CERIAS
The Center for Education and Research in Information Assurance and Security

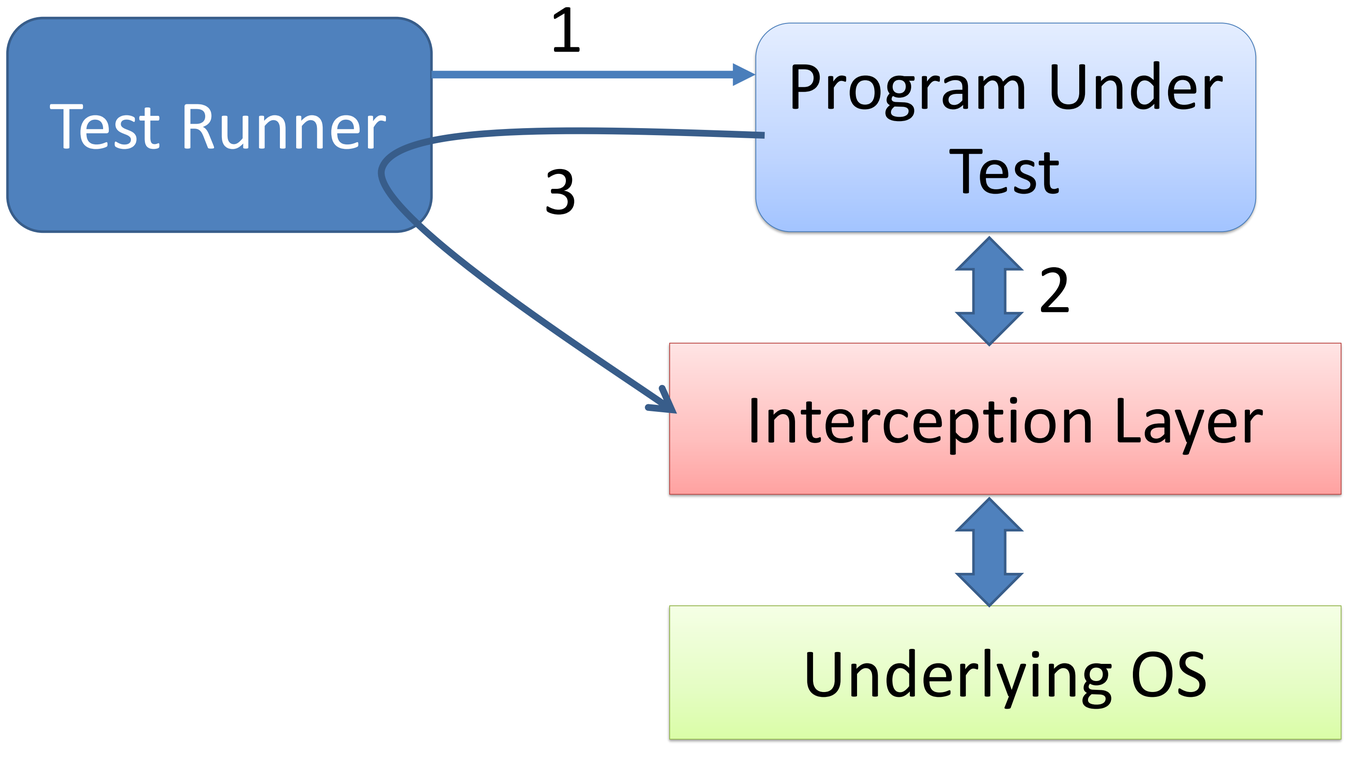
HexFuzz: Bug Finding through combined fault injection and fuzzing at library boundaries

Hui Peng, Hrishikesh Deshpande, Mathias Payer

Background & Motivation

- ❑ Fuzzing is an effective bug finding technique
- ❑ Existing random approaches are inefficient
- ❑ This work improves the state-of-art by combing fault injection and fuzzing at the interaction level

Workflow



1. Test Runner controls the execution of PUT.
2. All calls to system functions are routed to interception layer where:
   - Faults are injected
   - Inputs from read/recv etc are fuzzed using previous execution trace info
3. Execution trace is fed back to the interception layer

Highlights

- ❑ Fault injection finds bugs that are unlikely triggered under normal conditions.
- ❑ Fuzzing input at the interaction level improves the fuzzing strategy (ongoing)

Intermediate results

Package	# of bugs found
ruby	1
coreutils	1
enscript	4
php	1
gtypist	2