Designing UAPI for Fuzz-ability

Monday, 12 September 2022 16:10 (20 minutes)

Fuzzing (randomized testing) become an important part of the kernel quality assurance. syzkaller/syzbot report a hundred of bugs each month. However, the fuzzer coverage of the kernel code is far from being complete and some subsystems are easier to fuzz/reach, while others are harder/impossible to fuzz/reach. In this talk Dmitry will talk about patterns and anti-patterns of UAPI/subsystem design with respect to fuzz-ability:

• what makes it impossible to fuzz a subsystem
• what leads to unreproducible crashes
• why a subsystem may be excluded from fuzzing
• what makes a perfect interface/subsystem for fuzzing

I agree to abide by the anti-harassment policy

Yes

Primary author:  VYUKOV, Dmitry (Google)
Presenter:  VYUKOV, Dmitry (Google)
Session Classification:  Kernel Testing & Dependability MC
Track Classification:  LPC Microconference: Kernel Testing & Dependability MC