Fuzzing In-memory Code

Dr. Jared DeMott
CTO AND FOUNDER

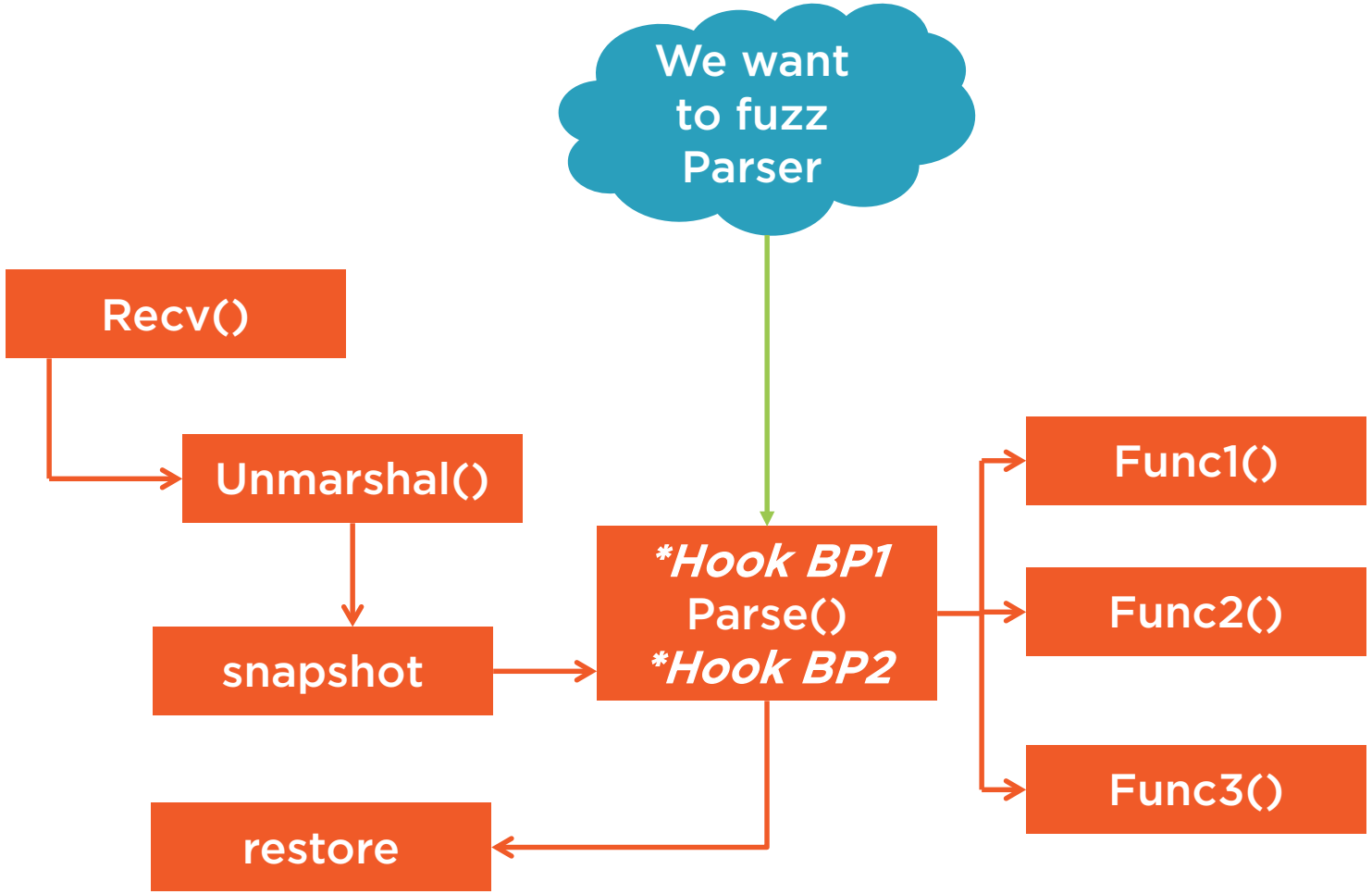
@jareddemott www.vdalabs.com

Overview

In-memory fuzzing

- Tools and techniques

Demo


We want
to fuzz
Parser
Recv()
Unmarshal()
snapshot
restore
*Hook BP1
Parse()
*Hook BP2
Func1()
Func2()
Func3()

Pros

Bypass fuzzing difficulties

- Encryption
- Poorly documented protocol
- Connection limits
- Built-in IDS

Cons

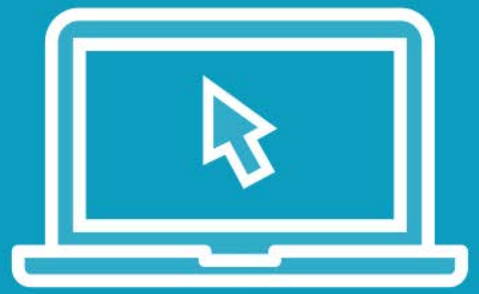
Black-box

- Poor system wide test
  - Quick check of key area
    - E.g. targeted unit test

Requires reverse engineering

- And hook/restore capability

Demo



In-memory fuzzing process

Summary

Used Pydbg and Immunity debugger to construct an in-memory fuzzing tool

Next up:

- Feedback fuzzers