Fuzzing & Static Analysis

Static Analysis

FlawFinder -- checks file content against internal database (“ruleset”) of known vulnerable c functions

that could lead to things like:

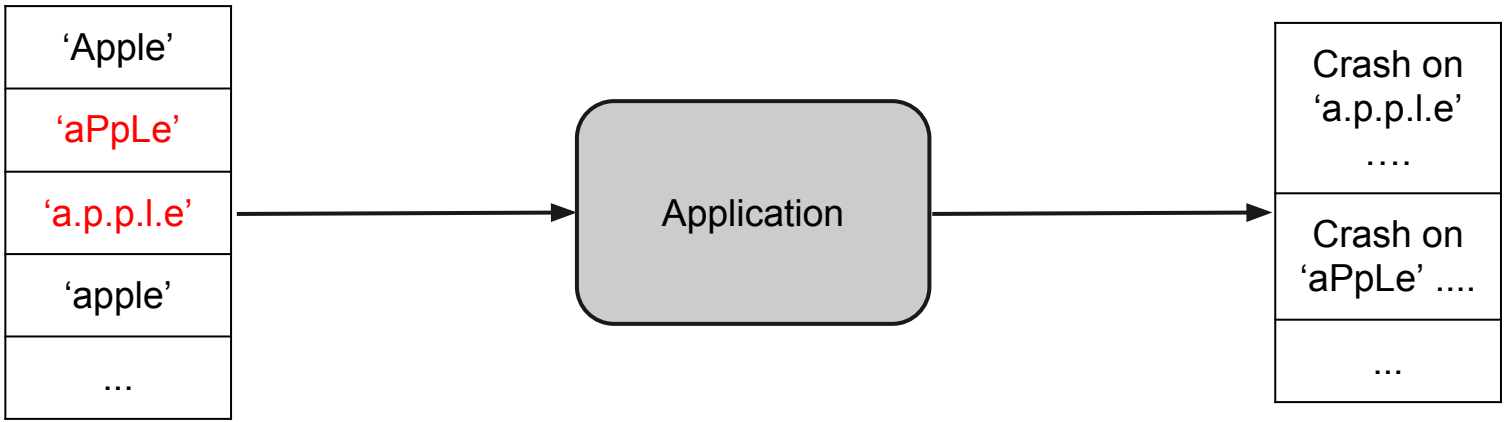
- buffer overflows
- format string vulnerabilities
- race conditions

Static Analysis

DEMO

- note flawfinder ranks risk levels based on the function and also parameters
- ex. constant strings less risky than user string

What is fuzzing?



Types of Fuzzing Strategies

Random fuzzing

Mutation-based (aka Template) fuzzing

Generational (aka model-based) fuzzing

Types of Fuzzing Strategies

Random fuzzing

- easy, not much deep knowledge required of protocol
- not very effective, not very efficient, false positives

Mutation-based (aka Template) fuzzing

- mostly looks like acceptable inputs so will actually travel interesting code paths
- but depends on template and how complete your knowledge of possible templates is (i.e. checksums, session ids)

Generational (aka model-based) fuzzing

- much more efficient
- may not catch random corner-case vulnerabilities; harder to set up

File Fuzzers

File Formats are an agreement of sorts

- what happens when this agreement breaks?
- what file types and application targets (doc viewers, media players, web browsers)?
- creating files -- byte manipulation, interesting inputs (neg/pos, max/min, empty, special)
  - these exploits may lead to buffer/integer overflows

File Fuzzers

http://msdn.microsoft.com/en-us/stopartnertest/minifuzz-overview-and-demo.aspx

1:50

takes template file(s)

SDL = security development lifecycle

Fuzzing Workflow

1. setup fuzzer to know how to access target
2. check valid responses and validate communication
3. send test cases to target
4. analyze crash results
5. fix and retest!

Fuzzing demo

SPIKE

All material, including all perl scripts and spikes are taken from THIS TUTORIAL which uses the vulnserver written by Stephen Bradshaw.

What is SPIKE?

- a C-based fuzz generator for testing network protocols
- creates fuzzed ‘SPIKES’ to send in network packets

Ollydbg

Vulnserver.exe

SPIKE

Wireshark

How would you fuzz an OS?

https://www.youtube.com/watch?v=nyCievjaPIU

How would you fuzz an online game?

https://www.youtube.com/watch?v=EVhSqWofeP8