Overview

Carnegie Mellon University

- **Edge cases matter**
  - Robust perception matters
- **The heavy tail distribution**
  - Fixing stuff you see in testing isn't enough
- **Perception stress testing**
  - Finding the weaknesses in perception

[General Motors]

98% Solved For 20+ Years

Carnegie Mellon University

- **Washington DC to San Diego**
  - CMU Navlab 5
  - Dean Pomerleau
  - Todd Jochem

    https://www.cs.cmu.edu/~tjochem/nhaa/nhaa_home_page.html
- **AHS San Diego demo Aug 1997**

What About Edge Cases?

Carnegie Mellon University

- **You should expect the extreme, weird, unusual**
  - Unusual road obstacles
  - Extreme weather
  - Strange behaviors

PREDICTED CONCEPT	PROBABILITY
bird	0.997
no person	0.990
one	0.975
feather	0.970
nature	0.963
poultry	0.954
outdoors	0.936
color	0.910
animal	0.908

https://www.clarifai.com/demo

- **Edge Case are surprises**
  - You won't see these in testing

➔ Edge cases are the stuff you didn't think of!

Why Edge Cases Matter

Carnegie Mellon University

- **Where will you be after 1 Billion miles of validation testing?**
- **Assume 1 Million miles between unsafe "surprises"**
  - Example #1:
    100 "surprises" @ 100M miles / surprise
    - All surprises seen about 10 times during testing
    - With luck, all bugs are fixed
  - Example #2:
    100,000 "surprises" @ 100B miles / surprise
    - Only 1% of surprises seen during 1B mile testing
    - Bug fixes give no real improvement (1.01M miles / surprise)

https://goo.gl/3dzguf

ML Is Brittle To Environment Changes

Carnegie Mellon University

- **Sensor data corruption experiments**

Defocus & haze are a significant issue

Synthetic Equipment Faults

Gaussian Blur & Gaussian Noise cause similar failures

Exploring the response of a DNN to environmental perturbations from “Robustness Testing for Perception Systems,” RIOT Project, NREC, DIST-A.

Ways To Improve AV Safety

Carnegie Mellon University

- **More safety transparency**
  - Independent safety assessments
  - Industry collaboration on safety
- **Minimum performance standards**
  - Share data on scenarios and obstacles
  - Safety for on-road testing (driver & vehicle)
- **Autonomy software safety standards**
  - Traditional software safety … ***PLUS*** …
  - **Dealing with surprises and brittleness**
  - Data collection and feedback on field failures

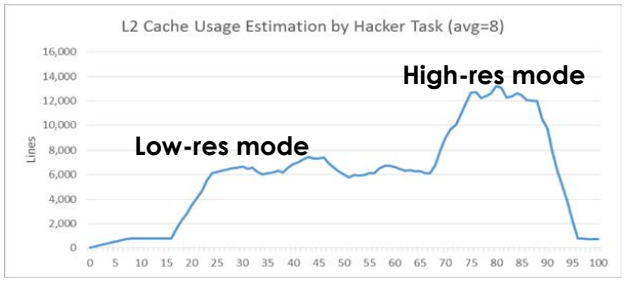
http://bit.ly/2MTbT8F (sign modified)

Outline

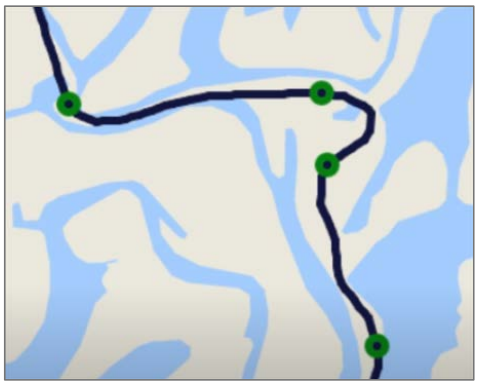
- **ScheduLeak**: methods to leak schedule information
- **Contego:** Integrate security & maintain real-time requirements

Demonstration 1
Cache-Timing Side-Channel Attack

- Attack Goals:
  - Probe (coarse-grained) memory usage of victim task
  - Recover locations of interest → points where memory usage (of victim task) is high



