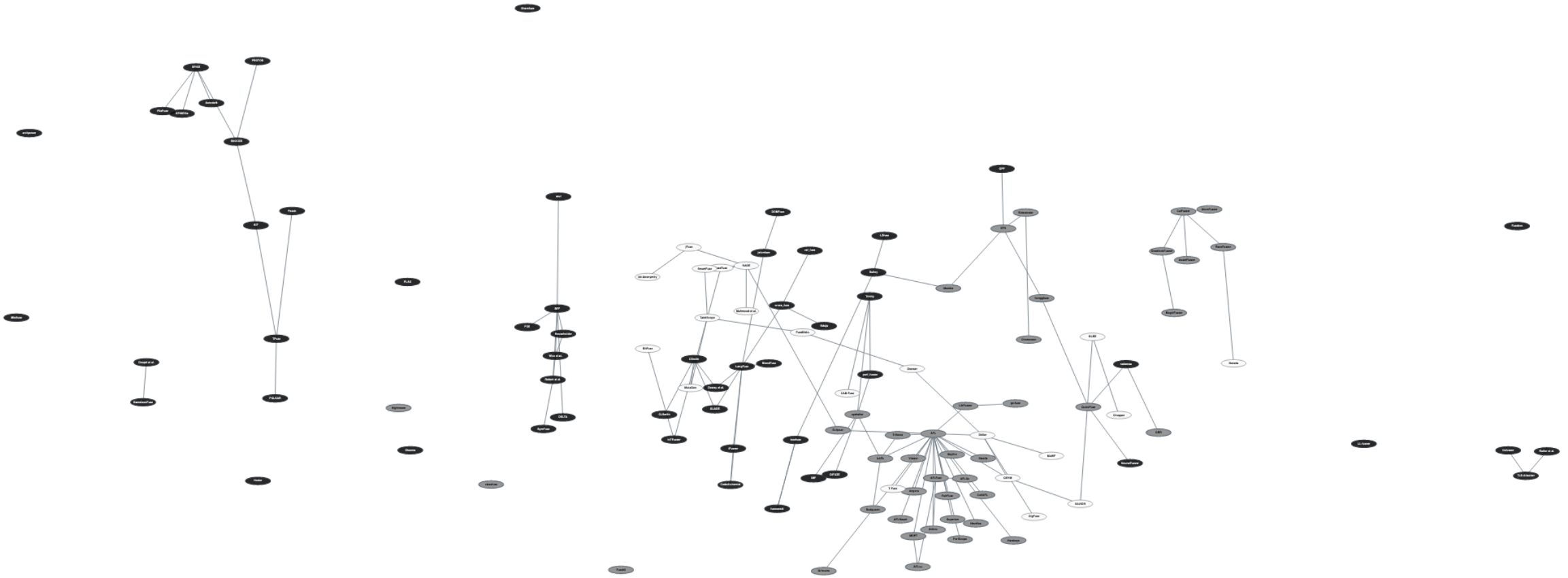
The Art, Science, and Engineering of Fuzzing: A Survey

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: there goal is defined by the user.

- **Not be method oriented**.

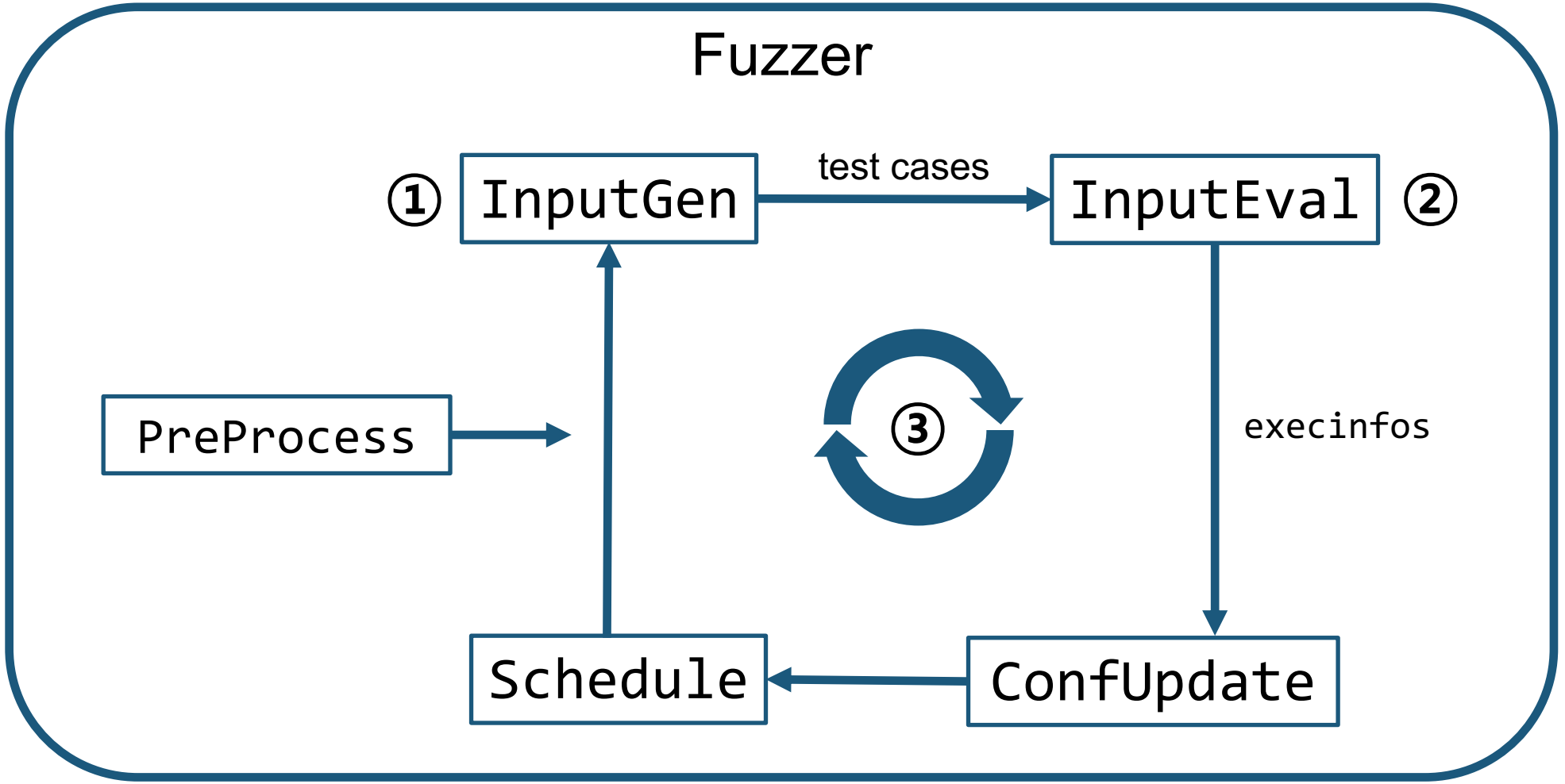
  ➔ The field has shown too much diversity.

