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\(^1\) just looks for “algorithmic complexity vulnerabilities”.

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

\(^1\)C. Lemieux, R. Padhye, K. Sen, and D. Song, “PerfFuzz: Automatically generating pathological inputs,” in Proceedings of the International Symposium on Software Testing and Analysis, 2018, pp. 254–265.
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 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

- InputGen
- InputEval

PreProcess

Schedule

ConfUpdate

Simple Execution

Seed bit flip

test cases

execinfos
Example

Fuzzer AFL

InputGen → InputEval

Mutation operations

Instrumented Execution

test cases

execinfos

Coverage-based Fitness Function

Instrumentation

PreProcess

Round Robin++

Schedule

ConfUpdate

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

LangFuzz

BFF

Diagram showing the relationships between various tools and methodologies in software testing.
Grey-box Outliers

CalFuzzer

Sidewinder
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)

"Ankou: Guiding Grey-box Fuzzing towards Combinatorial Difference", Valentin J. M. Manès, Soomin Kim, and Sang Kil Cha. In Proceedings of the International Conference on Software Engineering, 2020

Targets: 

Tool URL: 

Misc. URLs: 

Share:
Question?