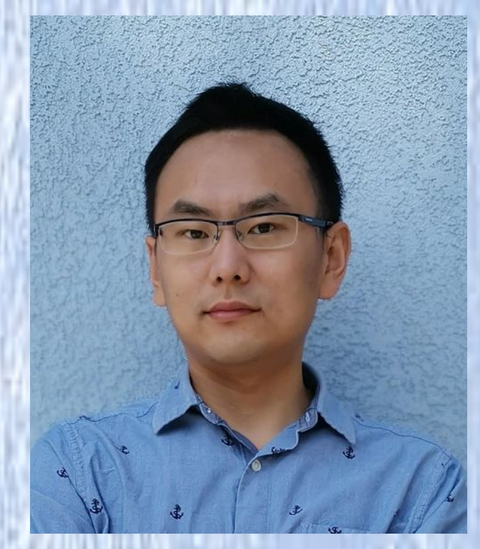
SaTC: CORE: Small: Collaborative: Deep and Efficient Dynamic Analysis of Operating System Kernels

Zhiyun Qian, Ardalan Amiri Sani
UC Riverside, UC Irvine

Awards
#1953932
#1953933



Problem Statement

- Commodity operating system kernel contain many bugs and vulnerabilities.
- Fuzzing is an effective dynamic analysis technique that can find many of these bugs and vulnerabilities..
- This Award identifies and attempts to solve critical bottlenecks unique to kernel fuzzing, which are referred to as **space-time bottlenecks**.
- Space bottlenecks prevent the fuzzer from reaching desired code blocks and triggering potential vulnerabilities. “Unmet dependencies in the kernel” are important space bottlenecks.
- Time bottlenecks force the fuzzer to stop its execution for some period of time, resulting in wasted fuzz time. “Repetitive reboots” are an important time bottleneck unique to kernel fuzzers.

Solutions

- **Research thrust 1: Dependency-Oriented Fuzzing**
  - Some notable results so far: Understanding the dependency challenge in kernel fuzzing [ICSE’22]

4 different types of kernel modules

792 fuzzing hours * 32 CPU core

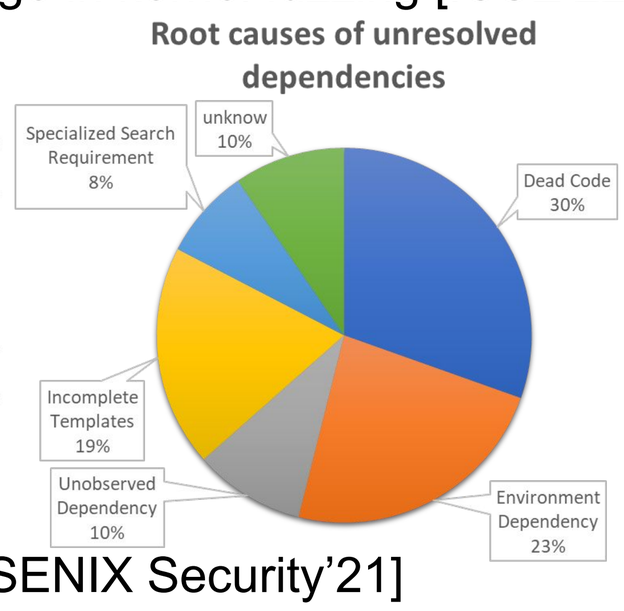
115 Unresolved Dependencies sampled

300 human hours

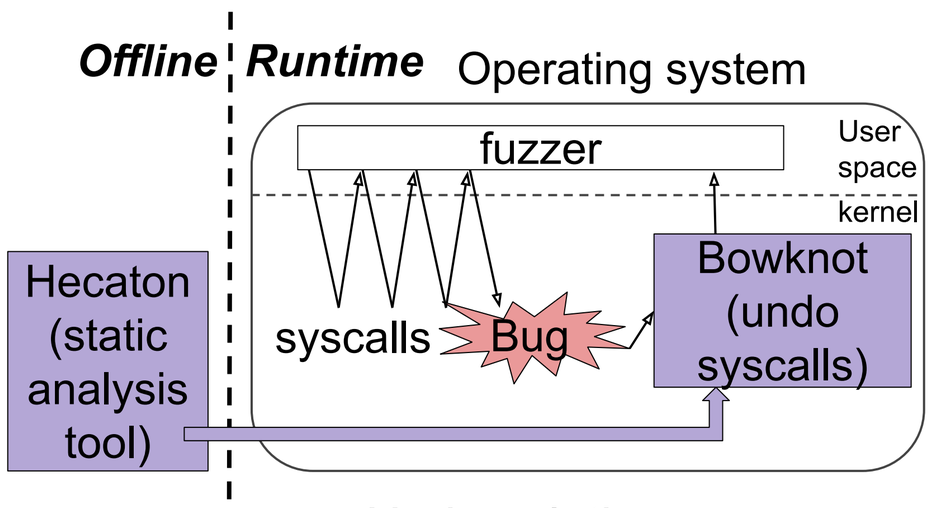
5 Root Causes + unknow category

Table 5: Prevalence of unresolved dependencies

Name	#UncoveredE/#E	#UD/#UC	#DomE_{UD}/#DomE_{UC}
cdrom	615/915 (67%)	37/54 (69%)	80/122 (99%)
snd_seq	7355/9255 (79%)	162/274 (59%)	204/356 (57%)
ptmx	3541/5105 (69%)	254/289 (88%)	763/830 (92%)
kvm	15471/28516(54%)	1554/2050(76%)	4073/5677(72%)
Sum	26982/43791(62%)	2007/2667(75%)	5106/8037(73%)

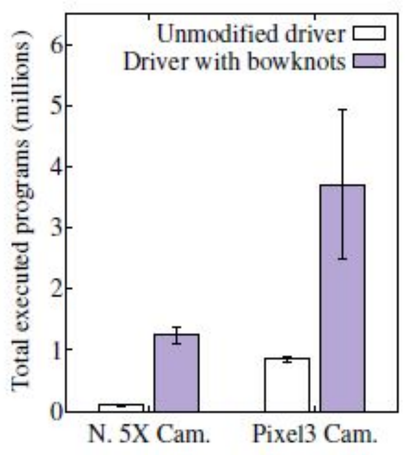


- **Research thrust 2: Reboot-Free Fuzzing**
  - Some notable results so far: Undo syscalls that result in a reboot [USENIX Security’21]

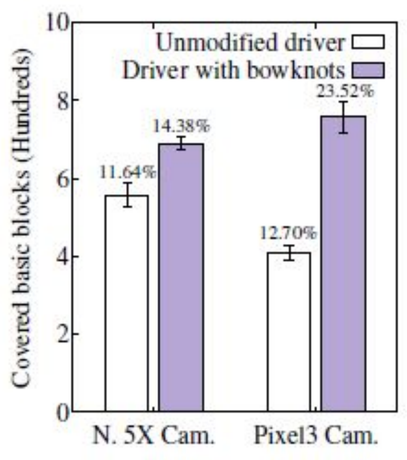


Undo solution

Fuzzing setup



#Fuzzing programs



Coverage

Broader Impacts

- Impacts on global societies and economies by securing operating system kernels
- Dissemination of research results
- Impact and graduate and undergraduate curricula
- Outreach to undergraduate, women, minority, and K-12 students