

Adding kernel-specific test coverage to GCC's -fanalyzer option

Thursday, 23 September 2021 08:20 (35 minutes)

I'm the author of GCC's static analysis pass, -fanalyzer. I've been experimenting with extending it to add kernel-specific diagnostics: detecting infoleaks and unsanitized syscalls at compile-time. I'd like to discuss these and other ideas for improving the test coverage of our kernel builds.

Primary author: MALCOLM, David (Red Hat)

Co-author: O'DONELL, Carlos (Red Hat)

Presenters: O'DONELL, Carlos (Red Hat); MALCOLM, David (Red Hat)

Session Classification: Kernel Dependability and Assurance MC