Beta Presentation
Android Exploit Fuzzing Analysis
The Capstone Experience
Team Google
Anurag Kompalli
Catherine Xu
Karan Singh
Michael Umanskiy
Romario Rranza
Shubham Chandna
Department of Computer Science and Engineering
Michigan State University
Fall 2022
Project Sponsor Overview

• Google – Tech
  ▪ Founded: Menlo Park, CA in 1998
    o Larry Page
    o Detroit, MI; Seattle, WA
    o 50 Countries; 70 Offices
  ▪ Main Product: Search Engine
  ▪ Revenue Source: Ad services
  ▪ Internet connectivity; Smart devices
    o Google Chrome, Google Home
  ▪ Developer of Android OS
Project Overview

• Problems:
  1. While syzkaller detects bugs in Android OS, the software is constantly evolving and needs improvement
  2. Fuzzing performance can be variable, depending on the configuration

• Solutions:
  ▪ Visualize bugs in the Android kernel intuitively
  ▪ Extending syzkaller descriptions
  ▪ Running multiple syzkaller instances with custom configuration
System Architecture

Backend

- {syzlang}
  - Descriptions
  - Syzkaller
    - syz-executor
    - syz-fuzzer
    - inputs
    - RPC
    - syscalls
  - QEMU
  - Android

REST API

- Node.js
- Docker

Frontend

- Angular
- User

The Capstone Experience
Team Google Beta Presentation
Dashboard

- **CrashTypes**: 1
- **Lines Covered**: 46k
- **Syscalls**: 2135
- **Uptime [min]**: 53

**Latest Crash**
```
kernelBUG in sys_trace
```

**Logs**
- 2022/11/13 19:56:40 minimized corpus: 2272 --> 2115
- 2022/11/13 19:56:40 fuzzer vm-8 connected
- 2022/11/13 19:56:29 loop: phase=4 shutdown=false instances=0/1
- repro: pending=0 reproducing=0 queued=0
- 2022/11/13 19:56:29 loop: starting instance 0
Orchestration

---

### Orchestration Table

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Port</th>
<th>Instance ID</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dev</td>
<td>8000</td>
<td>e18de8574629</td>
<td>Make Default</td>
</tr>
<tr>
<td>2</td>
<td>file_subsystem</td>
<td>8001</td>
<td>b0f51884e646</td>
<td>Make Default</td>
</tr>
<tr>
<td>3</td>
<td>binder_fops</td>
<td>8002</td>
<td>4b1a8a18b0cad2</td>
<td>Make Default</td>
</tr>
<tr>
<td>4</td>
<td>fix</td>
<td>8003</td>
<td>317d83437314</td>
<td>Make Default</td>
</tr>
</tbody>
</table>

---

- **Dashboard**: Syzkaller
- **Orchestration**: Syzkaller
- **Crashes**: Syzkaller
- **Insights**: Syzkaller

---

The Capstone Experience

Team Google Beta Presentation
Crashes

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Count</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>kernel BUG in sys_ptrace</td>
<td>3</td>
<td>2022-11-13 20:22:11.095416769 +0000 UTC</td>
</tr>
</tbody>
</table>
What’s left to do?

• Features
• Stretch Goals
  ▪ CPU Utilization
  ▪ Make Syzkaller Run on Google Cloud Engine
  ▪ Analyze exploits to Write Descriptions
  ▪ Write more Binder IPC Descriptions
• Other Tasks
  ▪ Aesthetic fixes for Orchestration Tab
Questions?