Contribution ID: **89** Type: **not specified**

KFuzzTest: Targeted Fuzzing of Internal Kernel Functions

Fuzz testing the Linux kernel with system-call fuzzers has been highly effective, but this approach struggles to reach and test deeply nested internal kernel functions. This leaves significant parts of the kernel's logic, particularly complex data parsers, under-tested and potentially vulnerable. We introduce KFuzzTest, a novel framework aiming to bridge this gap by directly exposing stateless or low-state internal kernel functions to a userspace fuzzer.

The KFuzzTest architecture is designed to be both powerful and developer-friendly. It provides a simple macro-based API that allows kernel developers to define fuzz test targets alongside their functions, specifying input domain constraints and type annotations. This metadata is compiled into dedicated ELF sections within the vmlinux binary, enabling automatic discovery by the userspace fuzzer. Communication between the fuzzer and the in-kernel test harness is facilitated via debugfs entries.

We have successfully integrated a proof-of-concept with syzkaller, demonstrating how this framework can perform coverage-guided fuzzing on internal kernel functions. This approach empowers developers to write effective, targeted tests for their own code. This presentation will cover the framework's design, implementation details, and a path forward for upstreaming the work to the Linux community.

Primary author: GRAHAM, Ethan (ETH Zurich)

Co-author: POTAPENKO, Alexander (Google)

Presenter: GRAHAM, Ethan (ETH Zurich)

Session Classification: Kernel Testing & Dependability MC

Track Classification: Kernel Testing & Dependability MC