

Automatic exploit generation

Maxime, Manh-Dung, Tristan, Emilien, Gabriel + noms
Supervision: Jules - Facebook

REDOCS 2020

October 29, 2020

Introduction

Work given by Facebook

Problem Overview

Context

- Bugs in devices
- Are they weaknesses ?

Formal challenge

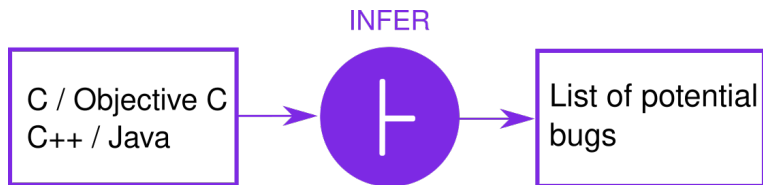
Can we automatically turn static analysis reports into executable confirming the vulnerability of a program ?



Section example

Give an example of main.c with a bug We can show pictures or live performance. Ask the audience to detect the bug.

Infer tool



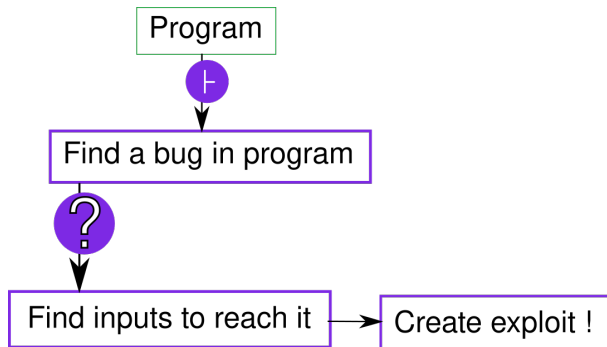


- Static analysis tool from Facebook
- **Capture** phase, then **Analysis** phase

Infer tool example

Give an example of our use of Infer on main.c We can show pictures or live performance.

Challenge approach



Challenge approach

Practical challenge

Given the Infer information about bugs of a program A, create a program B that crashes A

Table of content

1 Problem overview

- Context
- Infer tool
- Challenge approach

2 Proposed approaches

- Model checking
- SMT solvers/ SAT solver
- Fuzzing technique

3 Results and Future work

- Results
- Future Work

Proposed approaches

Model checking

Present model checking solution with Divine

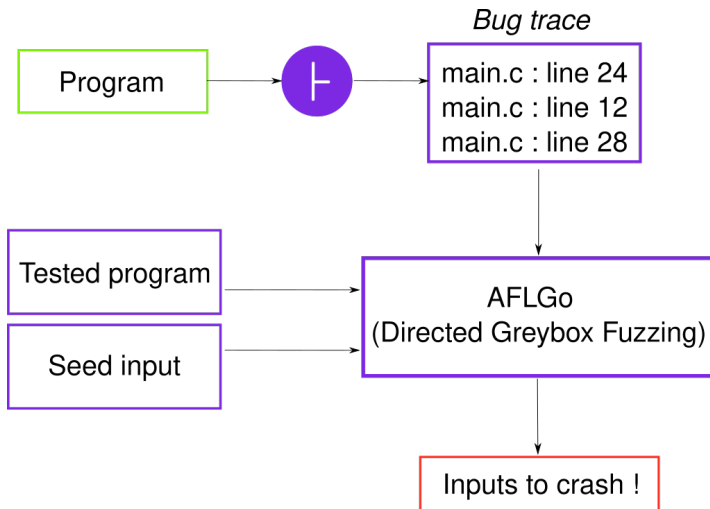
SMT / SAT solvers

Present logic solvers

Fuzzing technique

Present fuzzing techniques

Fuzzing technique



Results and future work

Results

Show a table approaches / program comparing results (yes/no, running time, implementation complexity, computational complexity)
Show some exploits results ?

Future work

Put eeeeeverything we think of. Ex

- Create a fully automatic process
- Find automatic ways to generate exploits

Thank you Questions ?

See the title