Enabling Greybox Fuzzing for Power Distribution System

2019-03-08

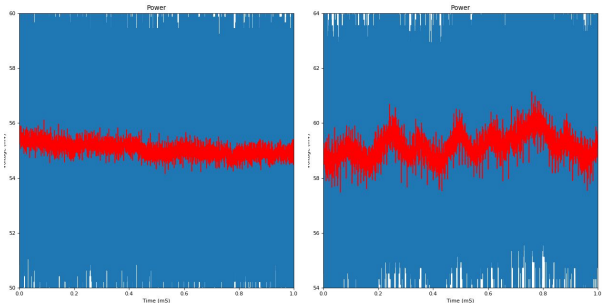
Defining the Problem

- Embedded System
  - Widely used in electricity control sys
- Threaten Model
  - Attacker utilize vulns to take control
- Challenges
  - Firmware/source are not available
  - Have no interface or debug port

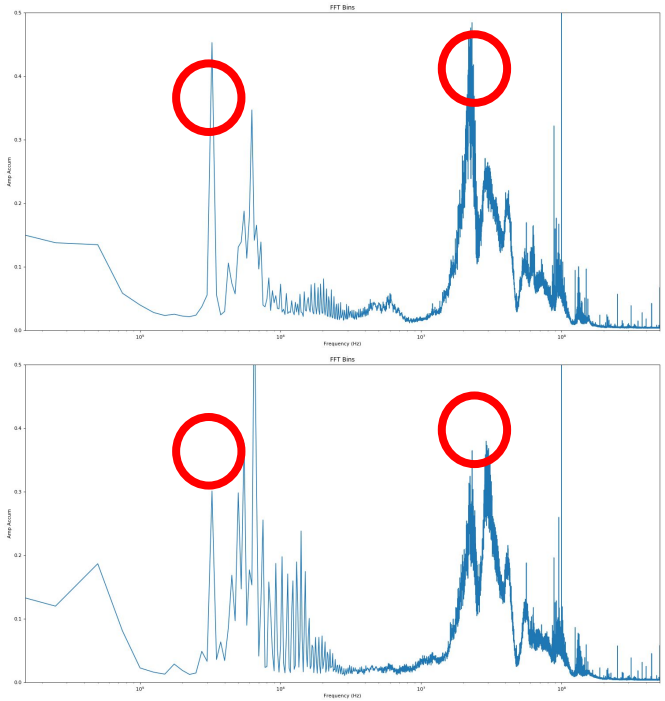
Finding Vulnerability

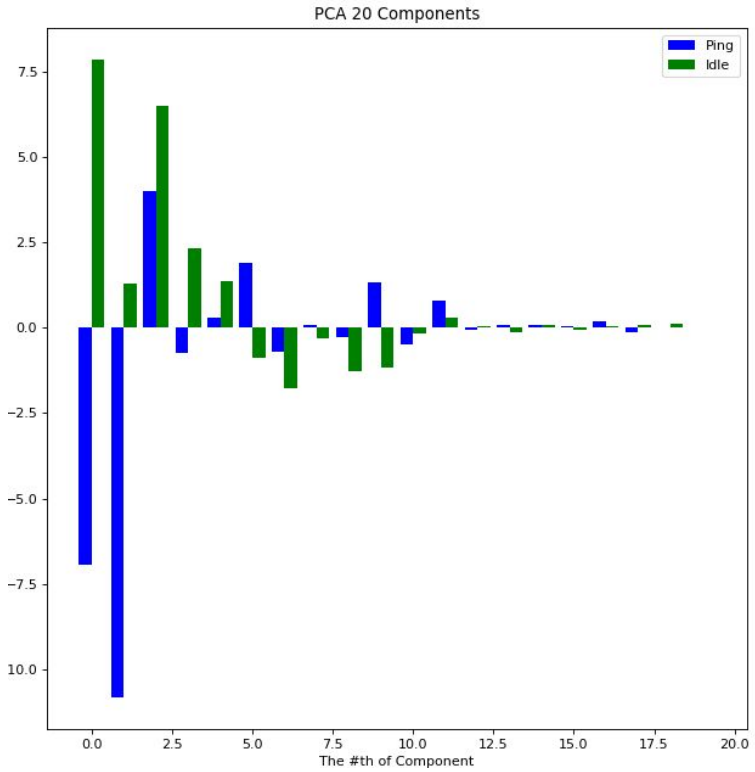
- Find a crash $\simeq$ find a vulnerability
- Method: fuzzing
  - Generate diff. inputs to reach a crash
  - Need prog. state(coverage / crash)
- System states: power side-channel
  - Solve the issues of no interface
  - Diff. state shows diff. power trace

