



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



*From Students...
...to Professionals*

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.

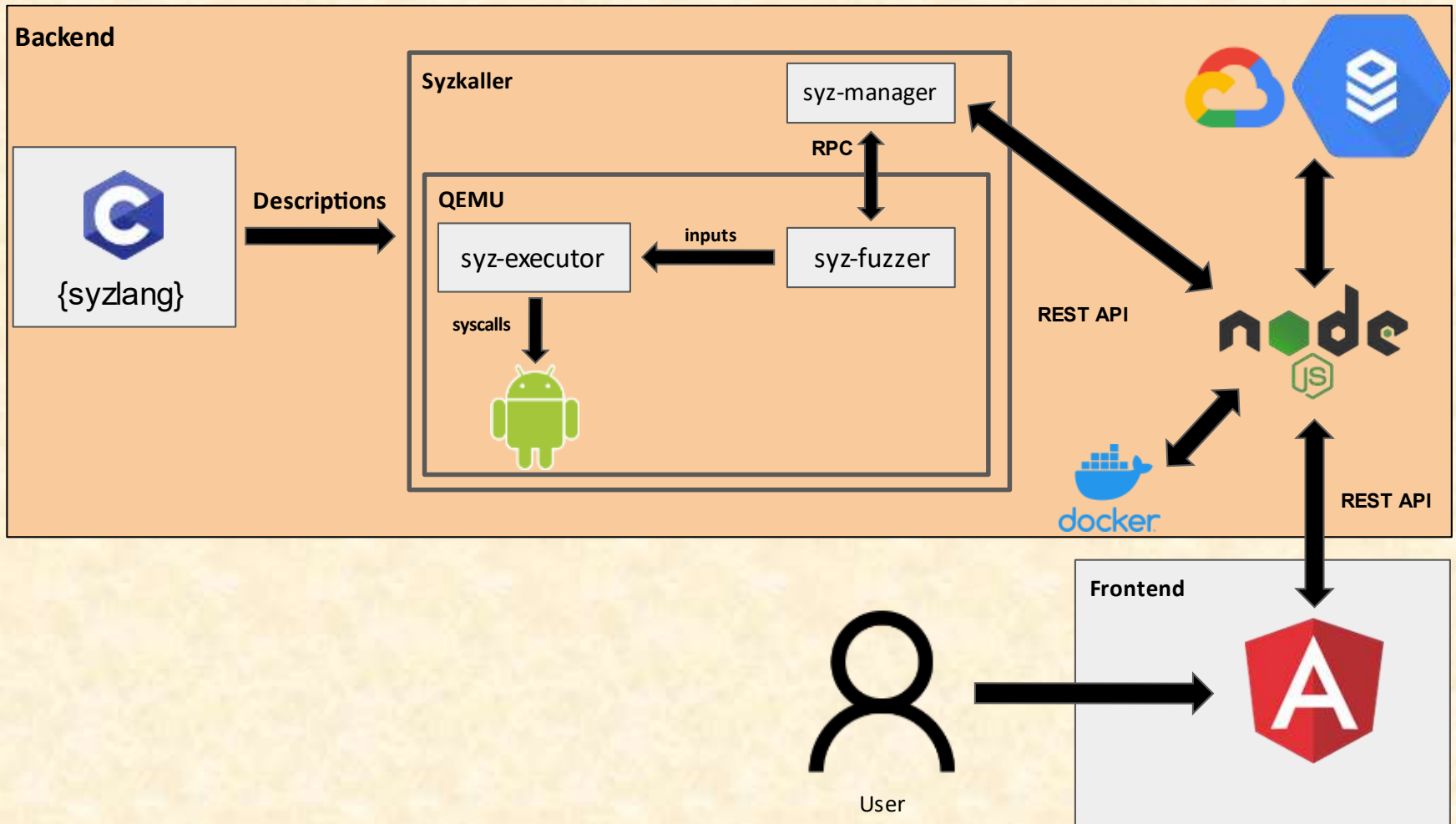


Project Overview

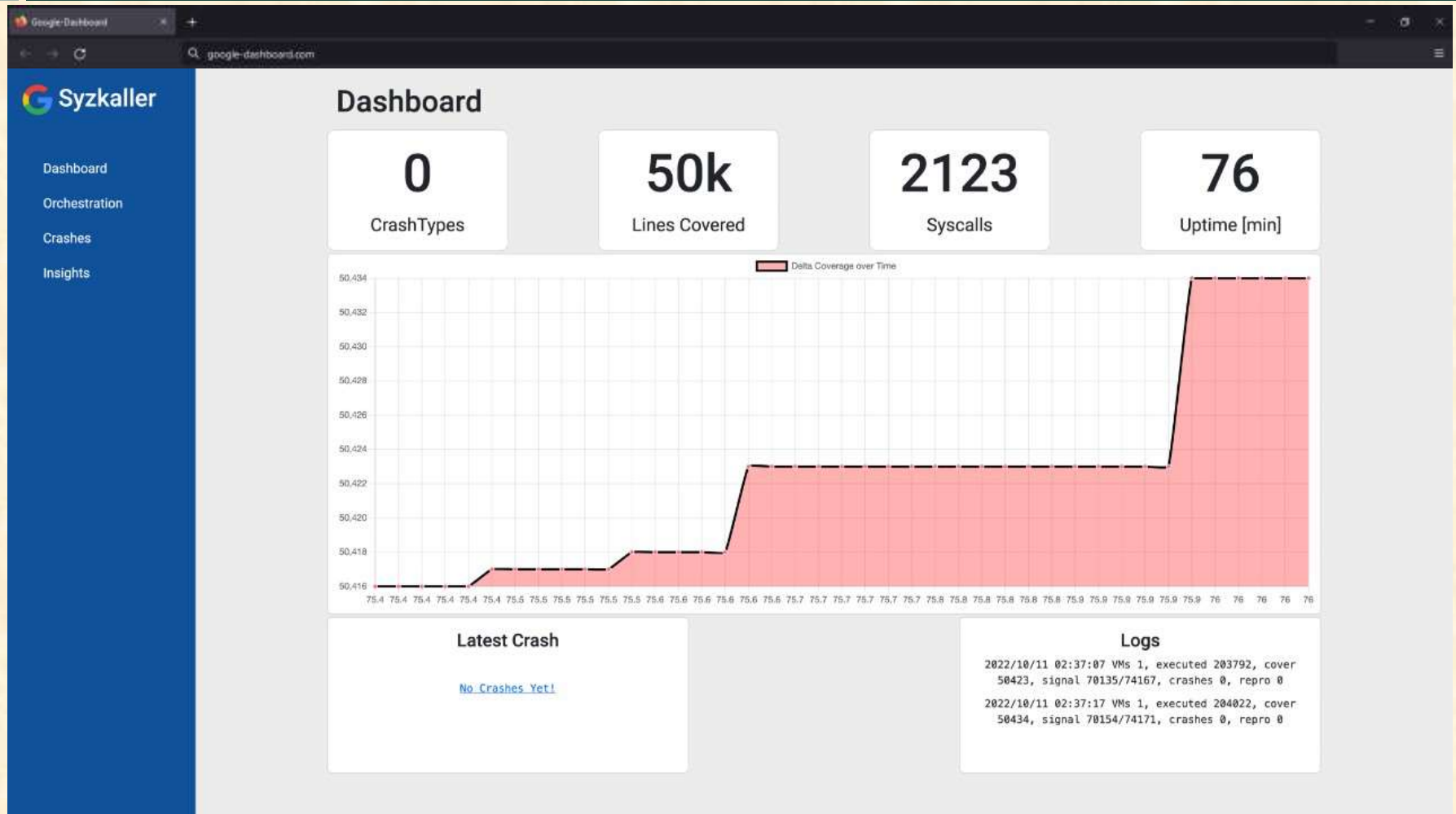
- Problems:
 1. While syzkaller detects bugs in Android OS, the software is constantly evolving and needs improvement
 2. Fuzzing performance can be variable, depending on the configuration
- Solutions:
 - Visualize bugs in the Android kernel intuitively
 - Extending syzkaller descriptions
 - Running multiple syzkaller instances with custom configuration



