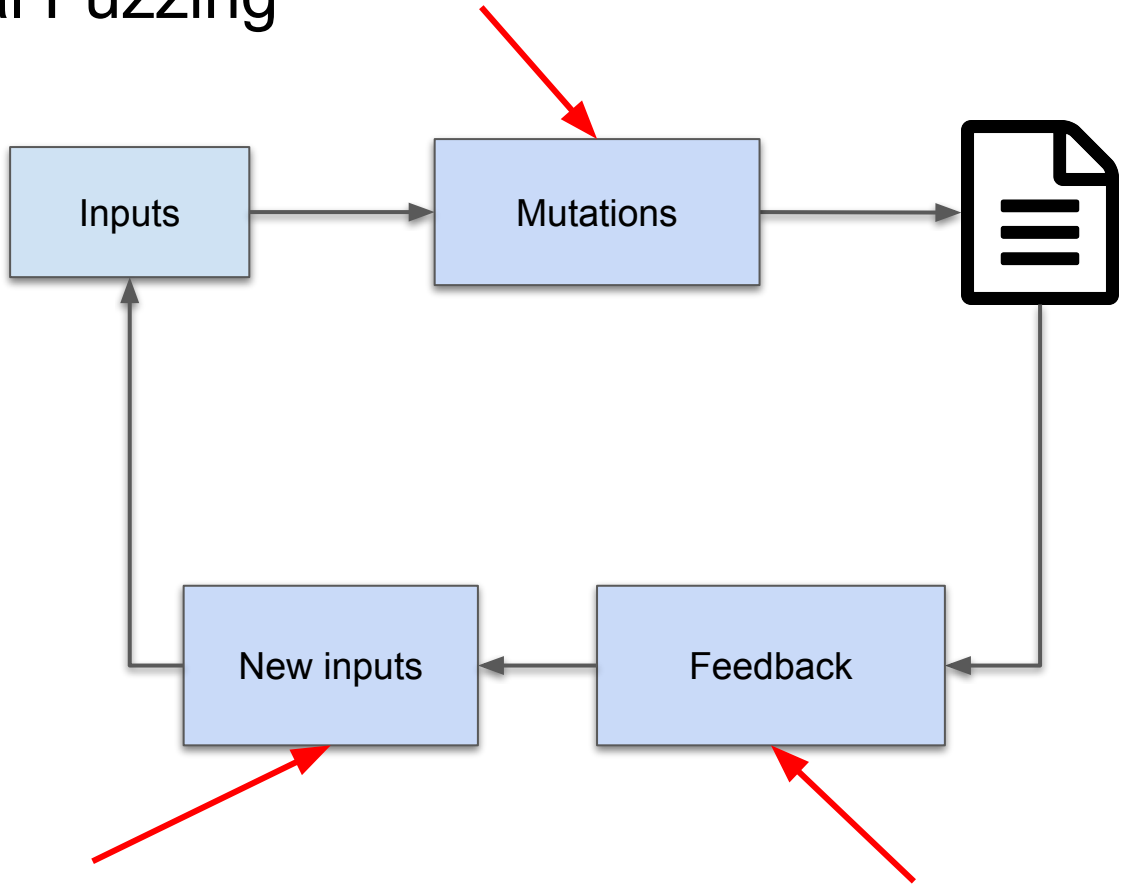
RTLFuzzLab:

Building A Modular Open-Source Hardware Fuzzing Framework

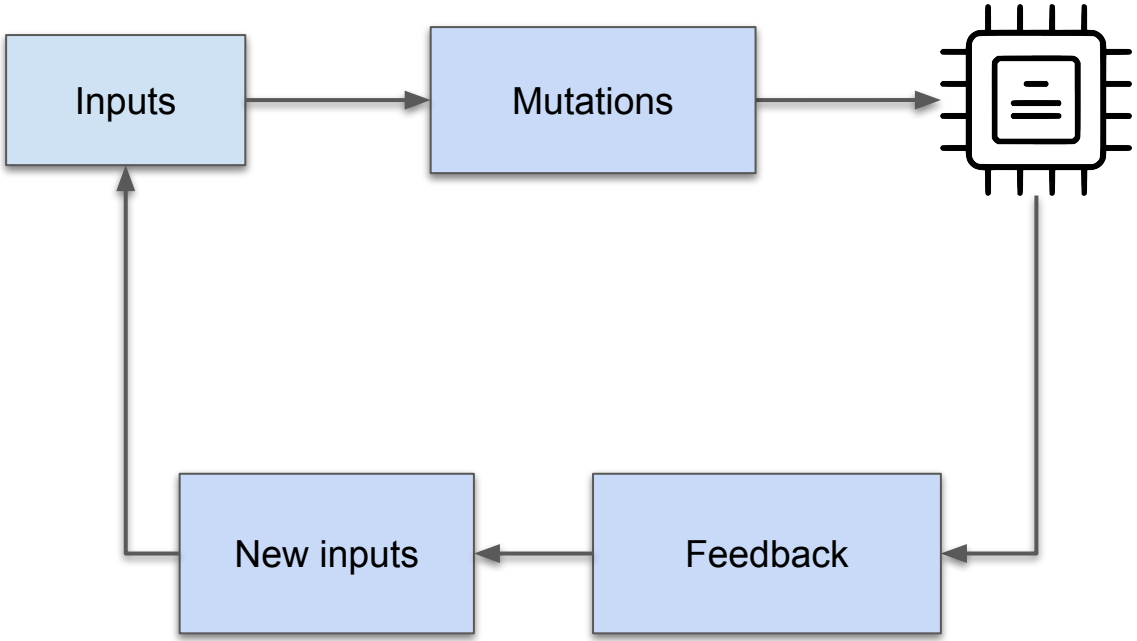
Brandon Fajardo <brfajardo@berkeley.edu>
University of California, Berkeley

