MICHIGAN STATE
UNIVERSITY

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

From Students…
…to Professionals

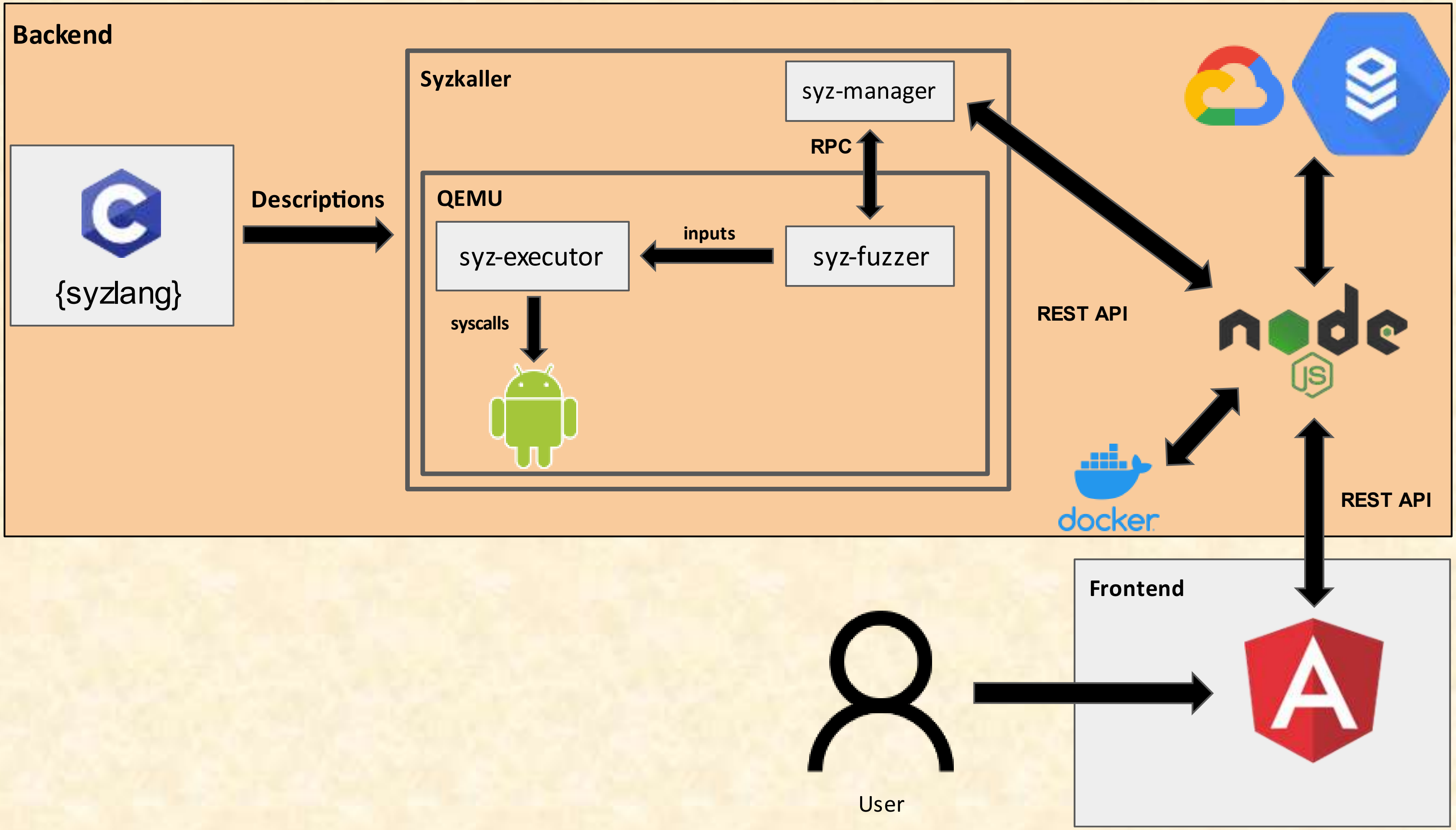
Project Sponsor Overview

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

