The Art, Science, and Engineering of Fuzzing: A Survey

Valentin J.M. Manès, HyungSeok Han, Choongwoo Han, Sang Kil Cha, Manuel Egele, Edward J. Schwartz, and Maverick Woo
A Complex Field
Fuzzing: Potential Definitions

• Some say: “Fuzzers are tools to make crashes.”
  ➞ What kind of crash?
  ➞ PerfFuzz\textsuperscript{1} just looks for “algorithmic complexity vulnerabilities”.

• Some say: “Fuzzers create inputs, either by \textbf{mutating seeds} (e.g. zzuf),
  or based on \textbf{models}, like grammars (e.g. Peach).”
  ➞ Random Testing may not use any seed.
  ➞ Concolic execution use neither.

Common Pitfalls

A definition should:

• **Not be goal oriented.**
  ➔ Fuzzers are tools: their goal is defined by the user.

• **Not be method oriented.**
  ➔ The field has shown too much diversity.
Fuzzing: What it is?

Fuzzing refers to a process of repeatedly running a program with generated inputs to test if a program violates a correctness policy.*
Fuzzers: How to Model Them?

Fuzzer

1. InputGen
2. InputEval

PreProcess

Schedule

ConfUpdate

test cases

execinfos

① ② ③
Survey Methodology

• We surveyed the field for 10+ years:
  - Major Github repositories
  - Major conferences (Security & Software Engineering)

• Let’s look at two examples: zzuf, AFL
Example

Fuzzer zzuf

Seed bit flip

InputGen

PreProcess

Schedule

ConfUpdate

test cases

execinfos

Simple Execution
Fuzzer AFL

InputGen

InputEval

Fuzzer AFL

test cases

t

execinfos

Coverage-based Fitness Function

Instrumentation

Mutation operations

Instrumented Execution

PreProcess

Schedule

ConfUpdate

Round Robin++

Example
Genealogy
Companion Website: fuzzing-survey.org
AFL: A Grey-box Hub
Black-box Hubs

LangFuzz

BFF

Languages

- LangFuzz
- BlendFuzz
- CrossFuzz
- Nduje
- Dewey et al.
- GLADE
- CSmith
- CLSmith
- IFuzzler
- CodeAlchemist

Black-box Frameworks

- BFF
- FOE
- Householder
- Woo et al.
- Robert et al.
- DELTA
- SymFuzz
Grey-box Outliers

CalFuzzer

CalFuzzer

AtomeFuzzer

AssetFuzzer

DeadlockFuzzer

RaceFuzzer

MagicFuzzer

Narada

Sidewinder

GIF

Liber

Safety

Mutation

Chopper

Deja

SubTec

NaradaFuzzer

Software Security

KAIST
Companion Website: fuzzing-survey.org

Make a PR to add fuzzers 😊
github.com/SoftSec-KAIST/Fuzzing-Survey
Share your fuzzer!

Sharable links: fuzzing-survey.org/?k=Ankou

[greybox] Ankou (2020)


Targets: 📦
Tool URL: ⚙
Misc. URLs: ☀
Share: 🔄
Question?