# syzbot ci

## Continuous Patch Series Fuzzing

Aleksandr Nogikh (Google)
LPC'25 Tokyo, Japan

# Agenda

- Context
- Bug Fixing Factors
- Shifting Left Kernel Fuzzing
  - Auto-Triage
  - Focused Fuzzing
  - Triage of Findings
- Pilot Deployment
- Preliminary Statistics
- Plans / Next Steps

# Context

**syzkaller** is a coverage-guided kernel fuzzer.

**syzbot** is a continuous kernel build / fuzz / report aggregation system.
**syzbot** uses **syzkaller** for the actual fuzzing.

Since 2017, syzbot has reported more than **13,500** bugs to the mailing lists.

These bugs were found when fuzzing tips of the kernel trees:
median bug discovery time is **51 days**
(with a very long tail, e.g. **75**th percentile is **291** days)

# Bug Fixing Factors (2025)

Share of reports addressed within 50 days after detection:

- With cause bisection: **42%**.
- No cause bisection: **24%**.

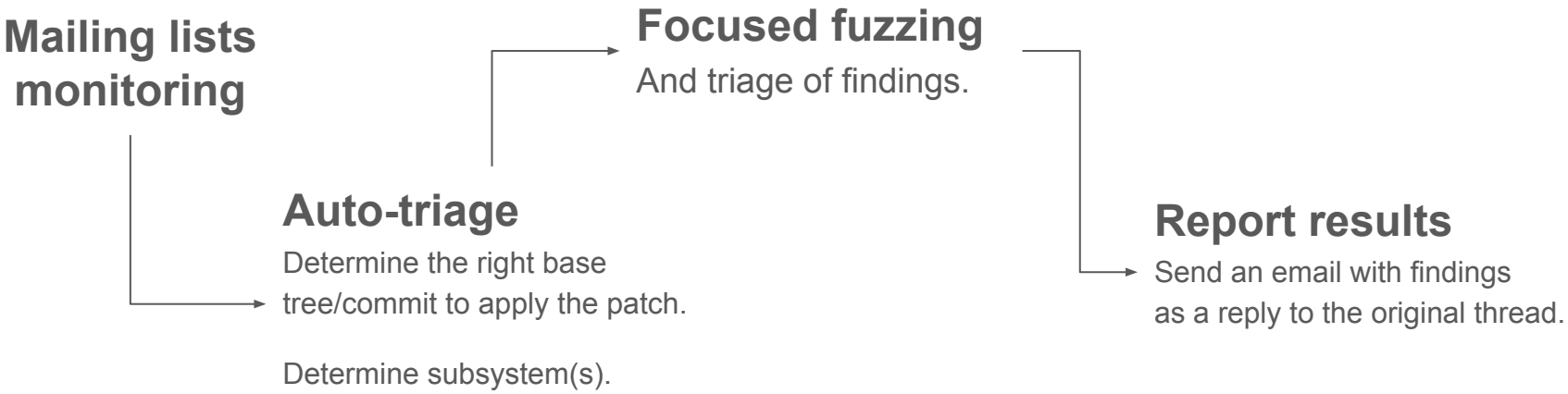
**Knowing the guilty patch is important.**

Bug fix rate per time to discover by the moment of report:

| < 7 days | 14-30 days | 30-100 days | 100-365 days | > 365 days |
|---|---|---|---|---|
| 52% | 49% | 46% | 36% | 24% |

**Reporting shortly after the issue is introduced is important.**

# Shifting Kernel Fuzzing Left




**Objective:** share results before series are applied to maintainer trees.

# Auto-Triage

Determine the target tree/commit and the affected kernel subsystem(s).

**Baseline approach:** hand-crafted mappings of the form

*CC'd mailing list => { tree, branch, subsystem }.*

Then the system selects tree/branch on which the patch series applies without conflicts (also considering the tree indicated in the subject line).

**The reality is unfortunately more complicated.**

# Auto-Triage: Challenges

- Most patch series don't have the **base-commit** tag.
- Often, series don't actually apply to the trees indicated in the patch subject.
- Some patches depend on other, not yet merged patch series.
- Some series are based on relatively old commits and no longer apply to HEAD.
- Some series apply cleanly, yet the kernel fails to build because of the incompatibilities elsewhere.

The auto-triage process currently fails for **~13%** of incoming patch series.

