Contribution ID: **101** Type: **not specified**

syzkaller/sanitizers status update

Wednesday 26 August 2020 07:15 (30 minutes)

syzkaller is an open-source coverage-guided OS kernel fuzzer used to continuously test the Linux kernel. To date syzkaller has found 3000+ bugs in the upstream kernel. The kernel sanitizers are a family of dynamic bug finding tools (KASAN, KMSAN, KCSAN) that detect various types of bugs in the kernel.
In this talk Dmitry will give an overview of new developments in the past year for syzkaller and sanitizers and share some stats for kernel bugs and syzkaller contributions. Then Dmitry will outline the testing process of the syzkaller itself and some nice features that the kernel testing process could borrow. The talk concludes with future work for syzkaller/sanitizers.

I agree to abide by the anti-harassment policy

I agree

Primary author: VYUKOV, Dmitry (Google)

Presenter: VYUKOV, Dmitry (Google)

Session Classification: Testing and Fuzzing MC

Track Classification: Testing and Fuzzing MC