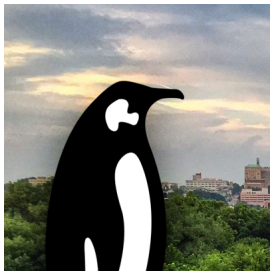

Contribution ID: **271** Type: **not specified**

Control Flow Integrity on RISCV

Monday, 13 November 2023 12:25 (20 minutes)

Memory safety issues impact program safety and integrity. One of the implications of such issues is subversion of programmer intended control flow of the program and thus violation of control flow integrity of program. There has been various software (and hardware) mechanisms using which one can enforce control flow integrity of the program. One such mechanism is using hardware assisted shadow stacks (for backward edge or return flow) and landing pad instruction (for forward edge or calls/jmps). Mainstream instruction set architectures (ISA) have extensions that can be leveraged by software to assist in enforcing control flow integrity. RISC-V has ongoing effort on similar lines to ratify an extension [1]. Additionally there has been RFC patch series [2].
This talk is mostly going to be around approach and design decisions around CFI patch series seeking input from community members. Additionally this talk will go into details of how to use CFI extension to enforce kernel control flow integrity on risc kernel.

1 - https://github.com/riscv/riscv-cfi
2 - https://lore.kernel.org/lkml/20230213045351.3945824-1-debug@rivosinc.com/T/

Primary author: GUPTA, Deepak

Presenter: GUPTA, Deepak

Session Classification: RISC-V MC

Track Classification: LPC Microconference: RISC-V MC