Apr 13, 2023 | RISC-V Control Transfer Records TG Meeting

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

Notes

- **Attendees**: Beeman, Bruce, JohnS, Snehasish
- **Slides/video** here
- Latency field
    - Cycle representation, looked at FP options and ranges supported
        - How large of values do we need when capturing only calls/rets, and how large of values do we want to have precise counts?
        - **AI Snehasish** to collect some data, decision deferred
    - Looked at scenarios where cycles will be lost, and options to address them
        - Snehasish: on LBRs will sometimes see crazy values, would be nice to have a valid bit
            - Beeman: likely confirms that LBRs keep counting through traps to OS
- Transfers to/from inhibited mode
    - Reviewed enabling from last meeting
    - Walked through examples of options for recording them (on trap vs trap return)
    - Agreed to record on trap, so that handler has option to manipulate the record
    - Discussed whether such external traps should have regular transfer type (INTR or EXC) or special type (External Trap)
        - Generally think less priv'd code should know little about such excursions, but maybe INTR vs EXC isn't a problem
        - Using External Trap encoding might allow repurposing Target PC fiel
        - No conclusion, will revisit
- Approved proposal for CTR depth discovery and configuration
    - New xctrcontrol.DEPTH field, can have hardcoded bits
- Reviewed RAS emulation mode
    - CALLs push, RETs pop
    - Reviewed what happens on a popped entry (cleared valid bit, rotated stack)
    - Walked through example
    - Bruce: how can you do flame graphs with this if we don't sum time across entries?
        - Beeman: Intel doesn't sum time, can't do flame graphs
        - Snehasish: generally see flame graphs constructed from num samples, rather than trace
        - Can use CTR for the stack component, but samples for the time component
    - Moving to shadow stacks might be better than CTR in RASEMU mode, but not sure if adoption of CFI will be common enough
        - Adds too much overhead to enable CFI just for profiling

    - RASEMU can be corrupted by long jumps
    - Believe LBR had issues with stack switching, but need to get details
- Out of time. Will aim to close on RASEMU mode next time.

Action items

- [ ]