NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

School of Computer Science and Engineering
College of Engineering

Optimizing Grey-Box Mutational Fuzzing Workflow for Effective Vulnerability Discovery

Student: Chew Kin Zhong **Supervisor:** Prof Liu Yang

Project Objectives

- Develop tools to optimise fuzzing workflow & ease fuzzer performance evaluation
- Evaluate the performance of common fuzzing techniques & research best practices for fuzzing
- Contribute to the open-source community by finding vulnerabilities in open-source projects

Developed Tools

Test Case Optimiser

- Merges multiple seed optimisation processes
- Utilises parallelisation to improve performance

Automated Crash Analyser

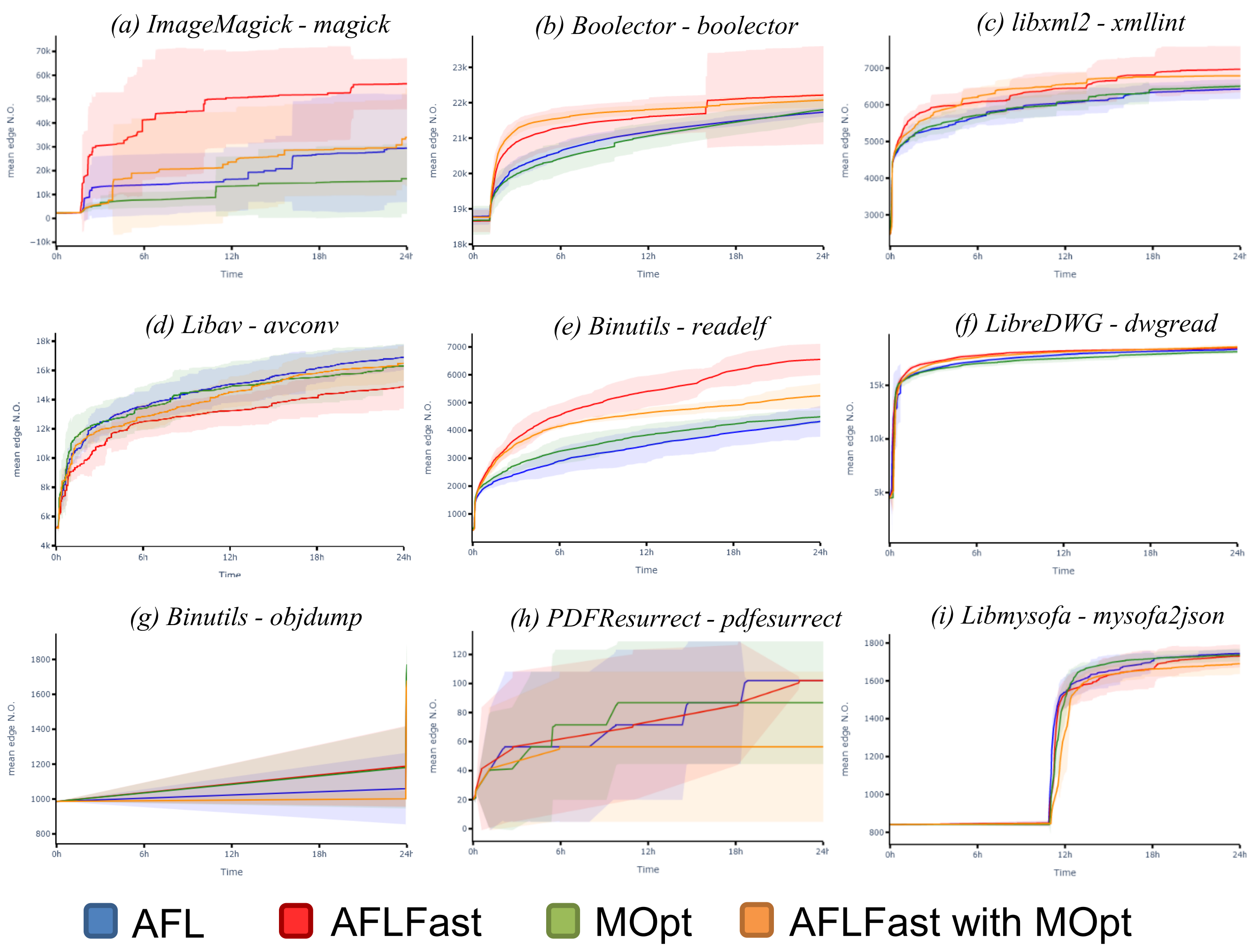
- Automates crash triaging by accurately classify crashes from fuzzing output
- Performs crash bucketing to reduce the number of duplicated bugs
- Identifies actionable vulnerabilities to be reported to relevant parties

Fuzzing Performance Visualiser

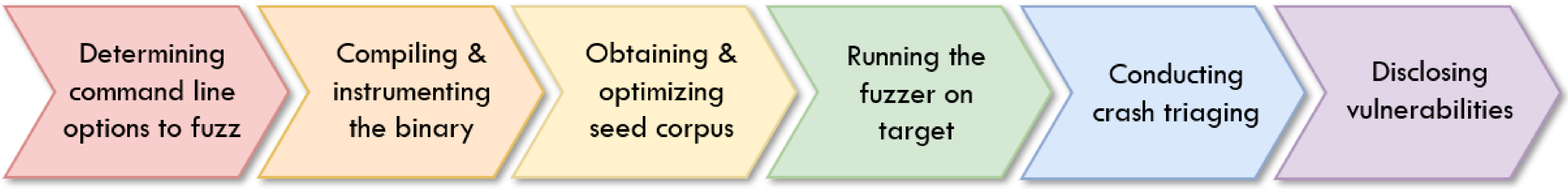
- Creates highly configurable and interactive visualisations from performance data

Evaluation of Fuzzing Techniques

Mean edge coverage growth over time



Proposed Fuzzing Methodology


Determining command line options to fuzz
Compiling & instrumenting the binary
Obtaining & optimizing seed corpus
Running the fuzzer on target
Conducting crash triaging
Disclosing vulnerabilities

Incorporates the developed tools, the evaluation results, and the current best practices

Fuzzing Real-World Applications

Fuzzing was conducted on various open-source projects. Responsible vulnerability disclosure was applied. 11 CVE ID requests are currently pending review.

Library	Unique Vulnerabilities Discovered	Assigned CVE
PDFResurrect	0	-
Libmysofa	1	1 CVE pending
LibreDWG	31	8 CVEs pending
Boolector	4	1 CVE pending
FFjpeg	1	1 CVE pending
FFmpeg	0	-