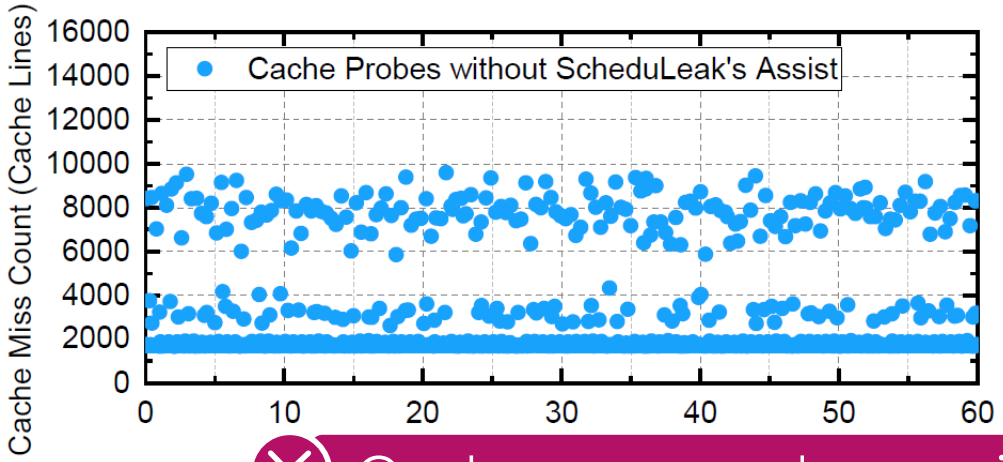
Measurements on Xilinx Zedboard Zynq-7000, FreeRTOS, [CPU Freq: 666MHz, L2 Cache: 512KB, 32 byte line size]

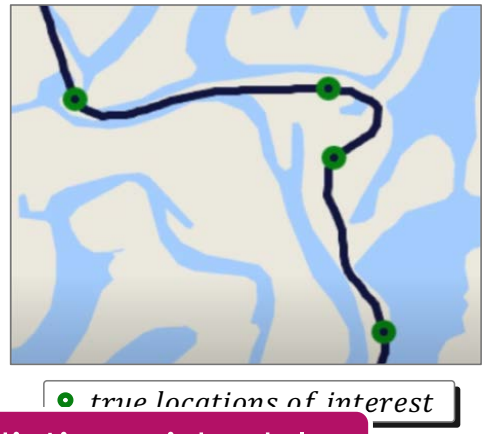


true locations of interest

Demonstration 1
Cache-Timing Side-Channel Attack

- **Without** ScheduLeak–based information
  - Attackers are forced to **randomly sample** the system
  - To detect memory usage changes

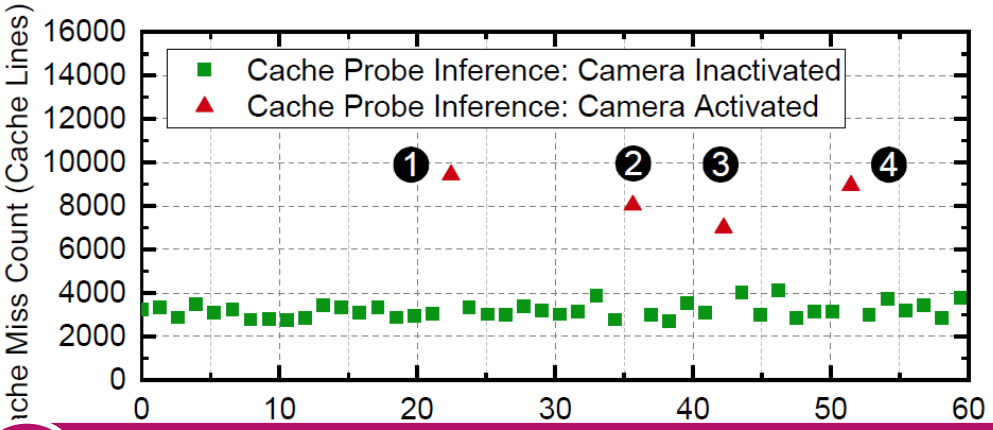




✗ Cache usage probes are indistinguishable

Demonstration 1
Cache-Timing Side-Channel Attack

- **With precise timing information** from ScheduLeak
  - Attackers can launch cache-timing attack at more precise points
  - **Very close to the execution of the victim task**



✓ Four locations are recovered from the cache usage probes

Contego

- Allow security tasks to run in two modes:
  - **PASSIVE**
    - Execute opportunistically with lowest priority
  - **ACTIVE**
    - Switch to other (active) mechanisms if abnormality is detected

Contego Example