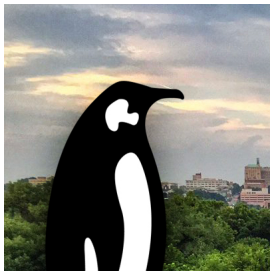

Contribution ID: **187** Type: **not specified**

Security Features status update

Monday, 13 November 2023 09:30 (50 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:

- -fstrict-flex-arrays=3
- -fsanitize=bounds
- __builtin_dynamic_object_size()
- arm64 Shadow Call Stack (backward edge CFI)

In progress:

- __counted_by(member) attribute for bounded Flexible Array Members

Needs work/discussion:

- -fbounds-safety language extension proposal
- handling nested structures ending in a Flexible Array Member (Clang)
- language extension to support Flexible Array Member in Unions
- arbitrary stack protector guard location (Clang: risc-v, powerpc)
- Link Time Optimization (Kernel support for GCC)
- forward edge CFI (GCC: KCFI)
- backward edge CFI (Kernel support for CET)
- arithmetic overflow protection (GCC & Clang)
- -Warray-bounds false positives (GCC)

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

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

Session Classification: Toolchains

Track Classification: Toolchains Track