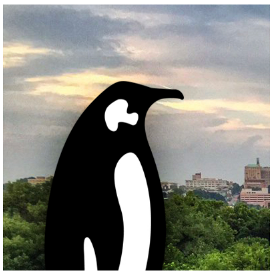
Linux Plumbers Conference 2023



Contribution ID: **151** Type: **not specified**

Syzbot: 7 years of continuous kernel fuzzing

Wednesday 15 November 2023 09:30 (45 minutes)

Syzbot is an automated system that continuously fuzzes OS kernels and routes the reports to kernel developers. Since 2017, syzbot has already found and published more than 10000 findings in the Linux kernel.

Levels of adoption and reception of the tool differ throughout the kernel, but it has definitely had a positive impact on the Linux kernel's health. To date, more than 5500 findings have been addressed and 3300+ Linux commits explicitly mention syzbot. Occasionally (for better or worse), our reports spark passionate discussions about kernel testing and development paradigms.

The talk begins with a brief overview of the tool and the functionality it offers to kernel developers to facilitate bug report triaging, debugging, and fixing. We'll also cover the major challenges of building and operating an automated kernel testing system that have been (and are still being) faced since the launch of syzbot.

The second half of the talk will be dedicated to the discussion of why some fuzzer-reported findings are addressed by the kernel developers community, while some are not, and what can be done to improve the situation. We'll share our understanding of the important factors as well as the relevant syzbot-accumulated statistics and we also hope to hear your opinion on the subject.

Additionally, we will elaborate on the syzbot areas that have been significantly reworked to address user feedback and to get more kernel bugs fixed. For instance, we'll talk about the classification of findings by the affected kernel subsystems and per-subsystem lists of not yet addressed bugs. Another highlight is the new functionality to detect missing fix backports for syzbot findings in stable trees.

We welcome and encourage discussion, feedback, and constructive criticism on how syzbot can be made more helpful to the kernel development community.

Primary author: NOGIKH, Aleksandr (Google)

Presenter: NOGIKH, Aleksandr (Google)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track