

Automatic exploit generation

Maxime Bélair ¹ Manh-Dung Nguyen ² Emilien Fournier ³
Tristan Benoit ⁴ Gabriel Sauger ⁵

Subject by: Jules Villard -



¹Orange Labs / IMT atlantique - maxime.belair@imt-atlantique.fr

²CEA LIST & Université Grenoble Alpes - manh-dung.nguyen@cea.fr

³ENSTA Bretagne / Lab-STICC - emilien.fournier@ensta-bretagne.org

⁴LORIA - tristan.benoit@loria.fr

⁵LORIA - gabriel.sauger@loria.fr

Problem Overview

Context

- Bugs in devices
- Are they weaknesses ?



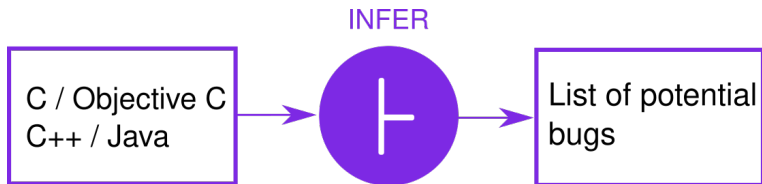
Formal challenge

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



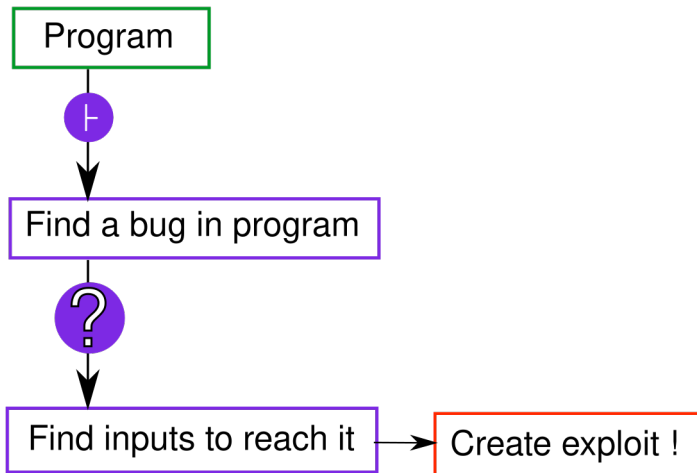


- Static analysis tool from Facebook
- **Capture** phase, then **Analysis** phase

Infer tool example

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

Practical approach



Practical 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
- Practical approach

2 Proposed approaches

- Model checking
- SMT solvers
- Fuzzing technique

3 Conclusions and perspectives

- Results comparison
- Future Work

proposed approaches

Model checking

Present model checking solution with Divine

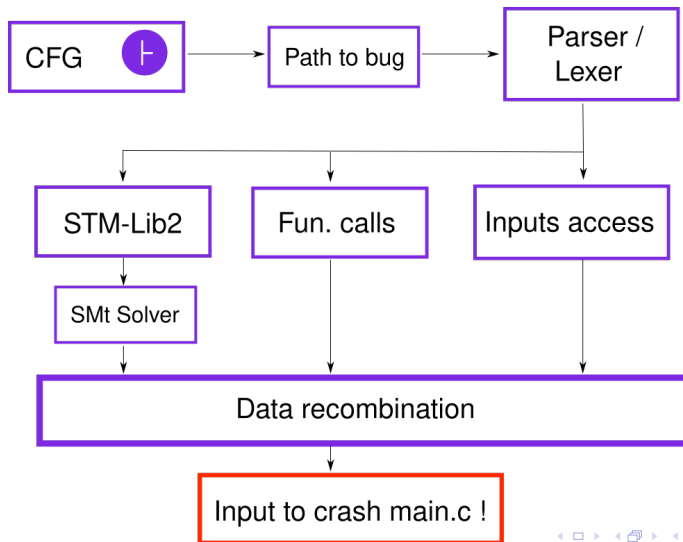
SMT solvers

Present logic solvers

SMT Solvers

Compiler / Interpreter information

SMT Solver



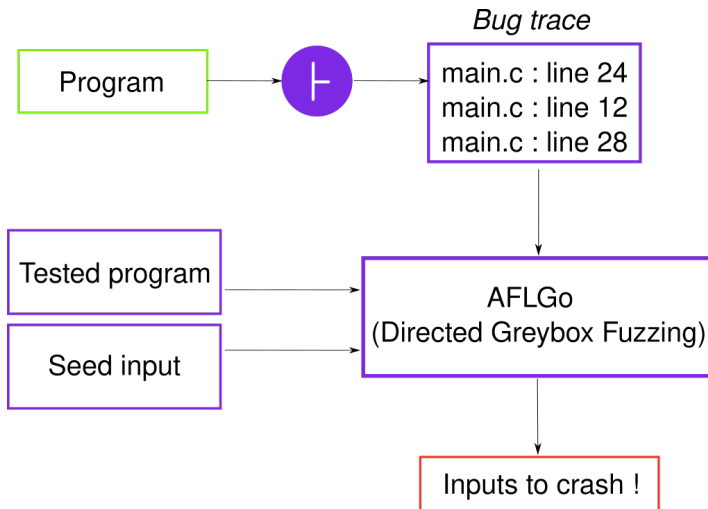
SMT results

Present the results we have and on which program. The performance review is NOT done here, but in Part 3/Result Comparison

Fuzzing technique

Present fuzzing techniques

Fuzzing technique



Conclusions and perspectives

Results comparison

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

Future work

Put eeeeeverything we think of. Ex:

- Generate
- Create a fully automatic process
- Find automatic ways to generate exploits (using dictionary like attacks)

Thank you Questions ?

See the title