Previous Result

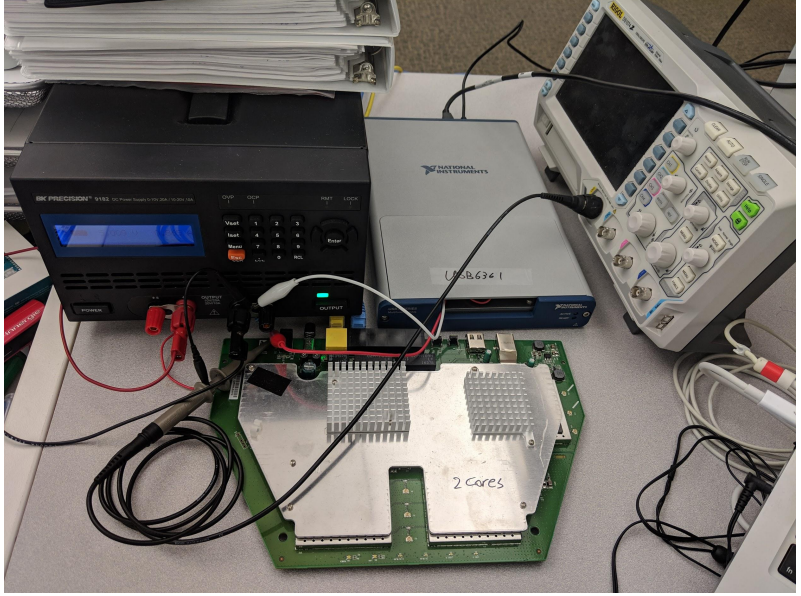


- Distinguishing state of idle & ping
  - DFT + PCA



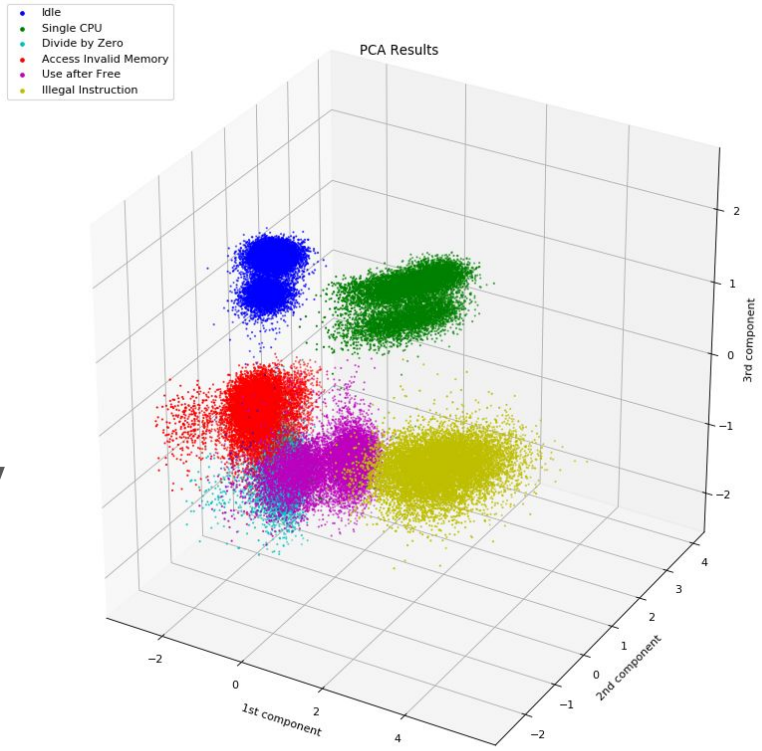


Data Collection



- Data-Acquisition
  - NI USB-6361
  - 2M/s sampling, 10M pts buffer, cont. mode
- D-Link 890L home router
  - 6 states: idle, normal, illegal instr., invd. mem access, div by 0, UAF

Exp. Results



- Customized Binary
  - Measure power
    on diff. states
    -> FFT -> PCA -> SVM -> Evaluate
- Cross-Validation: Accuracy 95+%
  - 10000 samples on each state
  - 3-5 principal components in PCA

Next Steps

- Applying to real programs
  - Build model on sampling data
  - Test on traces of real programs
- Use state info to help fuzzing
- Apply our work to more devices
  - Arduino, ARM Cortex-M0