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.*

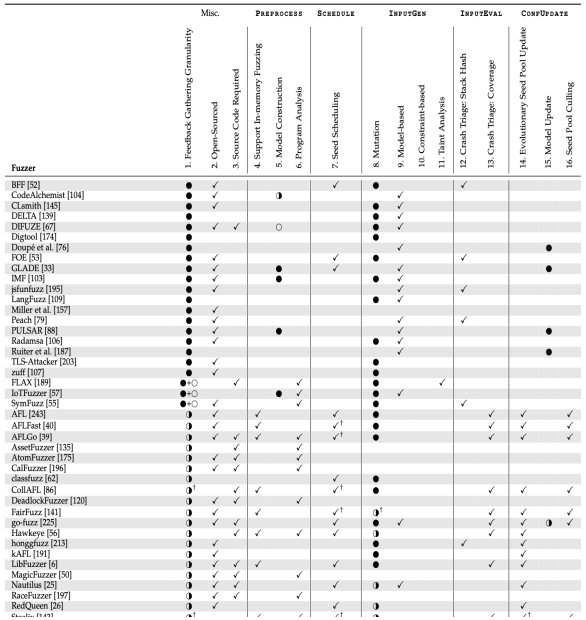
* This is a simplified version of the definition in the paper.

Fuzzers: How to Model Them?



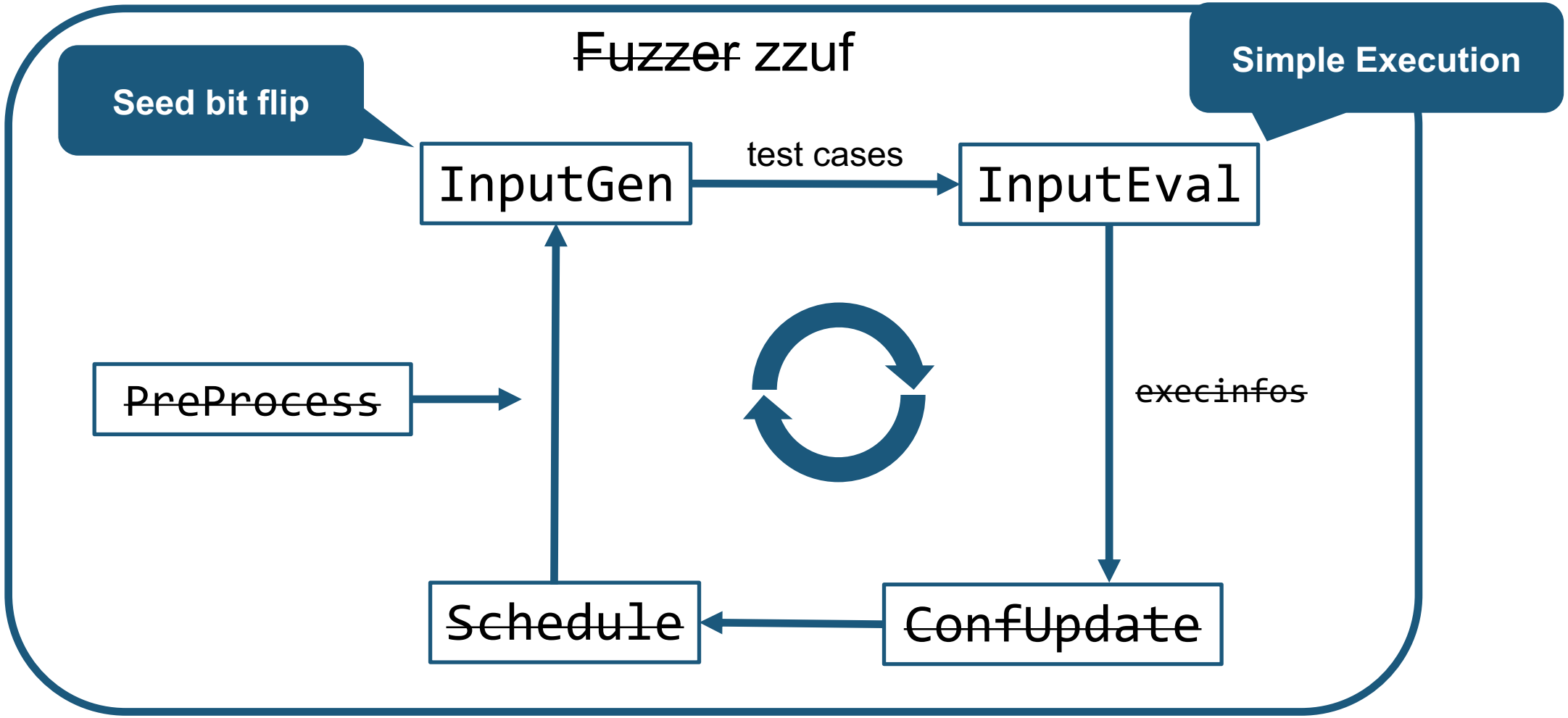
Survey Methodology

- We surveyed the field for 10+ years:
  - ❖Major Github repositories
  - ❖Major conferences (Security & Software Engineering)
- Let's look at two examples: zzuf , AFL