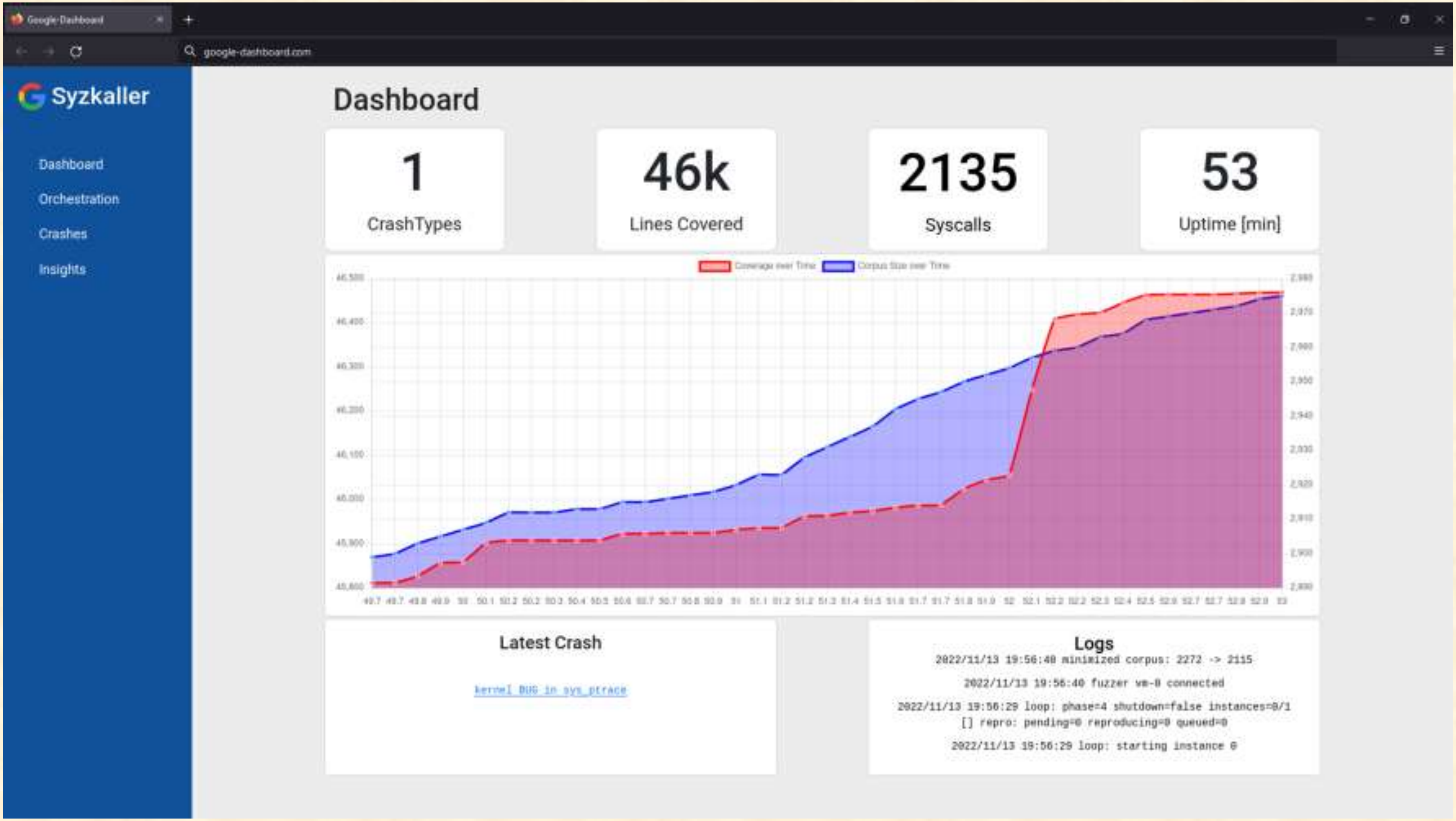
Project Overview

- 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



Dashboard



Dashboard

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

Latest Crash

