Contribution ID: **177** Type: **not specified**

GCC's -fanalyzer and the Linux kernel

Wednesday, 14 September 2022 12:00 (45 minutes)

I'm the author of GCC's -fanalyzer option for static analysis.

I've been working on extending this option to better detect various kinds of bugs in the Linux kernel (infoleaks, use of attacker controlled values, etc).

I've also created antipatterns.ko, a contrived kernel module containing examples of the bugs that I think we ought to be able to detect statically.

In this session I will:

- present the current status of -fanalyzer on the Linux kernel, and
- ask a bunch of questions about how this GCC option and the kernel should best interact.

I have various ideas on ways that we can extend C via attributes, named address spaces, etc for marking up the expected behavior of kernel code in a way that I hope is relatively painless. I'm an experienced GCC developer, but a relative newcomer to the kernel, so I'm keen on having a face-to-face discussion with kernel developers and other toolchain maintainers on how such an analyzer should work, and if there are other warnings it would be useful to implement.

I agree to abide by the anti-harassment policy

Yes

Primary author: MALCOLM, David (Red Hat)

Presenter: MALCOLM, David (Red Hat)

Session Classification: Toolchains

Track Classification: Toolchains Track