

Understanding and Detecting Memory Bugs in Rust



PennState



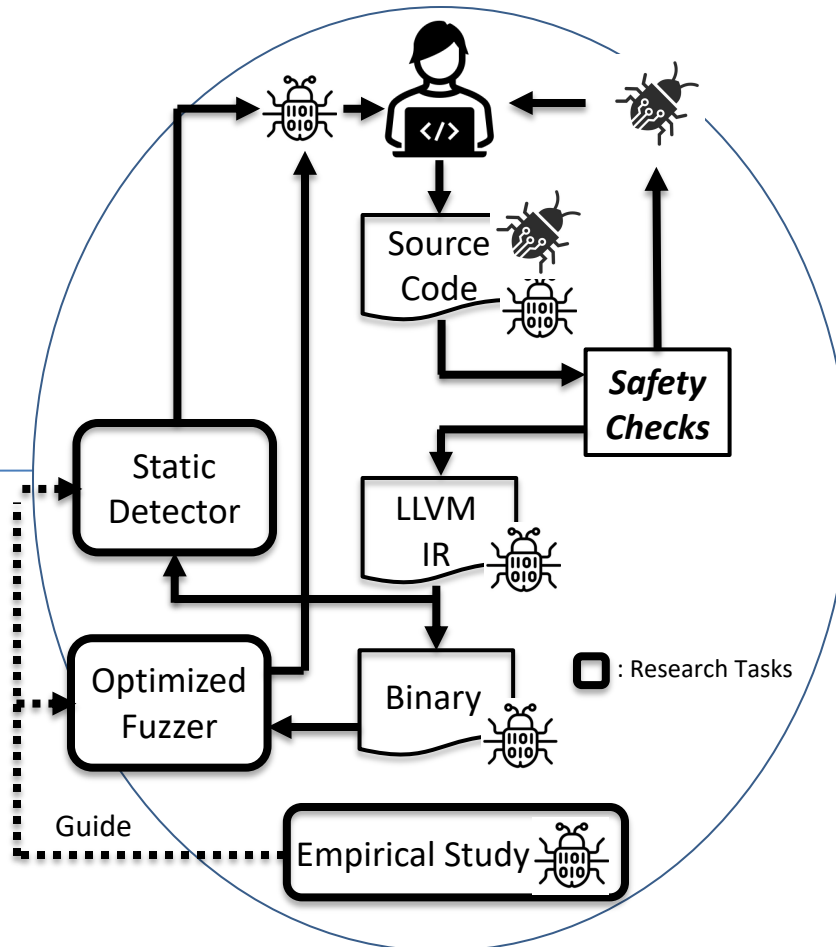
UC DAVIS
UNIVERSITY OF CALIFORNIA

Challenges:

- How to know the characteristics of Rust memory bugs?
- How to effectively detect memory bugs missed by Rust's safety checks?
- How to leverage Rust's unique language features to guide the bug detection?

Solutions:

- A comprehensive study on Rust memory bugs
- Automatically inferring execution conditions of unsafe code for static memory bug detection
- Using safe/unsafe info. to accelerate fuzzing techniques for Rust programs



Scientific Impact:

- A better understanding of common mistakes made by Rust programmers
- A summary of good and bad practices when modularizing Rust programs
- Experience in building bug detectors for new programming languages

Broader Impact and Broader Participation:

- More reliable systems software and a safer Rust ecosystem
- Knowledge exchange with and possible tech transfer to Amazon, Google, and Mozilla
- New course assignments on coding Rust and research opportunities

Award Numbers: 1955965 and 1956364

Affiliations: Penn State and UC Davis

Contacts: Linhai Song (songlh@ist.psu.edu) and Hao Chen (chen@ucdavis.edu)