Fuzzing

Mutational Fuzzing



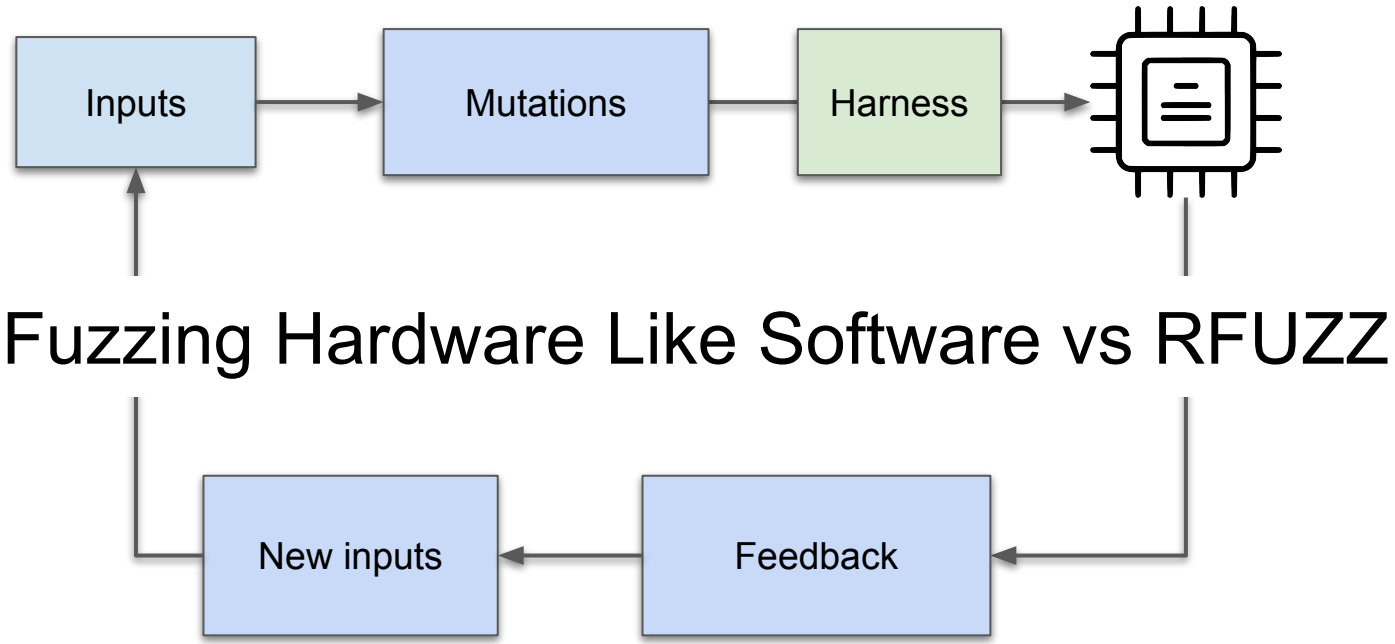
Hardware Fuzzing



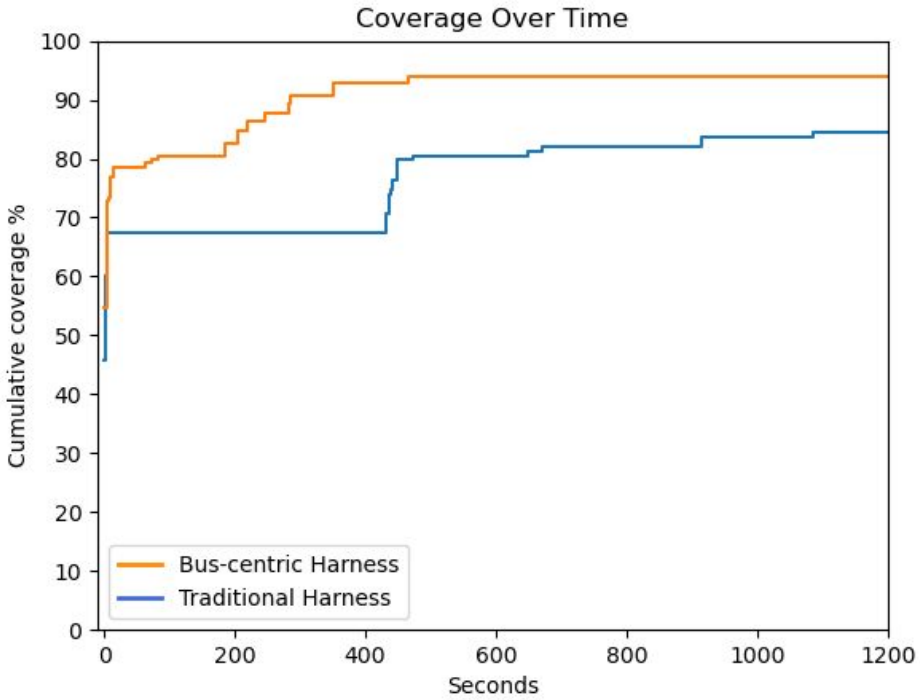
RTLFuzzLab

AFL on FIRRTL designs

Harness

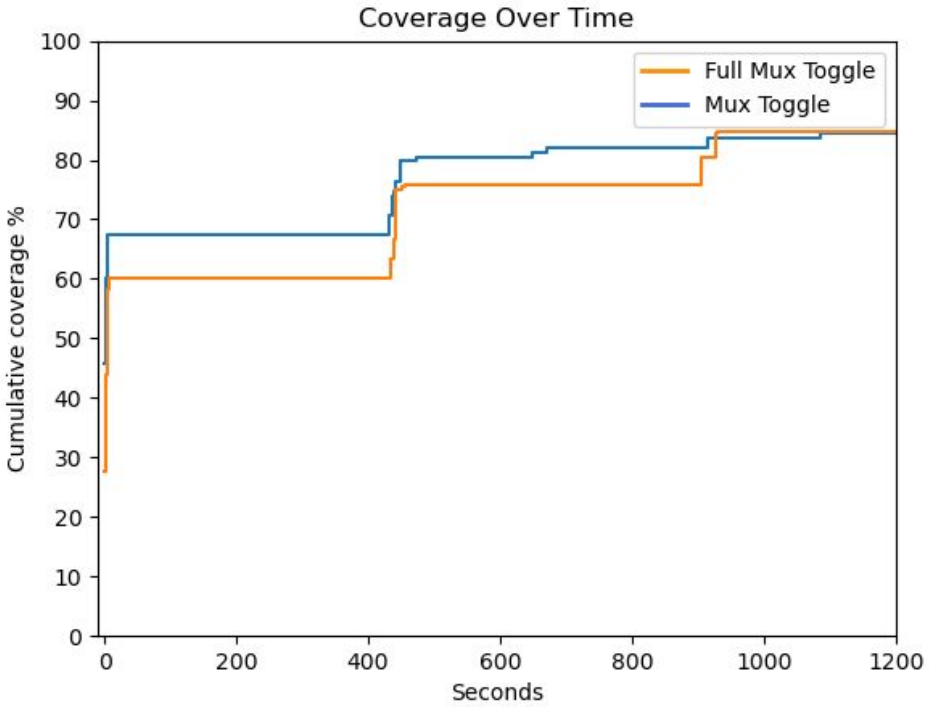

Inputs
Mutations
Harness
Fuzzing Hardware Like Software vs RFUZZ
New inputs
Feedback

Harness: Fuzzing Hardware Like Software vs RFUZZ



Unique Combinations

Feedback: Mux Toggle vs Full Mux Toggle



Demo

./fuzz.sh TLI2C.fir tlul 1 output 3 ~/AFL

- FIRRTL
- Harness
- Minutes
- Output folder
- Iterations
- Path to AFL

Conclusion

- https://github.com/ekiwi/rtl-fuzz-lab

Authors:

Brandon Fajardo <brfajardo@berkeley.edu>
Kevin Laeufer <laeufer@berkeley.edu>
Koushik Sen <ksen@berkeley.edu>
Jonathan Bachrach <jrb@berkeley.edu>