Who's In Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems

David Formby[1], Preethi Srinivasan[1], Andrew Leonard[2], Jonathan Rogers[2], Raheem Beyah[1]

Communications Assurance and Performance (CAP) Group
School of Electrical and Computer Engineering[1]

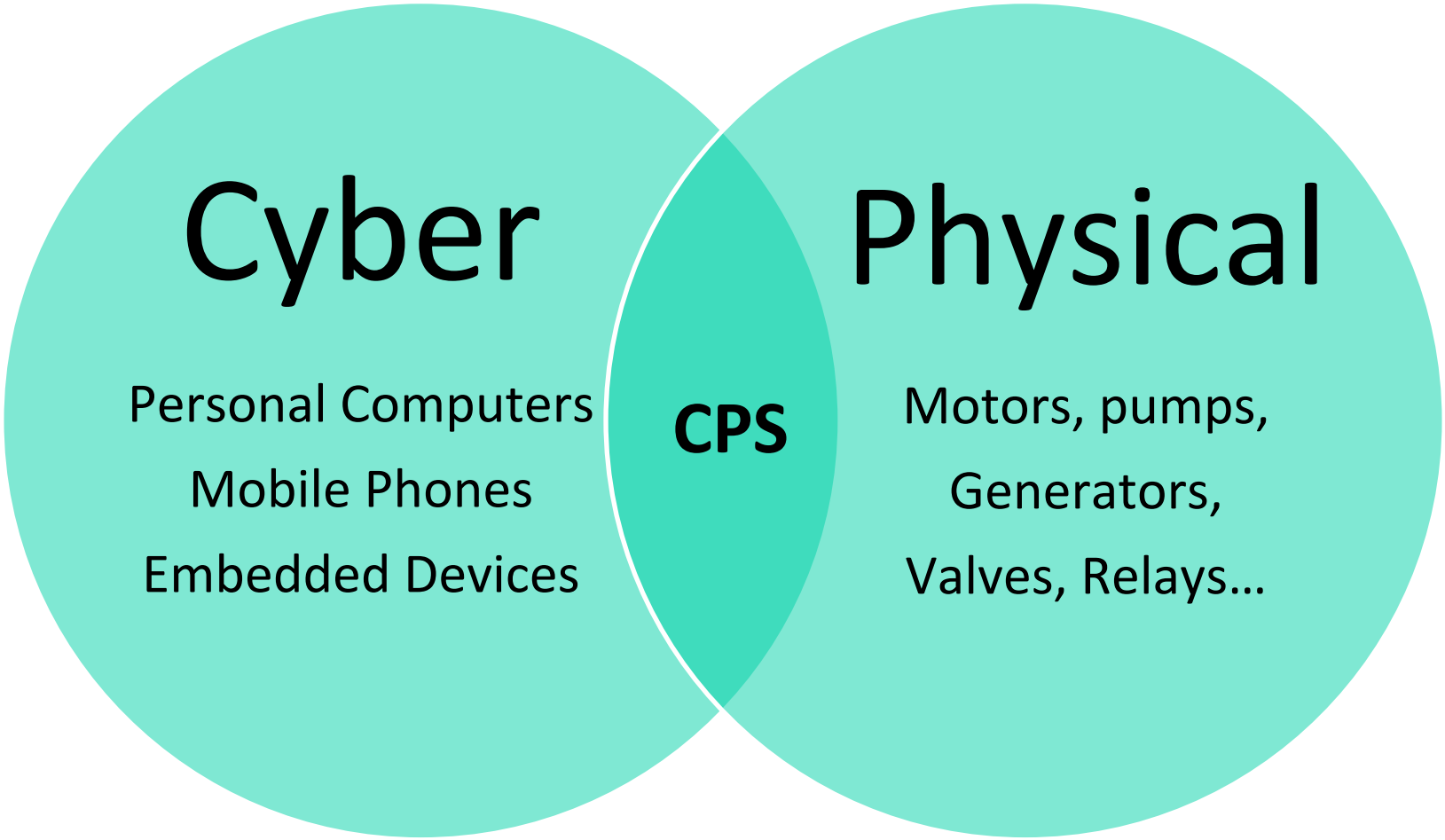
School of Mechanical Engineering[2]
Georgia Institute of Technology

