Model is the document that pulls together all the security components, extensions, use cases and recommendations of all the security related committees. It will define both best practice recommendations and minimum requirements for various use cases, how the various security extensions fit together to provide complete solutions across all workloads, ultimately providing security requirements for profiles. The aim is not to re-invent any non ISA feature or

protocol, but to recommend industry standards, best practice and highlight any aspects relevant to Risc-V.

Lastly, in accordance with best practice, there is a security incident response team.