kernel BUG in sys_ptrace

Logs

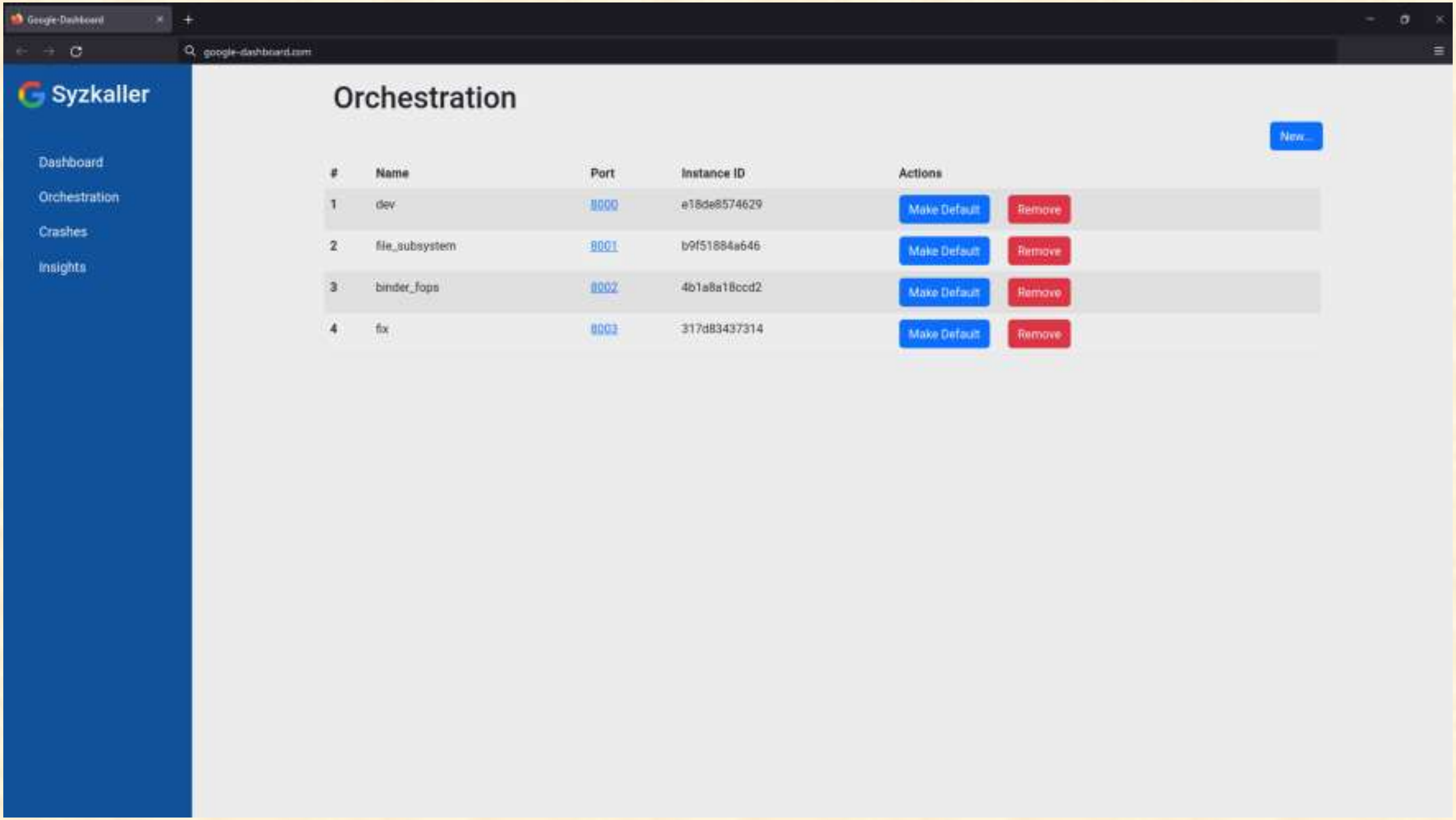
```
2022/11/13 19:56:40 minimized corpus: 2272 -> 2115

2022/11/13 19:56:40 fuzzer vm-0 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
```

