Security HC Meeting

January 19th, 2023

Agenda

- Request Made for Plan Milestones (Ratification Plan document and Status checklists)
  - S-mode PMP
  - IOPMP
  - Security Model

- CHERI charter review and approval – Alex to update the current charter and make the official call for candidates. Comments on the charter requested.
- Updates from TGs + SIG - none
- Security Model – Paul to begin use case / scenario chapter, utilising Ravi's starting point.

CHERI Charter

The CHERI SIG will work on a strategy for adding a capability based security model (CHERI) to the RISC-V ISA. Enabling a capability-based security model will ensure that RISC-V can provide strong security guarantees as well as mechanisms for compartmentalization that are more scalable than traditional MMU/PMP-based techniques. This SIG will work towards defining a CHERI-enabled instruction set, toolchain requirements, programming model and psABI.

Background:

- CHERI is a technology that extends instruction sets with new architectural features (so-called capabilities) to enable fine-grained memory protection and highly scalable software compartmentalization. CHERI was developed at the University of Cambridge and SRI and includes an instantiation for RISC-V (32- and 64-bit) using the custom opcode space.

Scope:

- Determine which which currently defined architectural CHERI-RISC-V features and instructions are required for a first standardized extensions
- Scope out the changes to the Qemu, Sail, and the LLVM toolchain for this effort
- Communicate with other security SIGs and TGs to ensure compatibility

Please review and comment at :
https://github.com/riscv-admin/cheri/blob/main/CHARTER.md