Jun 8, 2023 | RISC-V Control Transfer Records TG Meeting

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

Notes

- **Attendees**: Beeman, Snehasish, RobertC, JohnS, Bruce, Rajnesh
- **Slides/video** here
- Update: VS and VU bits in mctrcontrol were redundant, VS/VU in vsctrcontrol will dictate recording in VS/VS. Spec will be updated.
- Resume RASEMU corruption
    - Propose CTR clearing for stack switch, and CTR sp save/restore for stack unwind
    - Reviewed illustrations
        - On stack switch, clearing may lose some valid entries but ensures that no entries from another stack persist
        - On stack unwind, switch CTR sp along with sp. However, some now-invalid entries left with V=1
    - What if CTR stack wraps between setjmp and longjmp?
        - Then restoring CTR sp would still mean a corrupted stack
    - This workaround would need CTR sp to be U-mode accessible
    - Robert: CTR sp could have wrap bit to know if CTR stack wrapped
    - Robert: CTR could have read & write pointer, then no valid bit needed
- Discussed synthesized entries, e.g. for emulating a transfer inst
    - Today emulator would have to manually rotate the entire CTR stack
    - Could add command bits to rotate the stack, or increment/decrement CTR sp
        - Robert: Prefer push and pop to rotate forward and rotate backward
    - Have to be careful that CTR is not updated between CTR sp read and write
        - Bruce: could set FROZEN bit when doing RMW of CTR sp
- Discussed Linux perf LBR stack stitching, which uses LBR_TOS to combine stacks from multiple samples
- Reviewed new ISA that would support all of the above
- Robert: think we should expose wr ptr. Stitching would be better with a wrap bit.
- Beeman: would like to have more SW feedback before we add support to expose stuff to U-mode, to feel confident that it will be used
- Beeman: if RASEMU=0, user mode writes to CTR sp, or to CLR, will mess things up
    - Could gate writes by RASEMU=1
- Snehasish: CLR from user mode is probably good enough, not sure if CTR sp is useful
- Plan for now: add CTR sp accessible in M/S-mode. Await SW feedback before adding any user mode access.
- Out of 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