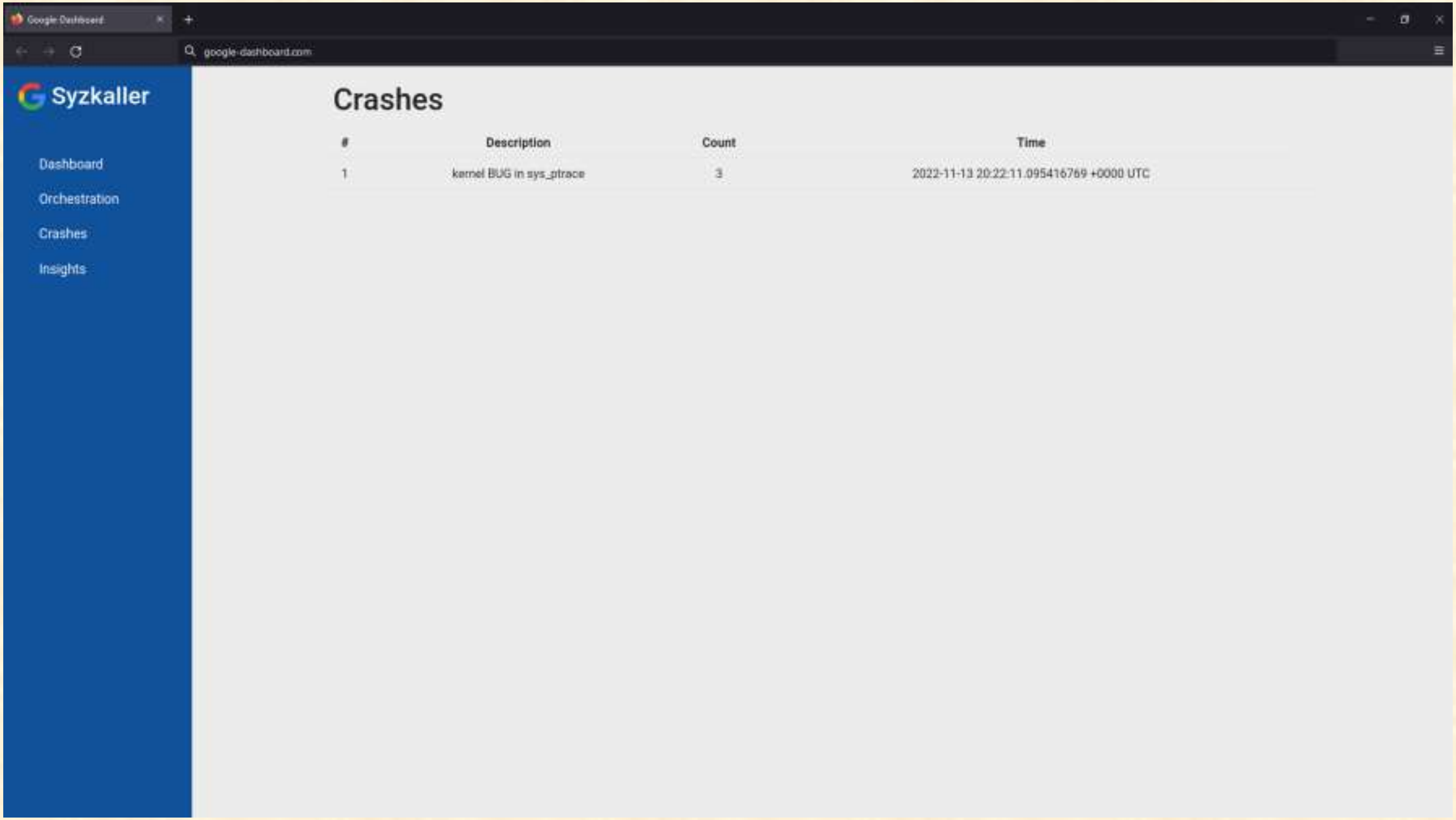
Orchestration



Orchestration

#	Name	Port	Instance ID	Actions
1	dev	8000	e18de8574629	Make Default Remove
2	file_subsystem	8001	b9f51884a646	Make Default Remove
3	binder_fops	8002	4b1a8a18ccd2	Make Default Remove
4	fix	8003	317d83437314	Make Default Remove

