May 16, 2024 | RISC-V Perf Analysis SIG Meeting

Attendees: Snehasish Kumar tech.meetings@riscv.org Beeman Strong

Notes

- **Attendees**: BoG, Snehasish, BruceA, JeffN, MattT, Chun, Robert, Beeman, Simon, Dmitriy, SimonD
- **Slides** here (forgot video, sorry!)
- Opens/updates
    - New Performance Sampling TG has infrastructure setup, will begin meetings in coming weeks
    - CTR still working on freeze collateral
- Call stack unwinding (Chun presenting)
    - RISC-V, ARM, & x86 all have shadow-stack (SS)
        - Used for ROP protection, but also for profiling/debug
        - Like call-stack, but without params and other data
        - Writes not allowed, but reads allowed
    - Could have SW collect this with samples, or even have HW push it out
    - There is performance cost to having SS on, few percent
        - But if it's mandated for security then using it for sampling is free
        - Snehasish: don't expect that for datacenter. Some SW layers are pretty deep, using SS may be overkill there.
        - Each process gets its own SS page (on Intel at least), so that is another limitation
    - Today SW uses frame pointers to record call-stack when collecting a sample
    - Why not prefer CTR stack over SS?
        - Datacenter really cares about stack accuracy, but maybe others don't. Datacenter also tends to be deeper than others.
        - Vtune tried to use LBR call-stack at client, but found that most samples had corruption. Presumably due to exceptions, etc.
    - HW assisted approach
        - Ideal would be to profile without any interruption to SW
            - So HW would snapshot state and store it out opportunistically
        - If we don't stop SW (e.g., with interrupt or firmware trap), how do we snapshot the stack before SW modifies it?
            - Could do so with CTR stack (with area cost), but not SS or CS in memory
            - Top of stack likely in L1 cache, but still have to do loads to get it
        - Is it faster? Simplest implementation would be a trap to firmware to collect stack, which may not be faster. If use HW FSM, gets complicated because there are multiple stack options (CS, SS, CTR) to consider and prioritize.

            - Chun: suggesting this only works with SS. So if SS implemented and enabled, then can use it.
        - Question about need: when will SS be in wide use? Most extensions we've pursued have been playing catch up, this would be speculative.
            - CET SS still not in use within Google
    - **Out of time**, can continue discussion on the email list
    - Some question about how RISC-V SS can be read, since page is marked R=0.
        - **AI Beeman Strong to check with Ved**

Action items

- [ ] Beeman Strong - May 16, 2024 - check with Ved about reading SS
- [ ] Beeman Strong - Jul 28, 2022 - Reach out about proprietary performance analysis tools
- [ ] Beeman Strong - Jul 28, 2022 - Reach out to VMware about PMU enabling