System Architecture



Dashboard Page



Orchestration Tab

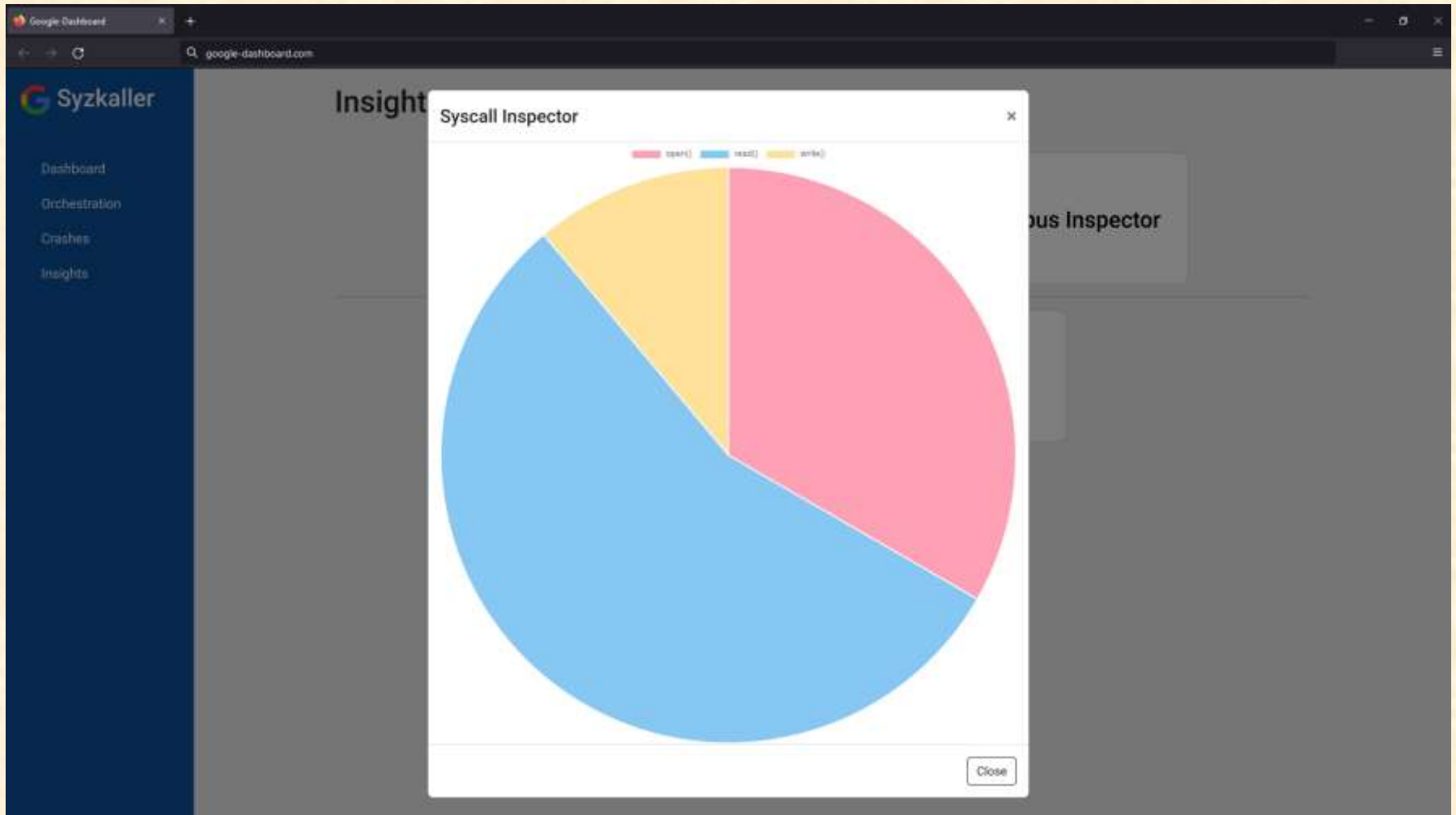
The screenshot shows a web browser window with the address bar displaying 'google-dashboards.com'. The page title is 'Orchestration'. On the left, a blue sidebar contains the Syzkaller logo and a navigation menu with links to 'Dashboard', 'Orchestration', 'Crashes', and 'Insights'. The main content area features a table with the following data:

