Maintaining Magma
A Ground-Truth Fuzzing Benchmark

Sara Vaccino, Qiang Liu, Mathias Payer, EPFL

Motivation

Software is full of bugs. Many bug-finding methods have been created to fight this issue. We evaluate these methods, by testing them on real-life bugs.

Challenge: Can real-life bugs be triggered?

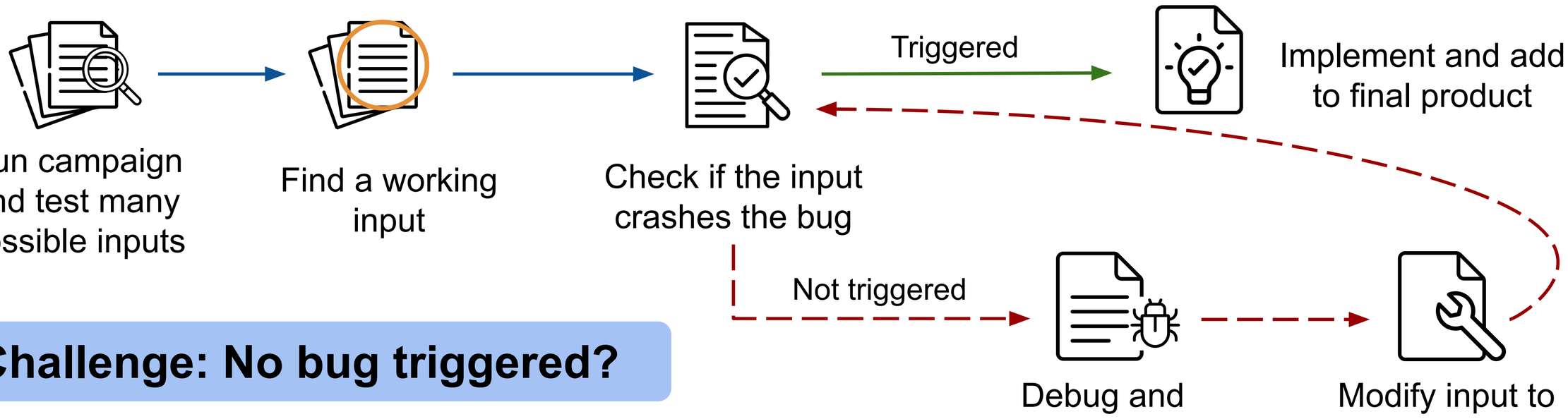
Goal: Provide proof that these bugs are reproducible.

Background

Magma is a benchmark evaluating a specific type of bug-finding methods, called fuzzers.

To test a program, a fuzzer generates an input, modifies the input randomly, and feeds the input to the program in hopes to find new bugs. This process is repeated multiple times to increase the coverage.