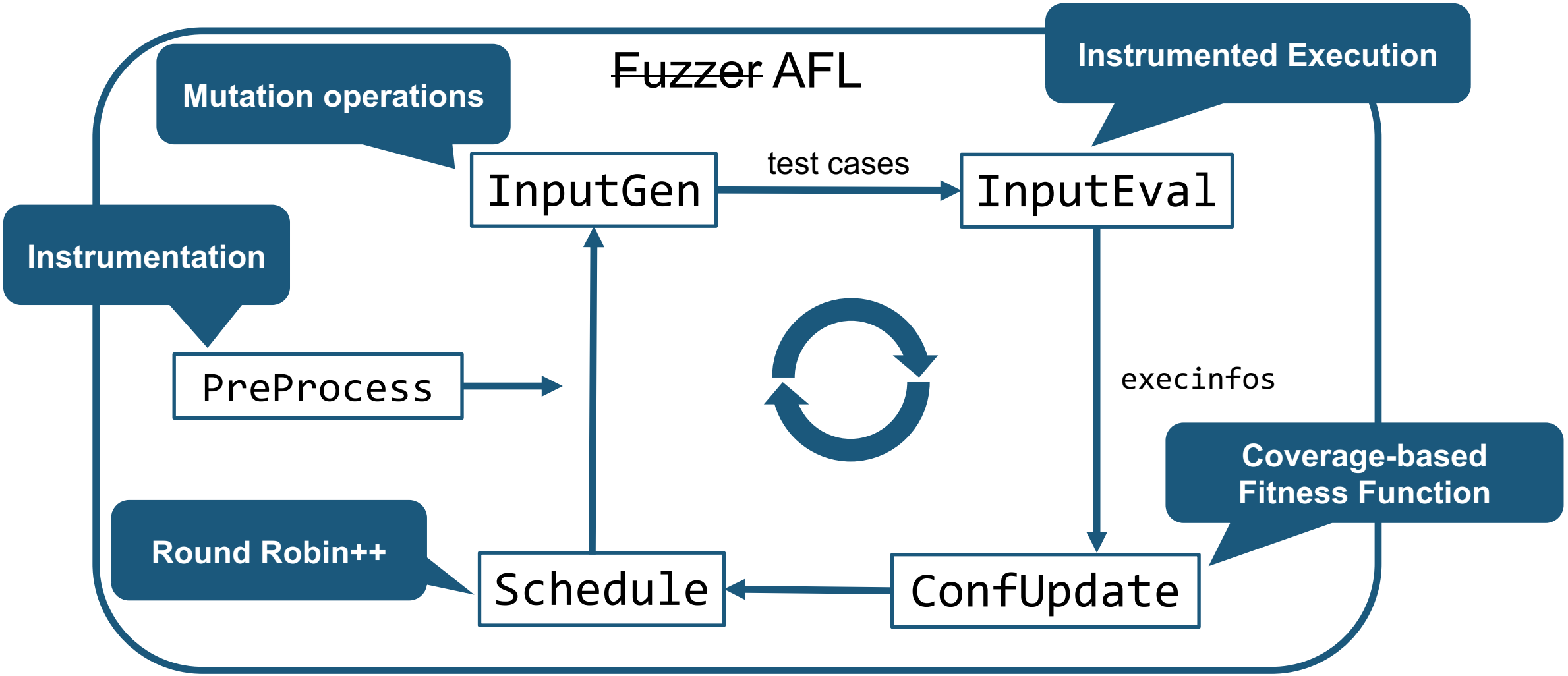


Fuzzer	Misc.			Preprocess		Schedule		InputGen			InputEval		ConfUpdate		
	1. Feedback Gathering Granularity	2. Open-Sourced	3. Source Code Required	4. Support In-memory Fuzzing	5. Model Construction	6. Program Analysis	7. Seed Scheduling	8. Mutation	9. Model-based	10. Constraint-based	11. Taint Analysis	12. Crash Triage: Stack Hash	13. Crash Triage: Coverage	14. Evolutionary Seed Pool Update	15. Model Update	16. Seed Pool Culling
BFF [52]	●	✓					✓	●				✓				
CodeAlchemist [104]	●	✓						●	✓							
CLsmith [145]	●	✓						●	✓							
DELTA [139]	●							●	✓							
DIFUZE [67]	●	✓	✓		○			●	✓							
Digtool [174]	●							●								
Doupé et al. [76]	●								✓						●	
FOE [53]	●	✓					✓	●				✓				
GLADE [33]	●	✓			●		✓		✓						●	
IMF [103]	●	✓			●			●	✓							
jsfunfuzz [195]	●	✓							✓			✓				
LangFuzz [109]	●							●	✓							
Miller et al. [157]	●	✓														
Peach [79]	●	✓							✓			✓				
PULSAR [88]	●	✓			●				✓						●	
Radamsa [106]	●	✓						●	✓							
Ruiter et al. [187]	●								✓						●	
TLS-Attacker [203]	●	✓						●								
zuff [107]	●	✓						●								
FLAX [189]	●+○		✓			✓		●			✓					
IoTFuzzer [57]	●+○				●	✓		●	✓							
SymFuzz [55]	●+○	✓				✓		●				✓				
AFL [243]	◑	✓		✓			✓	●					✓	✓		✓
AFLFast [40]	◑	✓		✓			✓†	●					✓	✓		✓
AFLGo [39]	◑	✓	✓	✓		✓	✓†	●					✓	✓		✓
AssetFuzzer [135]	◑		✓			✓										
AtomFuzzer [175]	◑	✓	✓			✓										
CalFuzzer [196]	◑	✓	✓			✓										
classfuzz [62]	◑						✓	●								
CollAFL [86]	◑		✓	✓			✓†	●					✓	✓		✓
DeadlockFuzzer [120]	◑	✓	✓			✓										
FairFuzz [141]	◑	✓		✓			✓†	◑†					✓	✓		✓
go-fuzz [225]	◑	✓	✓				✓	●	✓				✓	✓	◑	✓
Hawkeye [56]	◑		✓	✓		✓	✓	◑					✓	✓		
honggfuzz [213]	◑	✓						●				✓		✓		
kAFL [191]	◑	✓						●						✓		
LibFuzzer [6]	◑	✓	✓	✓			✓	●					✓	✓		
MagicFuzzer [50]	◑	✓	✓			✓										
Nautilus [25]	◑	✓	✓				✓	◑	✓					✓		
RaceFuzzer [197]	◑	✓	✓			✓										
ResQueens [26]	◑	✓					✓	◑						✓		
[illegible]	◑			✓		✓	✓†	◑					✓	✓†		✓

