Contribution ID: **148** Type: **not specified**

Where are we on security features?

Wednesday, 14 September 2022 10:00 (45 minutes)

There has been tons of work across both GCC and Clang to provide the Linux kernel with a variety of security features. Let's review and discuss where we are with parity between toolchains, approaches to solving open problems, and exploring new features.

Parity reached since last year:

- zero call-used registers
- structure layout randomization

Needs work:

- stack protector guard location
- Link Time Optimization
- forward edge CFI
- backward edge CFI
- array bounds checking
- -fstrict-flex-arrays
- __builtin_dynamic_object_size
- C language extension for bounded flexible arrays
- builtin for answering "does this object end with a flexible array?"
- -fsanitize=bounds
- integer overflow protection
- Spectre v1 mitigation

I agree to abide by the anti-harassment policy

Yes

Primary authors: COOK, Kees (Google); ZHAO, Qing

Presenters: COOK, Kees (Google); ZHAO, Qing

Session Classification: Toolchains

Track Classification: Toolchains Track