RISC-V®

IOPMP Task Group Meeting

March 16, 2023

Video link

Agenda

- Any update related to IOPMP: from the Runtime Integrity SIG?
  - M-mode isolation discussion: may be related to IOPMP, keep watching.
- Any feedback: Lock MDCFG and static IOPMP entries?
  - Feedback is welcome, but there is no so far.
- Reactions to violation, NVIDIA’s proposal: Channing
  - The slides are posted separately in the mailing list.
- The reaction to prefetch violation: Andes’ proposal
  - As follows!

Reactions to Prefetch Violation

- “Prefetch” is widely used to reduce read latency by guessing the following read addresses and reading back in advance.
- However, those guessed addresses could violate the IOPMP rules unintentionally.
- Such violation due to the prefetcher may not need to kill the whole process or to be intervened by security software. Instead, we could take an optional milder reaction.
- The proposed idea: optionally provide a configuration of the reaction for a violation recognized as a prefetch.

Reactions to Prefetch Violation (cont.)

- The prefetch violation always returns a bus error. No real data will be returned.
- No interrupt will be triggered. If an interrupt is needed, one can use the original interrupt.
- The reaction configuration of prefetch violation :
  - PrefReactEna: a bit to enable the reaction for the prefetch violation.
  - PrefReactErr: the error type of response for a prefetch violation.
  - Prefetch violation is not recorded.
- Add one bit into the record:
  - On PrefReactEna=disable, a bit PrefVio indicates if it is a prefetch violation.