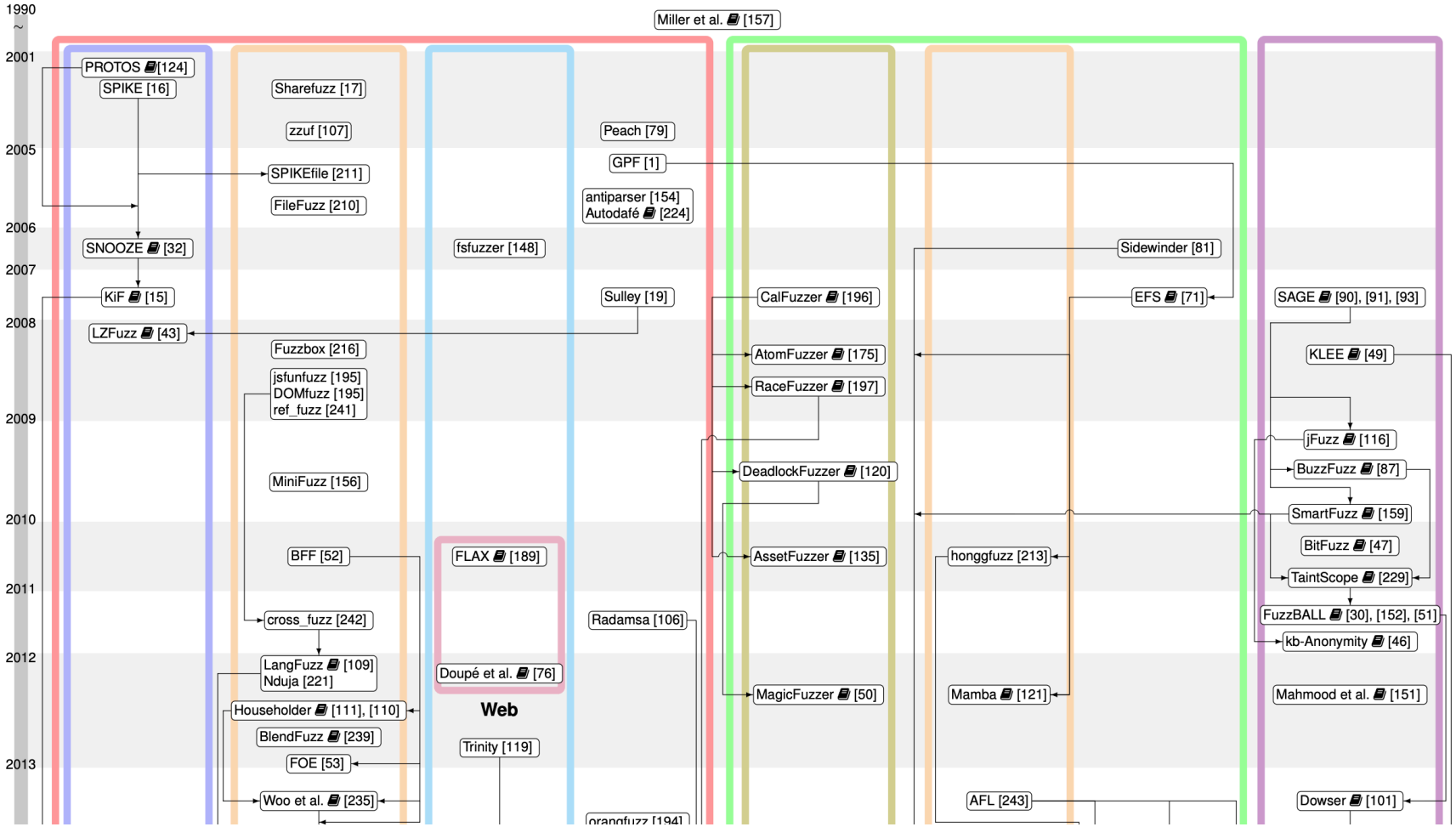
Example


~~Fuzzer~~ zzuf
Seed bit flip
Simple Execution
InputGen
test cases
InputEval
~~PreProcess~~
~~execinfos~~
~~Schedule~~
~~ConfUpdate~~