Methodology

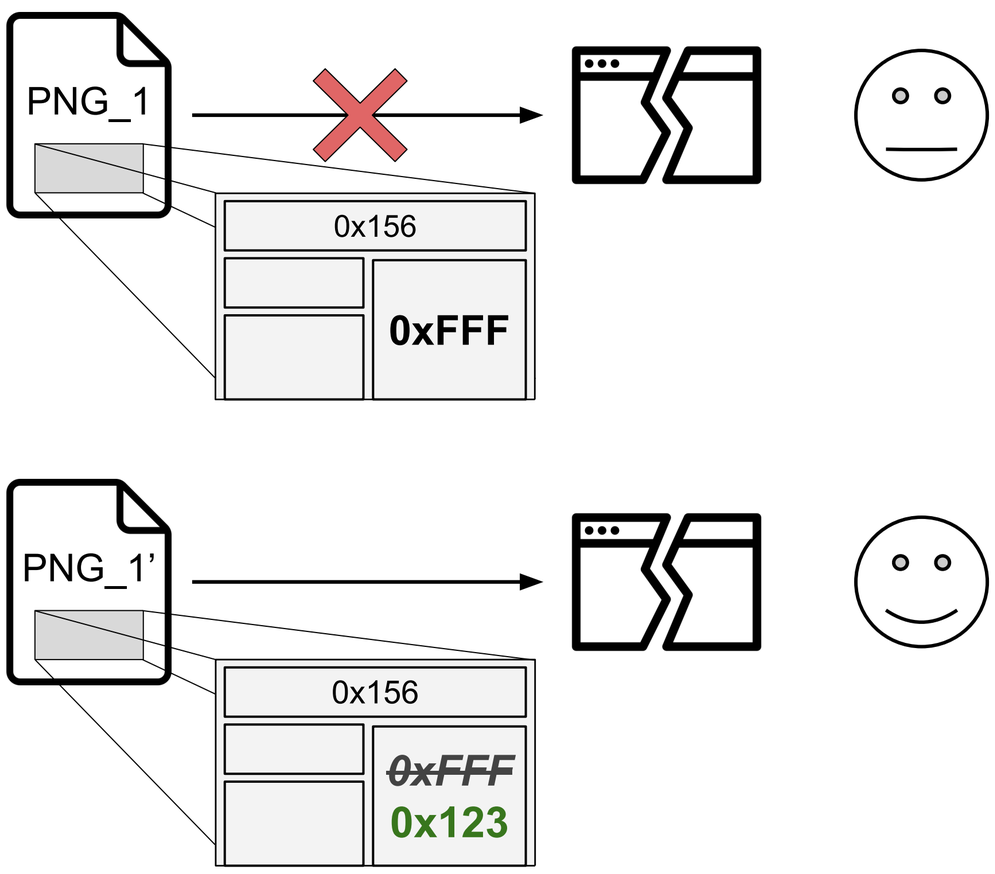


Challenge: No bug triggered?

Problem: Program does not crash

Goal: Find input that breaks the program

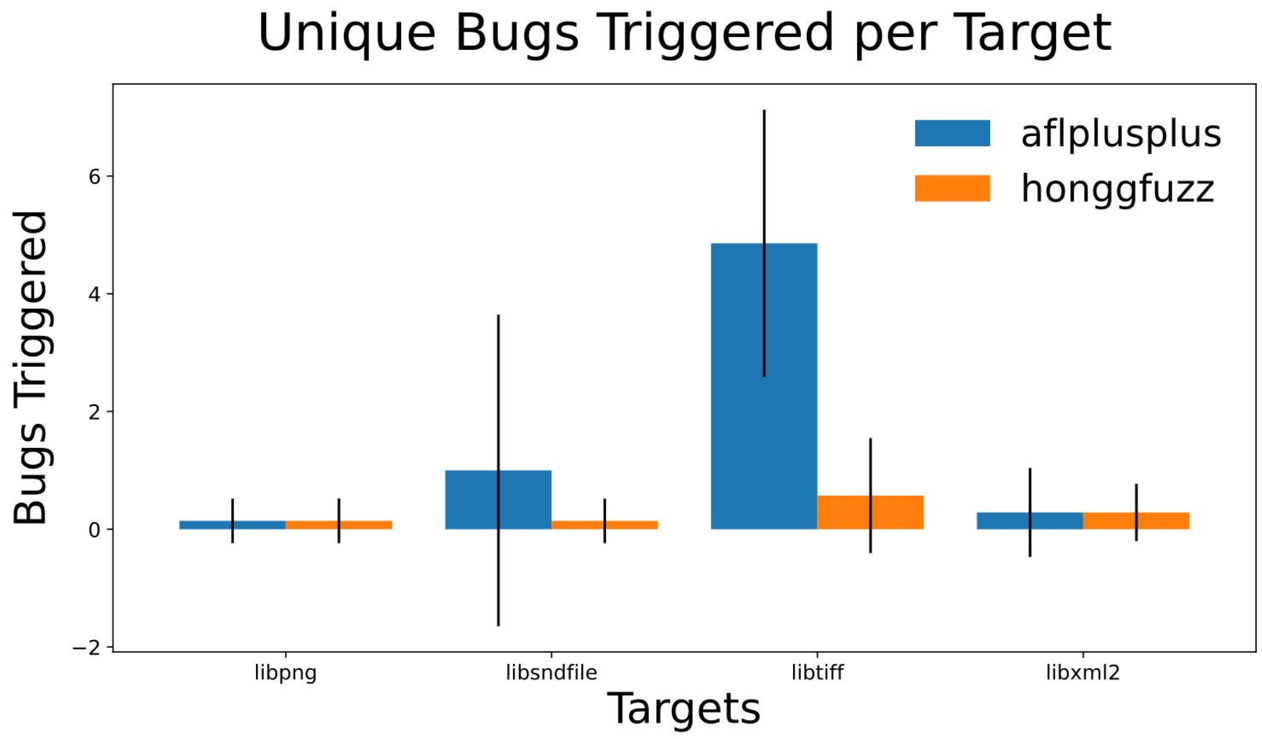
Solution: Change some bytes in the input



Results

7 Proof-of-Concepts implemented, 5 in progress.

We evaluated two fuzzers using the improved version of Magma and showed the number of unique bugs triggered per target.



Future Work

➔ Finish collecting the Proof-of-Concepts to trigger the injected bugs

➔ Potentially automate valid input construction

To Magma!

The diagrams on this poster have been designed using resources from Flaticon.com.