One Fuzz Doesn’t Fit All: Optimizing Directed Fuzzing via Program State Restriction

Prashast Srivastava¹, Stefan Nagy², Matthew Hicks³, Antonio Bianchi¹, Mathias Payer⁴

¹ Purdue University ² University of Utah ³ Virginia Tech ⁴ EPFL

Inefficiency of existing directed fuzzing approaches

Problem: Existing distance minimization based fuzzers perform wasteful exploration of target-unreachable code regions

Observation: Current exploration schemes particularly ill-suited for disjoint target locations

Solution: Preemptively terminate execution of target-unreachable code regions — Tripwiring

Tripwiring-directed Fuzzing

SieveFuzz Workflow

Bug Discovery Performance

Takeaway

Tripwiring is an optimal strategy for fuzzing target locations which exhibit disjointness

SieveFuzz can trigger bugs on average 47% more consistently and 117% faster than existing state-of-the-art undirected (AFL++) and directed fuzzers (AFLGo, BEACON)