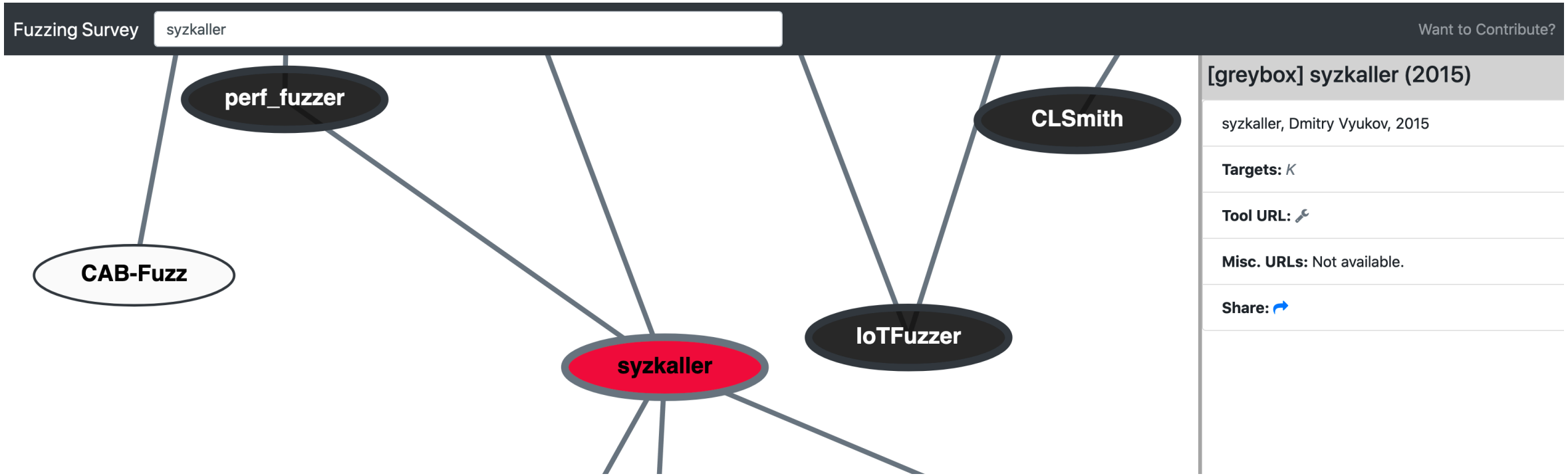
Example


~~Fuzzer~~ AFL
Mutation operations
Instrumented Execution
InputGen
test cases
InputEval
Instrumentation
PreProcess
execinfos
Coverage-based
Fitness Function
Round Robin++
Schedule
ConfUpdate

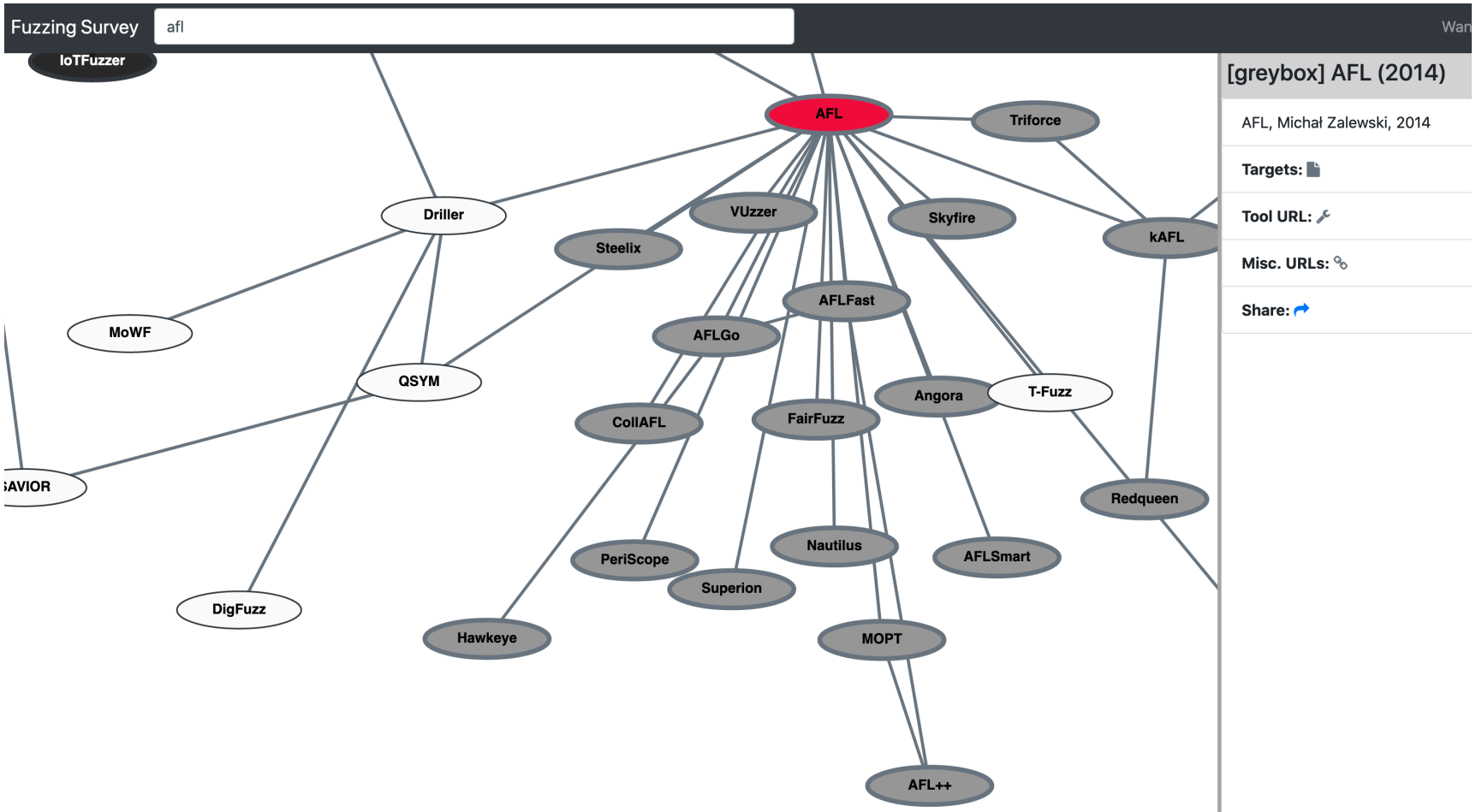
Genealogy


1990
~
2001
2005
2006
2007
2008
2009
2010
2011
2012
2013
Miller et al. [157]
PROTOS [124]
SPIKE [16]
Sharefuzz [17]
zzuf [107]
SPIKEfile [211]
FileFuzz [210]
SNOOZE [32]
KiF [15]
LZFuzz [43]
Fuzzbox [216]
jsfunfuzz [195]
DOMfuzz [195]
ref_fuzz [241]
MiniFuzz [156]
BFF [52]
cross_fuzz [242]
LangFuzz [109]
Nduja [221]
Householder [111], [110]
BlendFuzz [239]
FOE [53]
Woo et al. [235]
fsfuzzer [148]
FLAX [189]
Doupé et al. [76]
Web
Trinity [119]
Peach [79]
GPF [1]
antiparser [154]
Autodafé [224]
Sulley [19]
Radamsa [106]
orangfuzz [194]
CalFuzzer [196]
AtomFuzzer [175]
RaceFuzzer [197]
DeadlockFuzzer [120]
AssetFuzzer [135]
MagicFuzzer [50]
Sidewinder [81]
EFS [71]
honggfuzz [213]
Mamba [121]
AFL [243]
SAGE [90], [91], [93]
KLEE [49]
jFuzz [116]
BuzzFuzz [87]
SmartFuzz [159]
BitFuzz [47]
TaintScope [229]
FuzzBALL [30], [152], [51]
kb-Anonymity [46]
Mahmood et al. [151]
Dowser [101]

