Bug Finding

MOPS\SLAM (Model Checking)

\[ P \rightarrow \text{PDA}_P \]

\[ \text{FSA}_B \times \text{PDA}_P \rightarrow \text{PDA}_{\text{combined}} \]

Is Language of \( \text{PDA}_{\text{combined}} \) empty?

Fuzzing

Fuzzing - Running the program with random input

Paper to look at: "Fuzz Revisited"

- Tool called fuzz which outputs random numbers and feeds to target program
- Observes crash, infinite loop, complete
- Research team ran fuzz on different command line utilities
  - NextStep 40% Failure
  - Solaris, SunOS, HPUX, AIX 20-30% failure
  - Linux 9% failure
  - GNU 6% failure
- x fuzzer
  - an x server fuzzer
- Can issue different types of input
  - Perfectly correct
  - Semi correct
  - Totally random
- Never was able to crash x server
- Was able to crash applications with 40% failure rate when the fuzzer pretended to be x server

Fault Injection

- Most programs don’t handle errors well
- Tests behavior of program under adverse conditions
  - Cause actions to fail
    - Can be targeted or random
- Run program on top of fault injector system (fault injector system runs between program and OS)
- Two ways to implement fault injector
  - Modify OS
    - Load kernel module that causes system calls to randomly fail
  - LD_PRELOAD
    - Can write own dynamically library which gets loaded before program
    - Can intercept calls which would normally go to other libraries
    - Can define own open \ malloc \ other functions
void *malloc(size_t n)
{
    if(rand()%2)
        return NULL;
    else
        return real_malloc(n);
}