May 11, 2023 | RISC-V Control Transfer Records TG Meeting

Attendees: tech.meetings@riscv.org Beeman Strong Bruce Ableidinger

Notes

- **Attendees**: Beeman, Bruce, JohnS, Ved
- **Slides/video** here
- Update: S*csrind fast-track extension drafted, under ARC review
- Resuming RASEMU review
  - Updated instruction list to include Zc* insts
    - Ved: Table 2.1 in unpriv spec codifies RAS actions, but doesn't include Zc*
  - Had not yet discussed co-routine swap insts, which effect a RET then a CALL
    - So overwrite CTR entry 0 when RASEMU=1
- CTR RAS corruption
  - setjmp/longjmp and C++ exceptions cause stale/orphaned entries to be left
    - Ved: Thread switching in user space also switches the stack, can leave orphaned calls
      - switchto switches stack but not CTR
      - Would see 2 stacks in same CTR
  - CFI requires SW to do sspinc to pop orphaned entries off of shadow-stack (SS)
    - No point in leveraging that for CTR. sspinc is also used for other things, and SW should use SS over CTR stack when SS enabled.
  - Slide 24 has an error, RET at 0x540 will not mispredict. But later RET, back to routine that called foo(), will.
  - Could try to use that mispredict as an indication that CTR stack may be corrupted, but not clear how to make it useful
    - And stale/orphaned entries may be lost, if stack goes deep enough after longjmp()
  - No obviously useful solution to this, propose we do nothing for now
- CTR freeze
  - Can opt to inhibit CTR recording on breakpoint exception or LCOFI
    - Should not capture trap, to preserve entries leading to it
    - Future precise sampling mechanism may include some additional freeze on overflow, rather than LCOFI, depending on mechanism
  - Useful to ensure that transfers in event handler aren't recorded
    - Do OS's typically use vectored events? Would mean potentially several transfers before the source of the event is known
  - Freeze not useful when handling events in inhibited mode
  - D-mode inhibited always, don't need to use freeze for that
  - **AI Beeman**: check with Atish if expect perf to always get LCOFIs in M-mode, to work around interrupt masking
- **Out of time**

        - Will close on CTR freeze next time

Action items

- [ ] May 11, 2023 - Beeman Strong - check with Atish if expect perf to always get LCOFIs in M-mode, to work around interrupt masking