#	Name	Port	Instance ID	Actions	Status
1	prod	8003	143ff68b19cc	Make Default Remove	

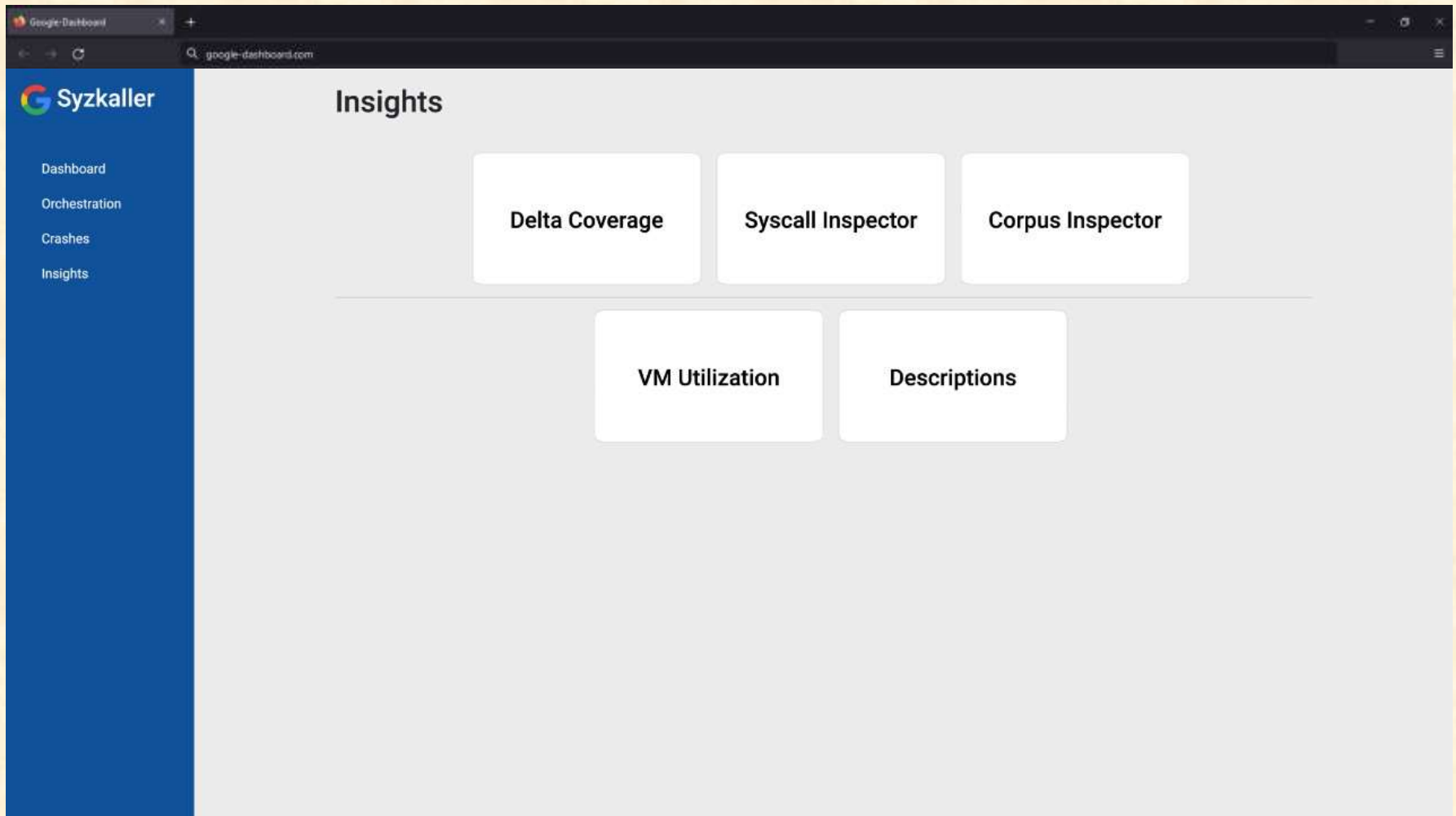
A 'New...' button is located in the top right corner of the main content area.



Insights Tab: Syscall Inspector



Insights Tab



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?

?

?

?

?

?

?

?

?

?