Georgia Institute of Technology

CAP Communications Assurance & Performance Group

@GTCAPGROUP

Cyber-Physical Systems (CPS)



Cyber-Physical Systems

- Industrial control systems (ICS)
  - Power grid, water/sewage, oil/gas, manufacturing, supervisory control and data acquisition (SCADA)
- Home automation
  - Lighting, locks, thermostat, security system

Vulnerabilities can lead to physical harm
ICS filled with vulnerable, legacy devices

ICSA-15-041-02
ICSA-15-006-01
ICSA-15-169-01B
https://ics-cert.us-cert.gov/advisories

Georgia Institute of Technology

COP Communications Assurance & Performance Group

Motivation

- ICS vulnerable to false data injection and false command responses
  - Can push system into unsafe state, cause physical harm
  - Previous fingerprinting work not suited for ICS
  - False data detection and IDS have limitations

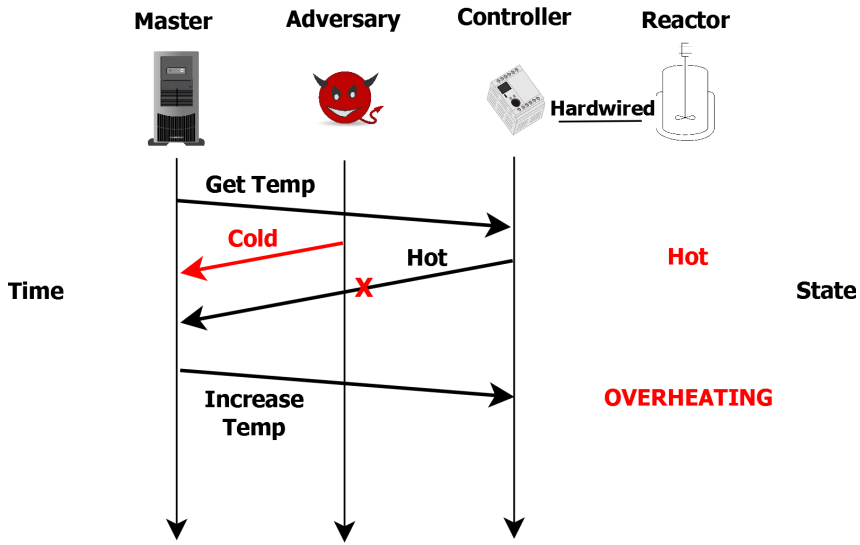
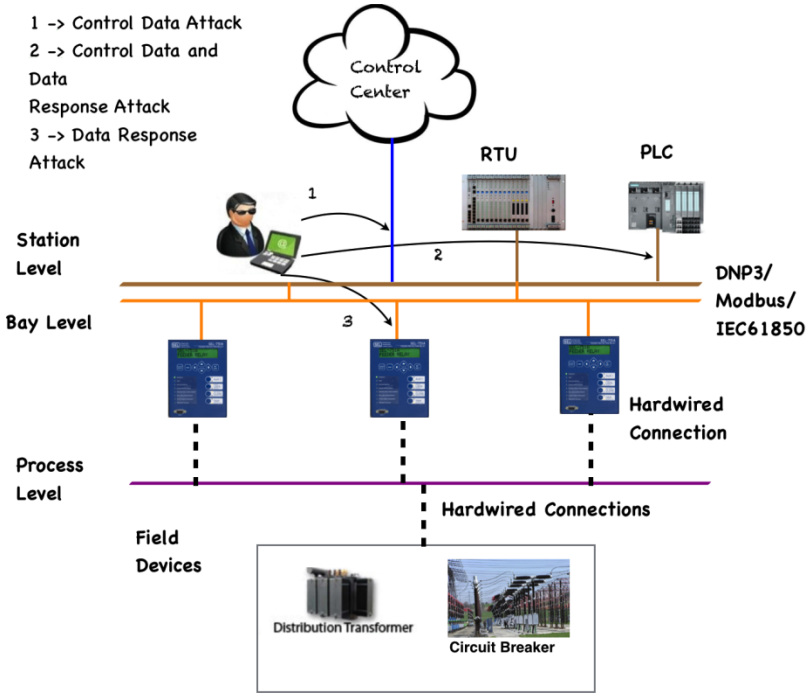