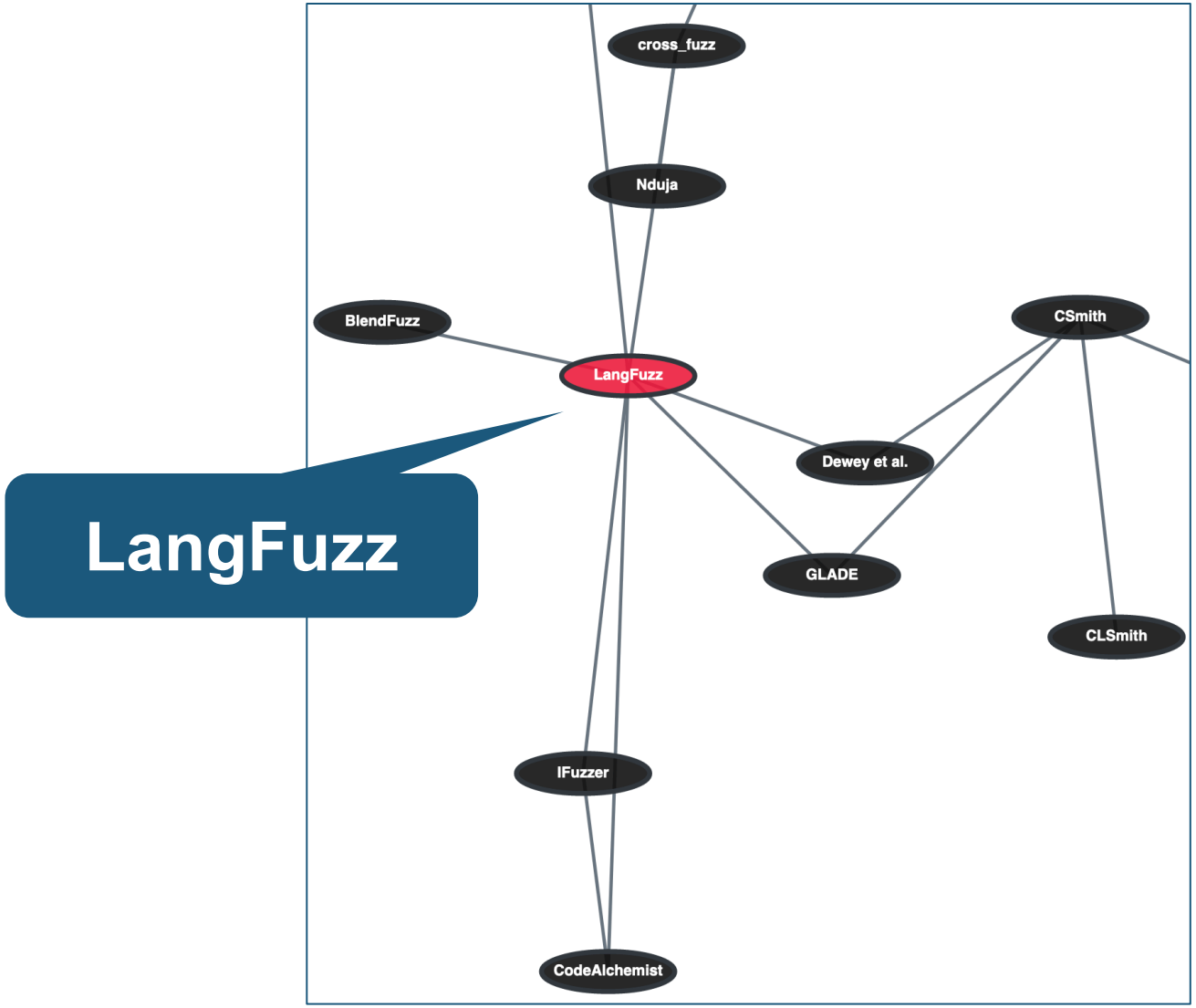
Companion Website: fuzzing-survey.org

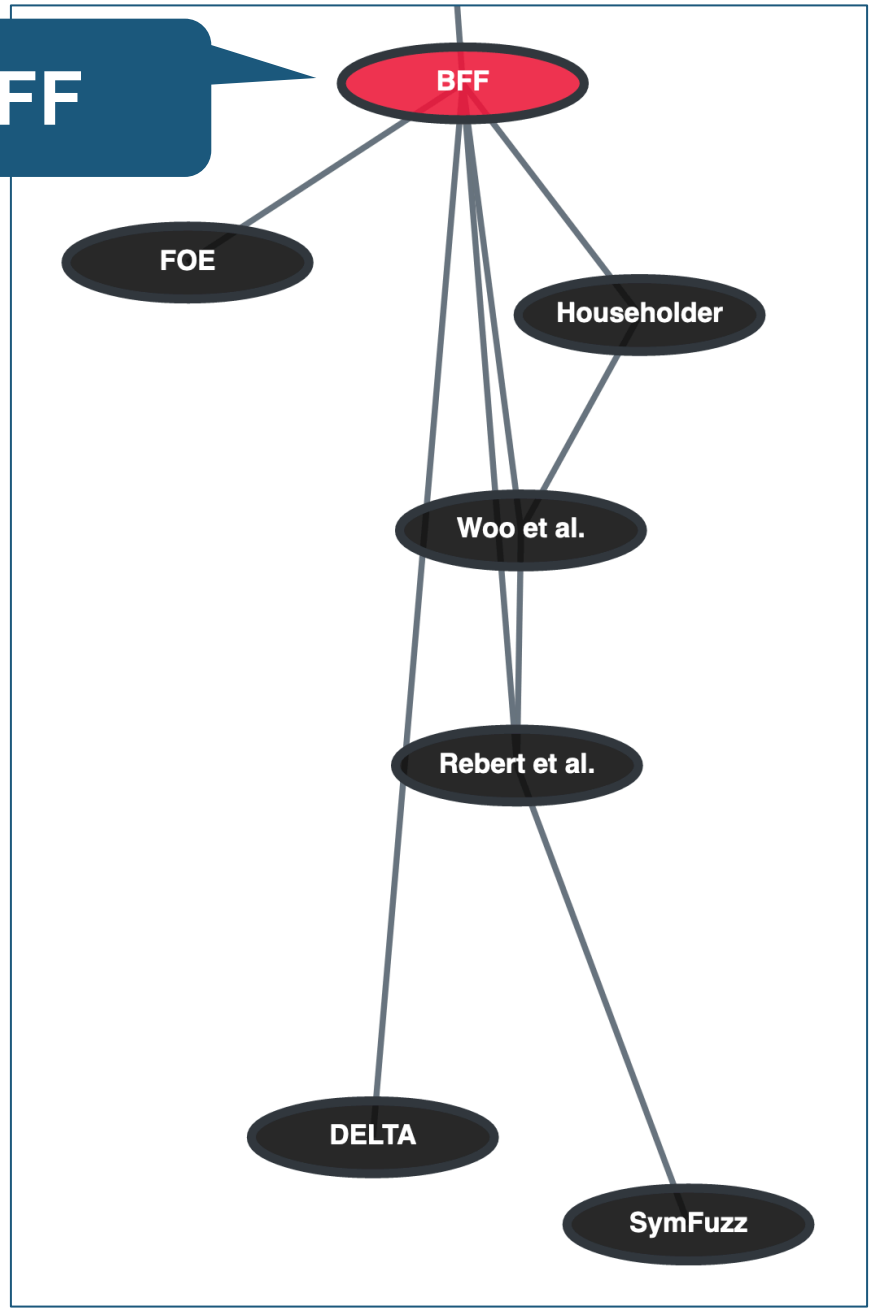


AFL: A Grey-box Hub