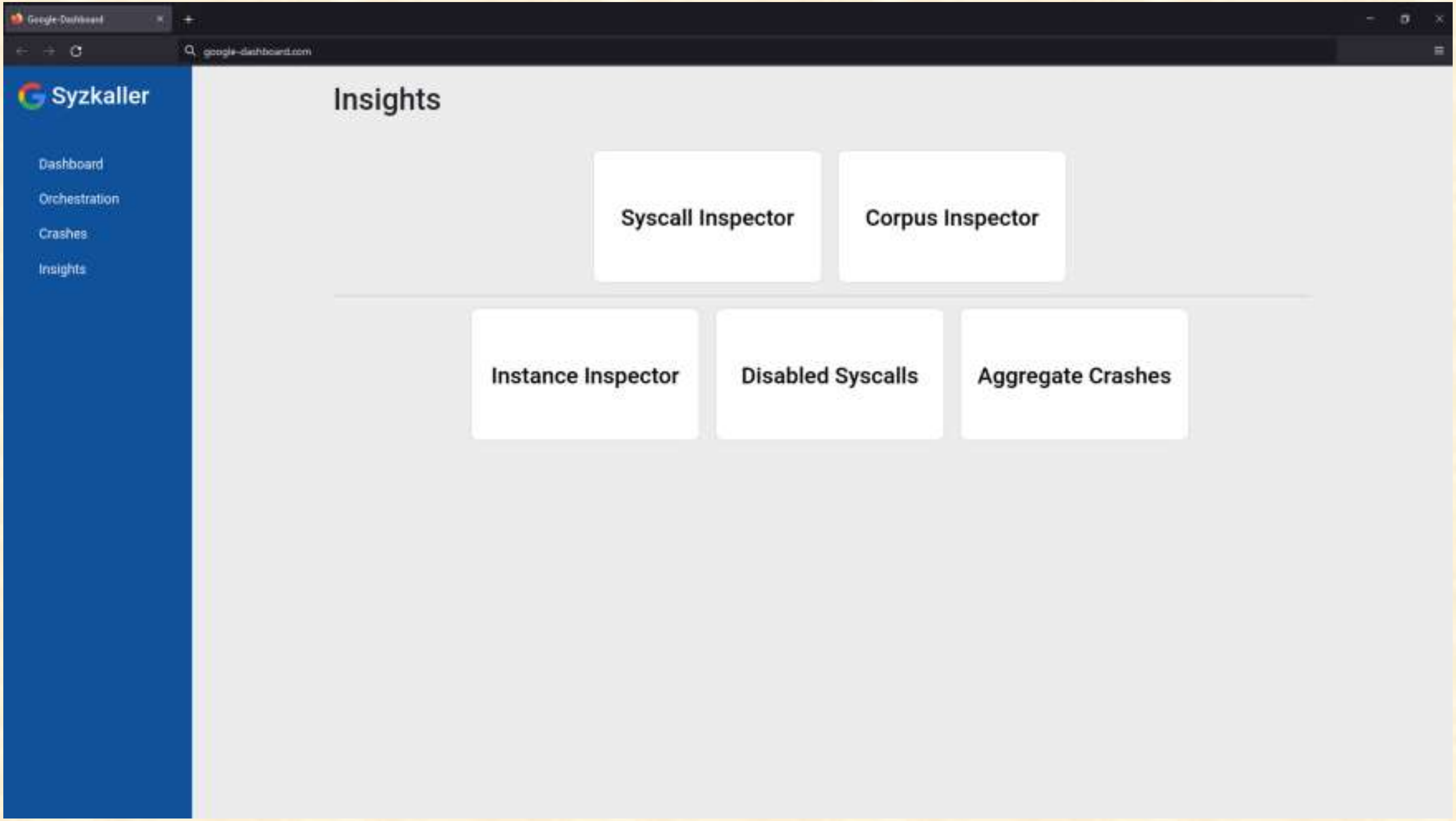
Crashes



Crashes

#	Description	Count	Time
1	kernel BUG in sys_ptrace	3	2022-11-13 20:22:11.095416769 +0000 UTC

Insights


Google-Dashboard
google-dashboard.com
Syzkaller
Dashboard
Orchestration
Crashes
Insights
Insights
Syscall Inspector
Corpus Inspector
Instance Inspector
Disabled Syscalls
Aggregate Crashes

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?

? ? ? ?

? ?

? ? ?