Automatic exploit generation

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

Subject by: Jules Villard - 

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

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

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

[4]LORIA - tristan.benoit@loria.fr

[5]LORIA - gabriel.sauger@loria.fr

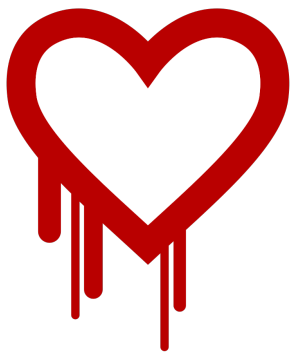
Problem Overview

Context

- Bugs in devices
- Are they weaknesses ?

Formal challenge

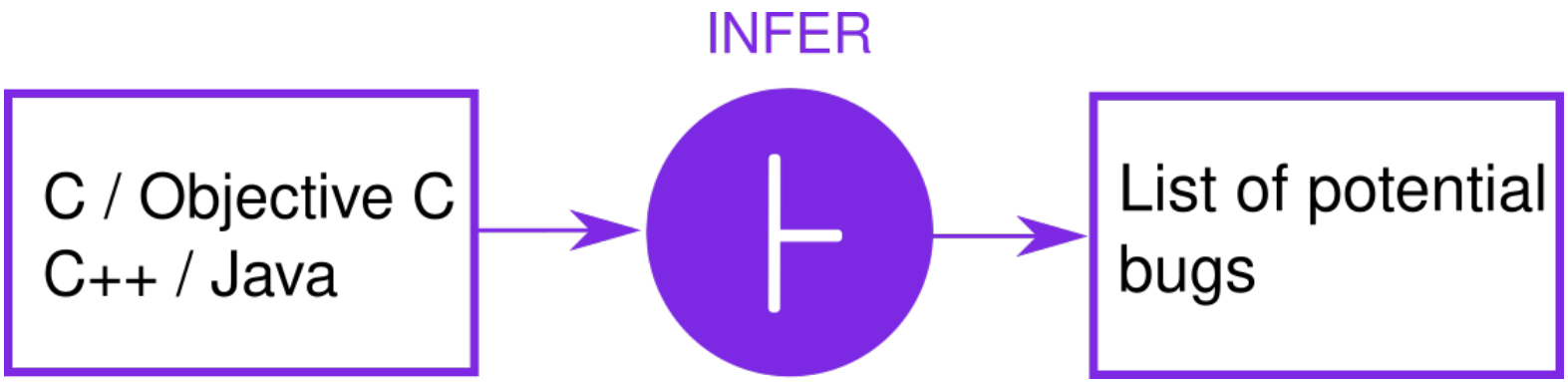
Can we automatically turn static analysis reports into executable confirming the vulnerability of a program ?



