Fuzzing

Mathias Payer, EPFL

Motivation

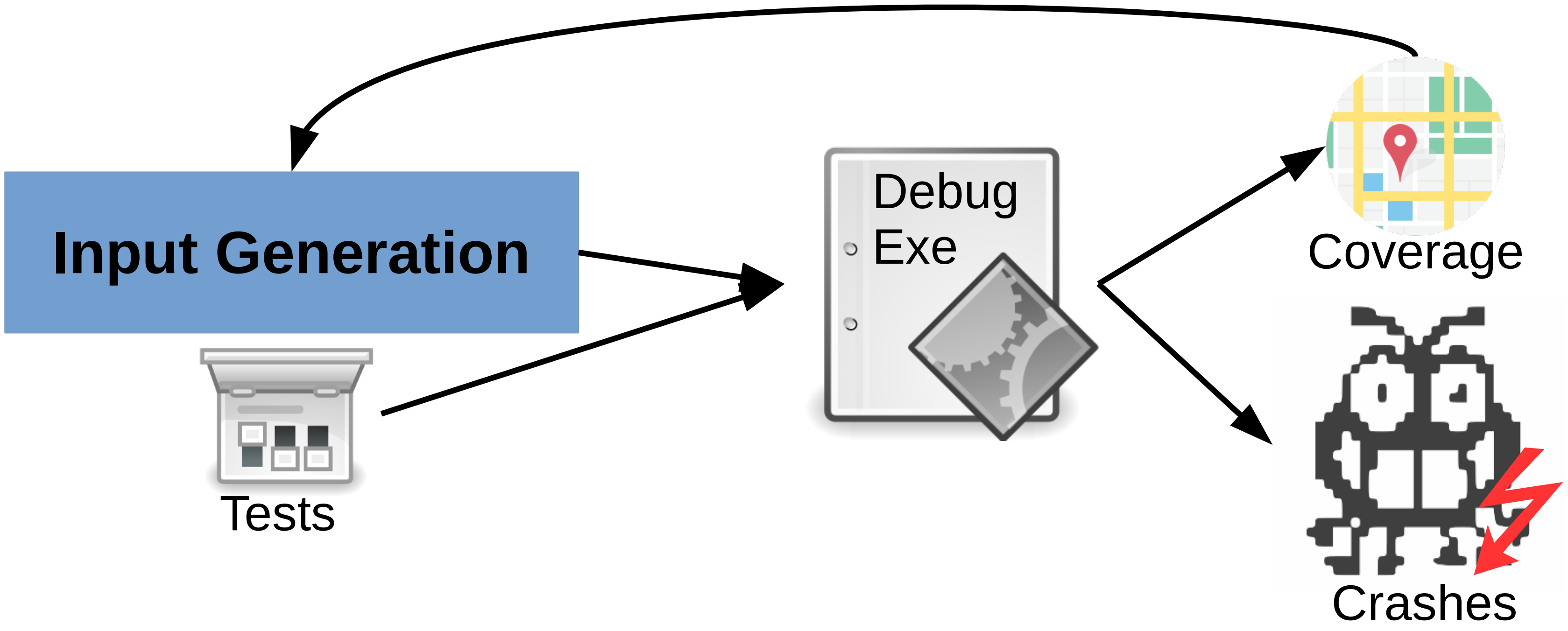
- Traditional testing can’t find vulnerabilities
  - Unit testing
  - Integration testing
- Proactive bug finding increasingly necessary
  - Software quality assurance
  - Protect software customers from being attacked

Automatic Bug Finding

- Static analysis
  - Analyze the program without executing it
  - Imprecision by lack of runtime information, e.g. aliasing
- Symbolic analysis
  - Execute the program symbolically
  - Keeping track of branch conditions
  - Not scalable
- Dynamic analysis
  - Inspect the program by executing it
  - Challenging to cover all paths

Fuzzing

- A random testing technique that mutates input to improve test coverage



- State-of-art fuzzers use coverage as feedback to evolutionarily mutate the input

FUZZ
ALL THE THINGS
memegenerator.net

Fuzzing as bug finding approach

- Fuzzing is highly effective bug finding (CVEs)
  - Proactive defense measure
  - First step in exploit development

OpenSSL BASH THE BOURNE-AGAIN SHELL

OpenBSD SQLite LibreOffice®

Different types of Fuzzers

- Black box, generate random input
  - Set of valid samples will help! (e.g., Radamsa)
- Model-based: generate grammar-based input
  - Follows specification more closely
- Coverage-guided fuzzing, feedback loop
  - Push input generation to new coverage
  - AFL, Hongfuzz, libFuzzer

AFL: Coverage-Guided Fuzzer

- Genetic algorithms to generate new input
- Simple, yet very effective: tons of security bugs
  - Take one input from queue
  - Minimize test case (as long as same behavior)
  - Mutate and execute
  - If new input: store sample in queue

Lab 01: Fuzzing

Lab 01: Fuzzing

- Goal: play with modern fuzzers
  - (Task 0): prepare your system and read up
  - Task 1: effects of seed selection
  - Task 2: fuzzing native vs. instrumented binaries
  - (Task 3): different forms of instrumentation
- Work smart, intended time per task:
  - 2 hours of thinking time
  - 4-6 hours of CPU time
- Write a quick summary of your findings
  - Deadline: November 13

FUZZING IS AWESOME
CHANGE MY MIND
imgflip.com