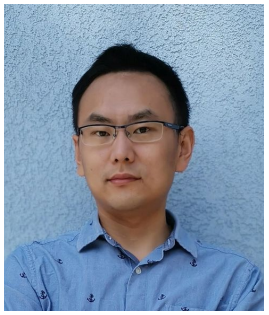
SaTC: CORE: Small: Collaborative: Deep and Efficient Dynamic Analysis of Operating System Kernels

Zhiyun Qian, Ardalan Amiri Sani
UC Riverside, UC Irvine




Challenge:

- **space-time bottlenecks** in kernel fuzzing.
- Space bottlenecks: "Unmet dependencies"
- Time bottlenecks: "Repetitive reboots"

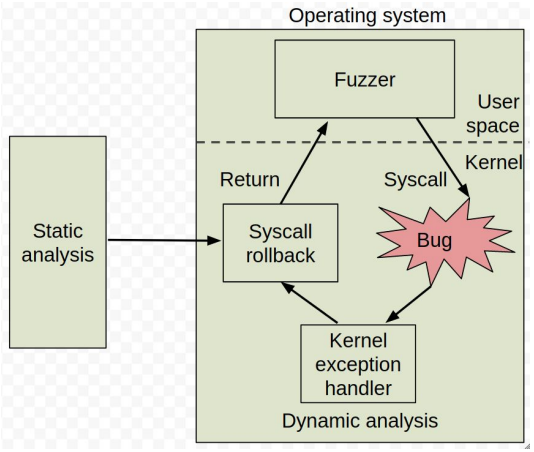
4 different types of kernel modules

792 fuzzing hours * 32 CPU core

115 Unresolved Dependencies sampled

300 human hours

5 Root Causes + unknow category



Solutions:

- Identify [ICSE'22] and overcome dependencies
- Eliminate reboots, e.g., by undoing syscalls [USENIX Security'21]

Scientific Impact:

- Improves the state of the art in kernel fuzzing
- Helps enhance the security of operating system kernels

Broader Impact and Broader Participation:

- Outreach to undergraduate, women, minority, and K-12 students
- Impact and graduate and undergraduate curricula
- Dissemination of research results

NSF Awards #1953932 and #1953933