# Focused Fuzzing

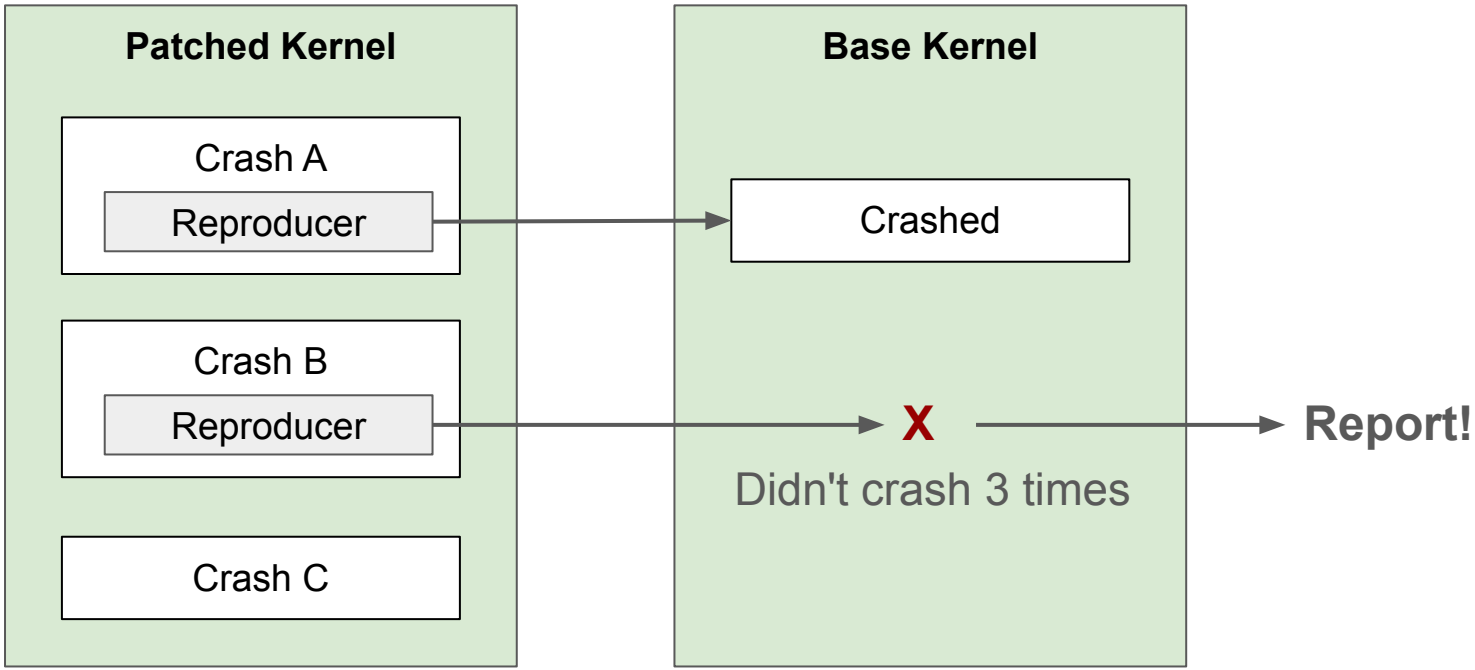
**Prioritized seed selection:**

1. Seeds that cover functions whose object code has changed.
2. Seeds that cover files modified by the patch series.
3. The rest (lowest prio).

Only selected syscalls are fuzzed (depending on triage results).

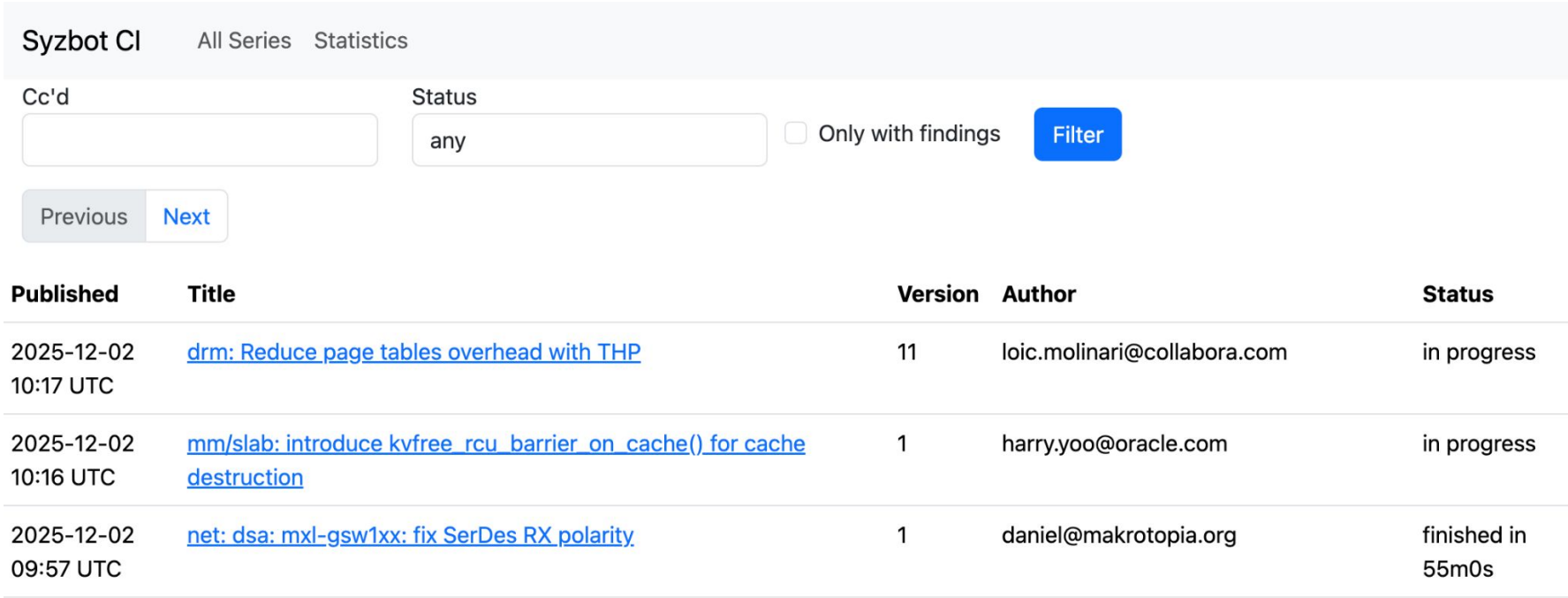
Base program corpuses are taken from syzbot.

