RISC-V®

Security HC

1st October 2024

Agenda

- John Ingalls (sifive) has two fast track proposals that were discussed at the chairs meeting this week.

- Do we have any discussion points or agenda topics for the members day open slots ?
  - We have slots for Security HC, Runtime integrity SIG and Trusted computing SIG.
  - For Security HC we plan to give an update overview based on the latest deck on google drive

Please all chairs update slide 5 of https://docs.google.com/presentation/d/19pXyRsSqXyy5XeodcjDkTYsFdgy2GwCzz09Ic_3Ojwg/edit?usp=sharing

RTI SIG will discuss MTE.

Any topics to be discussed please mail the relevant SIG or security @lists.riscv.org

Fast tracks

- ‘Svukte’ provides a simple mechanism checking the top address bit to prevent side channel timing attacks on Kernel Address Space Layout Randomization (KASLR). https://docs.google.com/presentation/d/1N8bYBjQSMWahFSOY4zf4a1fnel7SpWwzv-QyVG_-CCI
- Concerns expressed that the ACTs are complete to a minimum standard prior to ratification – i.e. more than just CSR presence.

- ‘Smpmpmt is a straightforward addition of the Svpbmt (Page Based Memory Type) override control ability to the PMP CSRs for control of memory types even in the absence of virtual memory overrides. https://docs.google.com/presentation/d/1fKnMUc2H5BqSw0inxcPyJpyaZQykAPvpoWlyx6l_ajQ’
  - Needs discussion about its interaction, or lack thereof, with EPMP.
- Request to clarify composition with other PMA sources, and how entry PMP priority affects compsiiton.
- It was noted that PMP resources are limited, and additional regions for memory type may not be available.
- Scheme will fit with ePMP and SPMP, but above consideration need documenting.