Network Protocols Fuzzing

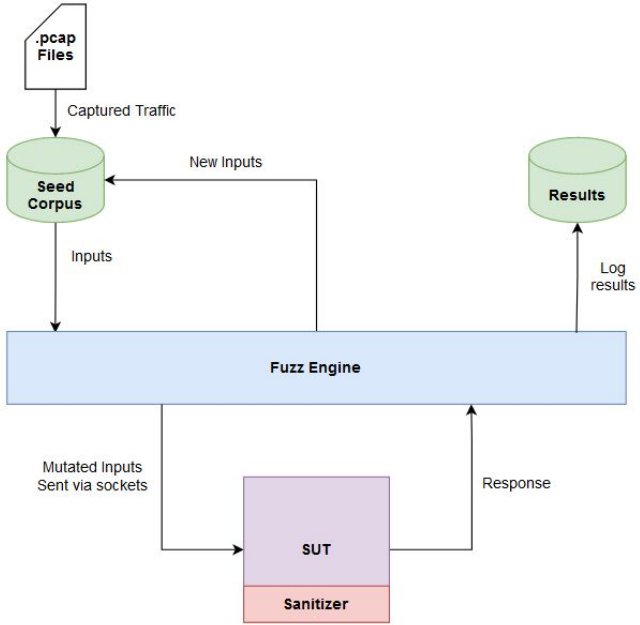
Claudiu-Florentin GHENEA
George-Andrei IOSIF

Introduction

- Network protocols
- Vulnerabilities in network protocols
- Fuzzing
  - Knowledge about the source code
  - Knowledge about the input format
  - Knowledge about the state of the process
  - Input generation technique

Attack Description

1. Establishing a way to generate the inputs
   - Giving an initial corpus, namely some valid traffic
   - Defining the protocol via a meta language
2. Sending inputs to the SUT, via sockets
3. Monitoring the state of SUT
   - Response codes
   - Instrumentation
4. Mutating the inputs accordingly
5. Jumping to the second step



Detections. Countermeasures

- Antifuzzing
- Rate limiting
- Crash reporting

Related Work

- Code review
- Taint analysis
- Symbolic execution
- Formal validation

Conclusions

- Ongoing research
  - AFLNet
  - Boofuzz
- Effective and pragmatic way to detect vulnerabilities in a network protocol
- Not a silver bullet, such as formal validation