# Triage of Findings



# Pilot Deployment (2025)

https://ci.syzbot.org




| Published | Title | Version | Author | Status |
|---|---|---|---|---|
| 2025-12-02 10:17 UTC | drm: Reduce page tables overhead with THP | 11 | loic.molinari@collabora.com | in progress |
| 2025-12-02 10:16 UTC | mm/slab: introduce kvfree_rcu_barrier_on_cache() for cache destruction | 1 | harry.yoo@oracle.com | in progress |
| 2025-12-02 09:57 UTC | net: dsa: mxl-gsw1xx: fix SerDes RX polarity | 1 | daniel@makrotopia.org | finished in 55m0s |

# Current Rollout State (2025)

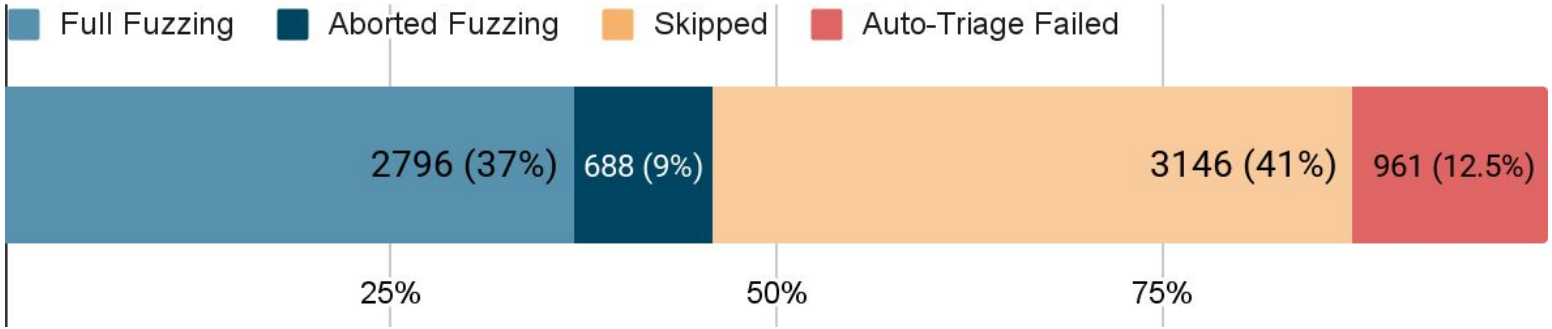
Monitors series from:

- bpf
- io-uring
- kvm
- linux-block
- linux-ext4
- linux-fsdevel
- linux-mm
- linux-unionfs
- linux-wireless
- netdev
- netfilter-devel

# Statistics

Between Aug 2025 and early Dec 2025: **105 findings reported**.

## Per-series statistics:




**Full fuzzing** takes 3 hours, if no patched code is covered in 30 minutes, the session is **aborted**.
Fuzzing is **skipped** if the resulting binaries are identical (no-op change or not enabled in .config).
**Auto-Triage** fails if it cannot find the right base tree/commit.

# Challenges

- Fuzzing is inherently not-deterministic.
  - But we can focus its attention on the modified code paths.
- The current baseline auto-triage approach misses some of the important patch series.
- The overall recall is limited by the need to have reproducers.
  - Try snapshot-based fuzzing that has a much higher reproduction rate?
- The system can only cover as much code as syzbot/syzkaller can, so some series are skipped.

# Plans / Next Steps

- Address the limitations (at least to a reasonable extent).
- Expand the system to cover more mailing lists.
- Run more test utilities on the system?
- Cover LTS backport candidates?
- Fuzz not yet published patch series on demand (even more shift left)?

# syzbot ci

## Continuous Patch Series Fuzzing

Aleksandr Nogikh (Google)
LPC'25 Tokyo, Japan