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

• Fuzzing: Black box software testing technique
  ▪ Inputs malformed data to find implementation bugs
  ▪ State-of-the-art-tool: Syzkaller

• Descriptions: Interface that uses syzkaller fuzzing to detect bugs by passing inputs to the kernel.
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**

- **Syzkaller**
  - syz-executor
  - syz-fuzzer
  - syz-manager

- **QEMU**
  - syzlang
  - syscalls

**Frontend**

- **User**

**Connections**

- Descriptions
- RPC
- REST API

**Tools**

- Node.js
- Docker
Dashboard Page

The Syzkaller Dashboard page displays the following metrics:

- **CrashTypes**: 0
- **Lines Covered**: 50,000
- **Syscalls**: 2,123
- **Uptime [min]**: 76

The dashboard also includes a timeline graph showing coverage over time, with a red shaded area indicating increased coverage. The latest crash status is indicated as "No Crashes Yet!".
Orchestration Tab

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Port</th>
<th>Instance ID</th>
<th>Actions</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>prod</td>
<td>8080</td>
<td>143ff68b19cc</td>
<td>Make Default, Remove</td>
<td></td>
</tr>
</tbody>
</table>
Insights Tab: Syscall Inspector
Insights Tab

The Capstone Experience

Team Google Alpha Presentation
What’s left to do?

• Work on the Crashes tab to display the latest crashes and their reports
• Write more descriptions for syzkaller
• Enable custom configurations for syzkaller in the Orchestration tab
• Add more visualizations to the Insights tab relating to the Corpus and VM Utilization
Questions?