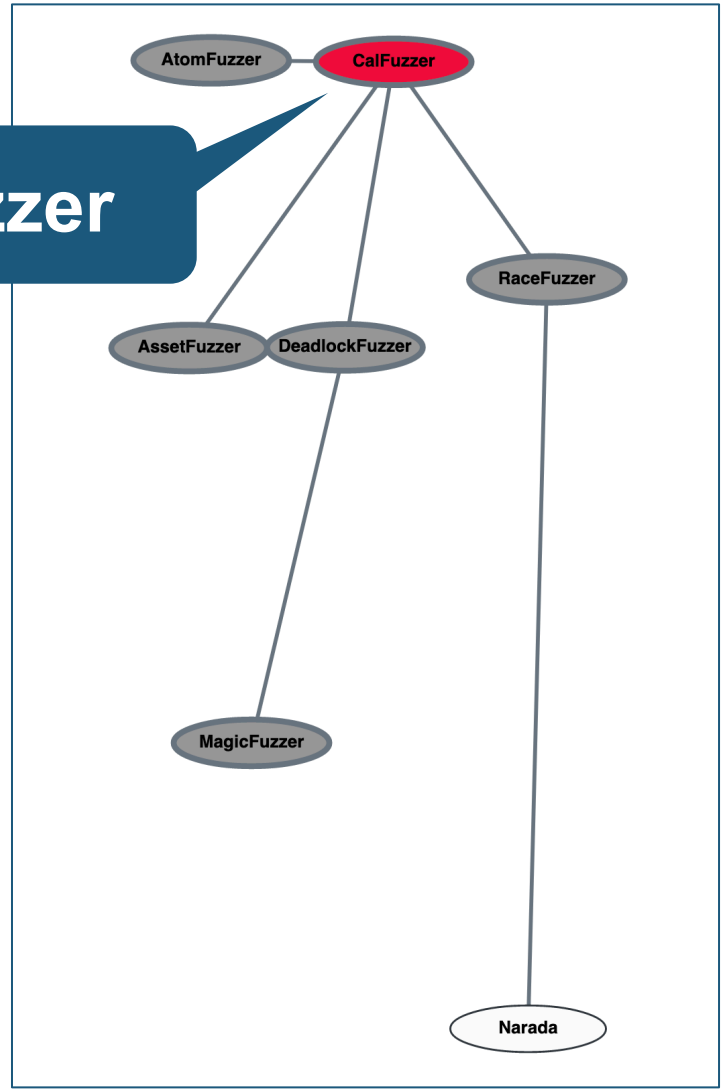


Black-box Hubs

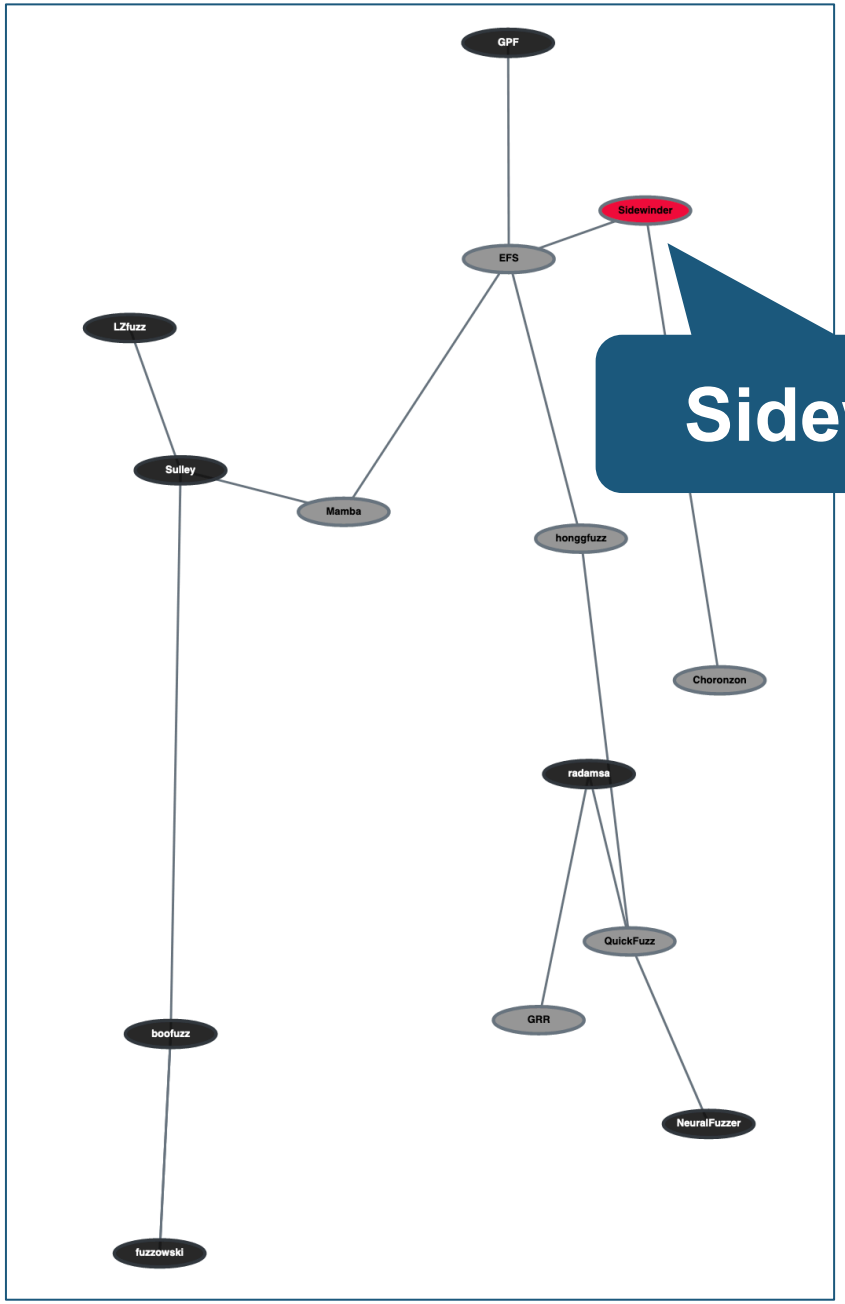




Grey-box Outliers



CalFuzzer



