
RISC-V®
Security HC
15th October 2024

Agenda

- Svukte - constant time or data independence. The extension requires data independence, but that is not testable. Constant time is testable but may over constrain implementation. QEMU patches state the extension requires constant time… it was agreed that the wording in the extension is ok, and noted again that data independence and constant time are not the same thing.
- Summit next week –

Please update your TG entries on slide 6

https://docs.google.com/presentation/d/19pXyRsSqXyy5XeodcjDkTYsFdgy2GwCzz09Ic_3Ojwg/edit?usp=sharing

any other topics for the members day meetings ?

Agreed to add CHERI TG as active

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