Contribution ID: **257** Type: **not specified**

Linux Kernel Control-Flow Integrity Support

Wednesday, September 14, 2022 5:00 PM (45 minutes)

Control-Flow Integrity (CFI) is a technique used to ensure that indirect branches are not diverted from a pre-defined set of valid targets, ensuring, for example, that a function pointer overwritten by an exploited memory corruption bug is used to arbitrarily redirect the control-flow of the program. The simpler way to achieve CFI is through instrumenting the binary code being executed with proper checks that verify the sanity of the indirect branches whenever they happen. To help with this goal, some CPU vendors enhanced their hardware with extensions that make these checks simpler and faster. Currently there are 4 different instrumentation setups being more broadly discussed for upstream: kCFI, which is a full software instrumentation that employs a fine-grained policy to validate indirect branch targets; ARM's BTI, which is an ARM hardware extension that achieves CFI in a coarse-grained, more relaxed form; Intel's IBT, which is an X86 hardware extension that similarly to BTI also achieves coarse-grained CFI, but with the benefit of also enforcing this over speculative paths; and FineIBT, which is a software/hardware hybrid technique which combines Intel's IBT with software instrumentation to make it fine-grained without losing its good performance while still adding resiliency against speculative attacks.

In this session, kernel developers and researchers (Sami Tolvanen, Mark Rutland, Peter Zijlstra, Joao Moreira) will provide an overview on the different implementations, their upstream enablement and discuss the contrast in approaches such as granularity or implications of design differences such as callee/caller-side checks.

I agree to abide by the anti-harassment policy

Yes

Primary authors: MOREIRA, Joao (Intel Corporation); RUTLAND, Mark (Arm Ltd); ZIJLSTRA, Peter (Intel OTC); TOLVANEN, Sami (Google)

Presenters: MOREIRA, Joao (Intel Corporation); RUTLAND, Mark (Arm Ltd); ZIJLSTRA, Peter (Intel OTC); TOLVANEN, Sami (Google)

Session Classification: Toolchains

Track Classification: Toolchains Track