Sidewinder

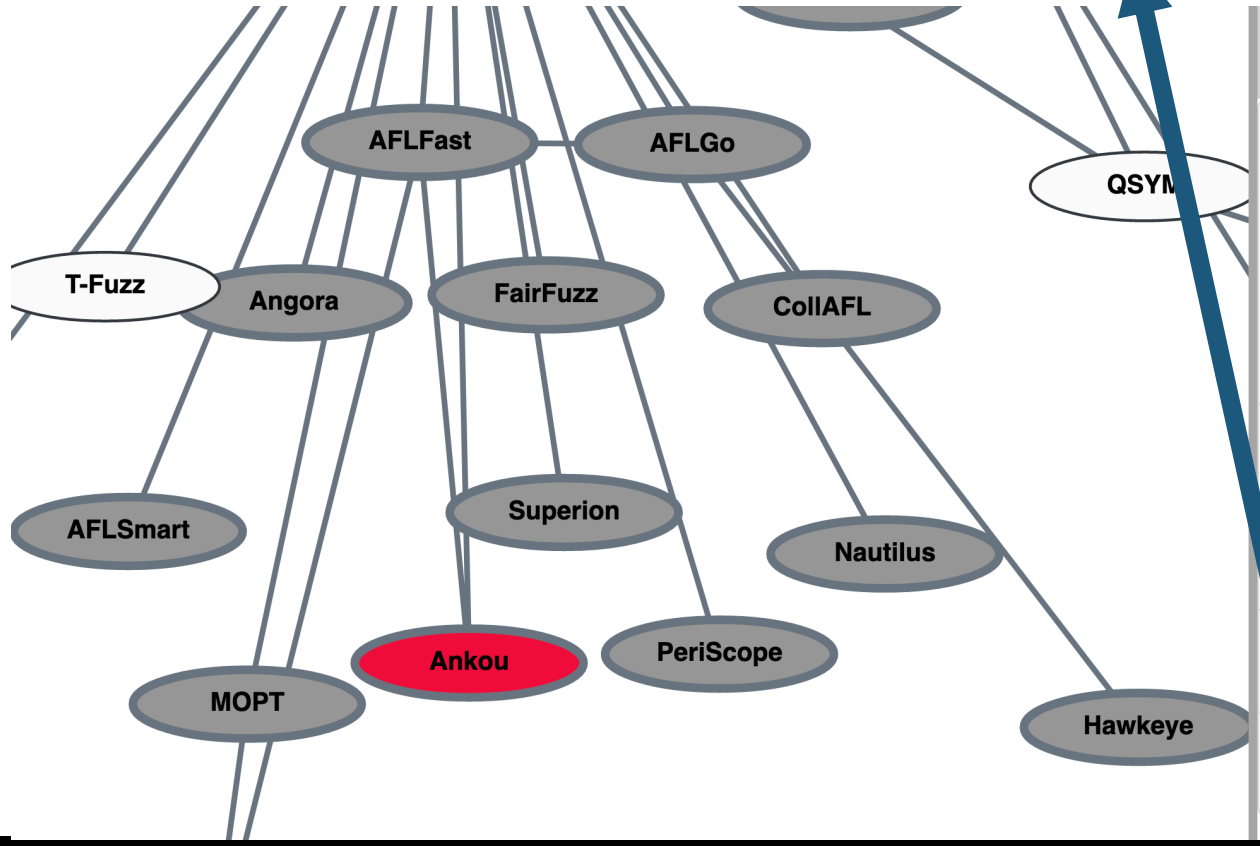
Companion Website: fuzzing-survey.org

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?