Fuzzing APIs

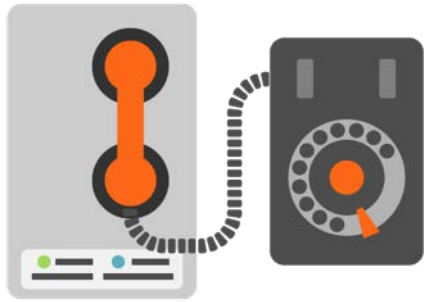
Dr. Jared DeMott
CTO AND FOUNDER

@jareddemott www.vdalabs.com

Overview

Explain API Fuzzing

Demo



Fuzzing traditionally done on trust boundaries

- Parser expected to be fully robust
- Can check all inputs

Library API may check arguments

- More for debugging since this often isn't a true boundary
- Not easy to verify all arguments
  - Native pointers to memory, etc.

Pros

- Unit fuzzing
  - Directly pass malformed args
- Speed increase
- Fuzz hard to reach places

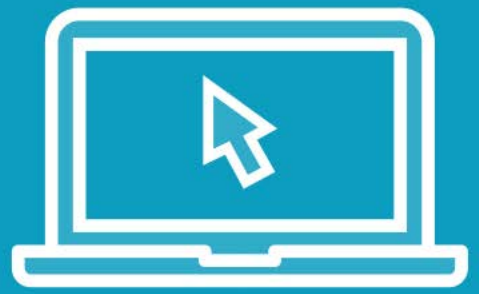
Cons

- False positives
  - If fuzzed “too far” outside of prescribe usage

How to interact with library?

- Fuzzer can directly call it
- Write a stub program

Demo



Use Peach to do API fuzzing

Summary

Pros and cons of API Fuzzing

Similar technique called in-memory