Contribution ID: **100** Type: **not specified**

Finer-grained kernel control flow integrity and challenges

Kernel control flow integrity RFC patches [1] are out. It uses existing hooks in shadow call stack config for riscv hardware assisted shadow stack. Forward cfi is finer grained cfi using a toolchain which matches landing pad labels between callsite and taken-targets. Talk will focus on following emerging challenges, proposed solutions and further discussions/comments on them.

Forward cfi
- How to co-exist with execution contexts sharing S-mode without awareness of landing pad. Two examples here are UEFI runtime services and loadable kernel modules.

Backward cfi
- How to do faster shadow stack allocations. Kernel shadow stack creation needs that direct mappings must also be unmapped so that attacker doesn't get an alternate way of writing to shadow stack. This means tlb shootdowns on conversions of vmalloced memory <–> shadow stack. Similarly returning shadow stack back to vmalloc requires this memory to become RW again. Changing perms and tlb shootdowns will lead to slower fork path.

Common topic to both fcfi and bcfi
- eBFP, tracing and probes
- policy on enabling and lockdown

[1] https://lore.kernel.org/all/20250724-riscv_kcfi-v1-0-04b8fa44c98c@rivosinc.com/

Primary author: Mr GUPTA, Deepak

Presenter: Mr GUPTA, Deepak

Session Classification: RISC-V MC

Track Classification: RISC-V MC