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

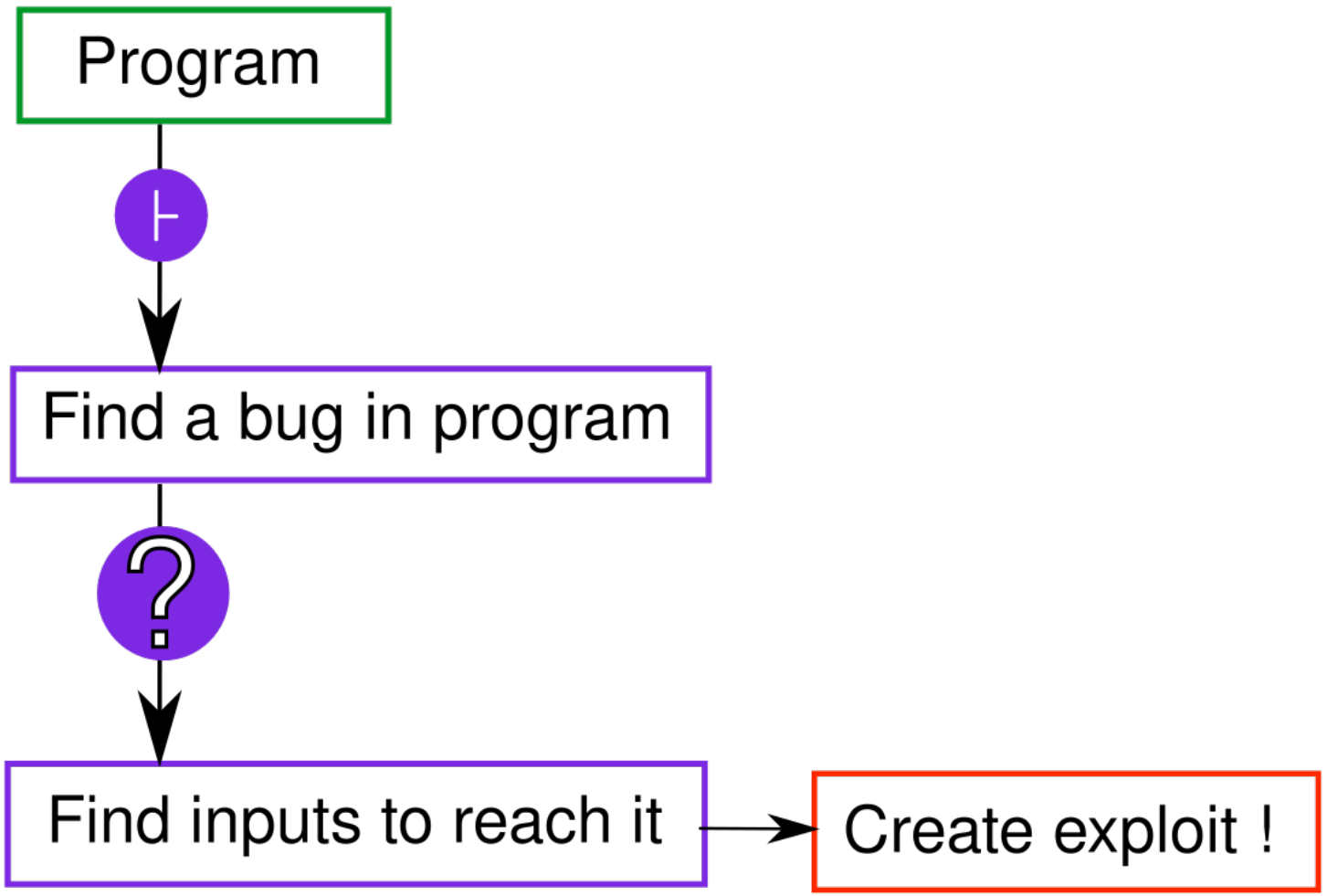


- Static analysis tool from Facebook
- **Capture** phase, then **Analysis** phase

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

Proposed approaches

Model checking

Present model checking solution with Divine

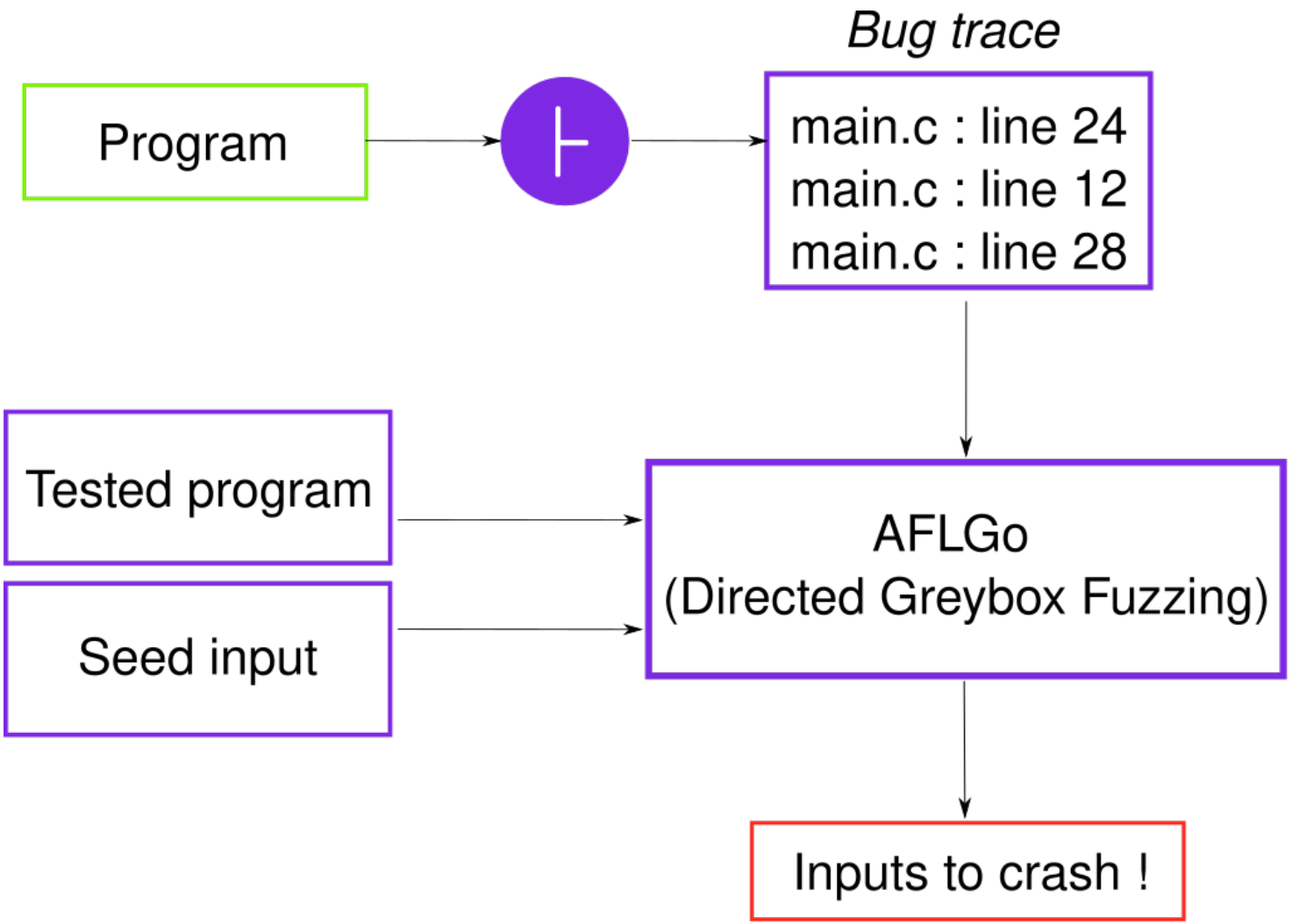
SMT / SAT solvers

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