Illustration of simple false data injection

- CPS fingerprinting helps defend against these attacks

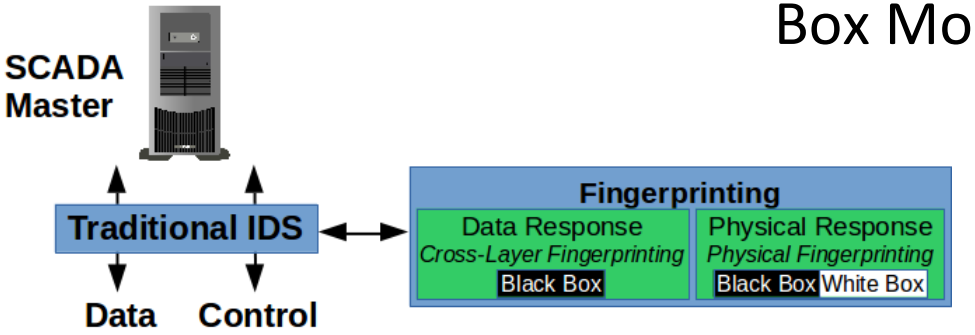
Attacker Model

- Two cases
  - Compromised PLC
    - Stuxnet
  - Physical access
    - Insider
    - Weak physical security
- Goal
  - Inject false data and command responses while masquerading as a different device



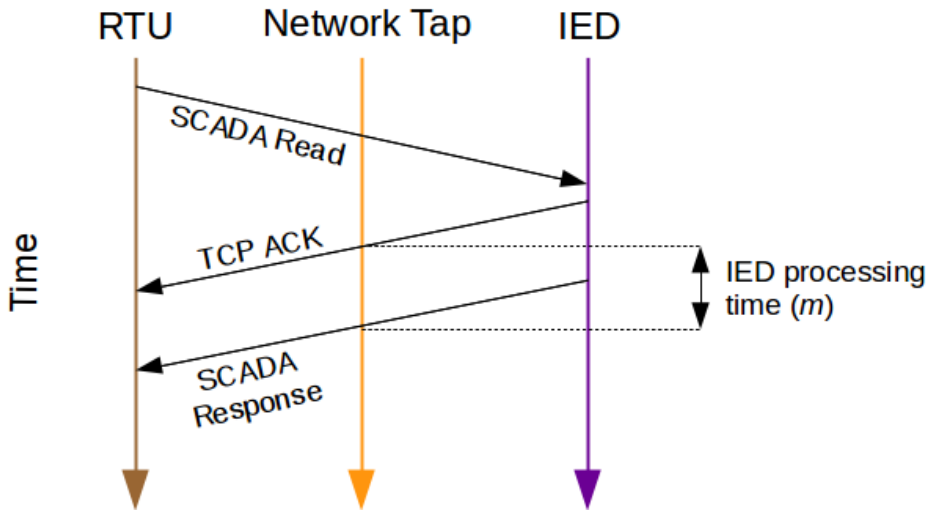
CPS Fingerprinting

- Data Acquisition
  - Cross Layer Response Time (CLRT)
  - Estimate device processing time
  - Black Box Model fingerprints
- Control
  - Physical fingerprinting
  - Estimate physical operation time
  - Black Box Model fingerprints
  - *New class* of fingerprinting - White Box Modeling



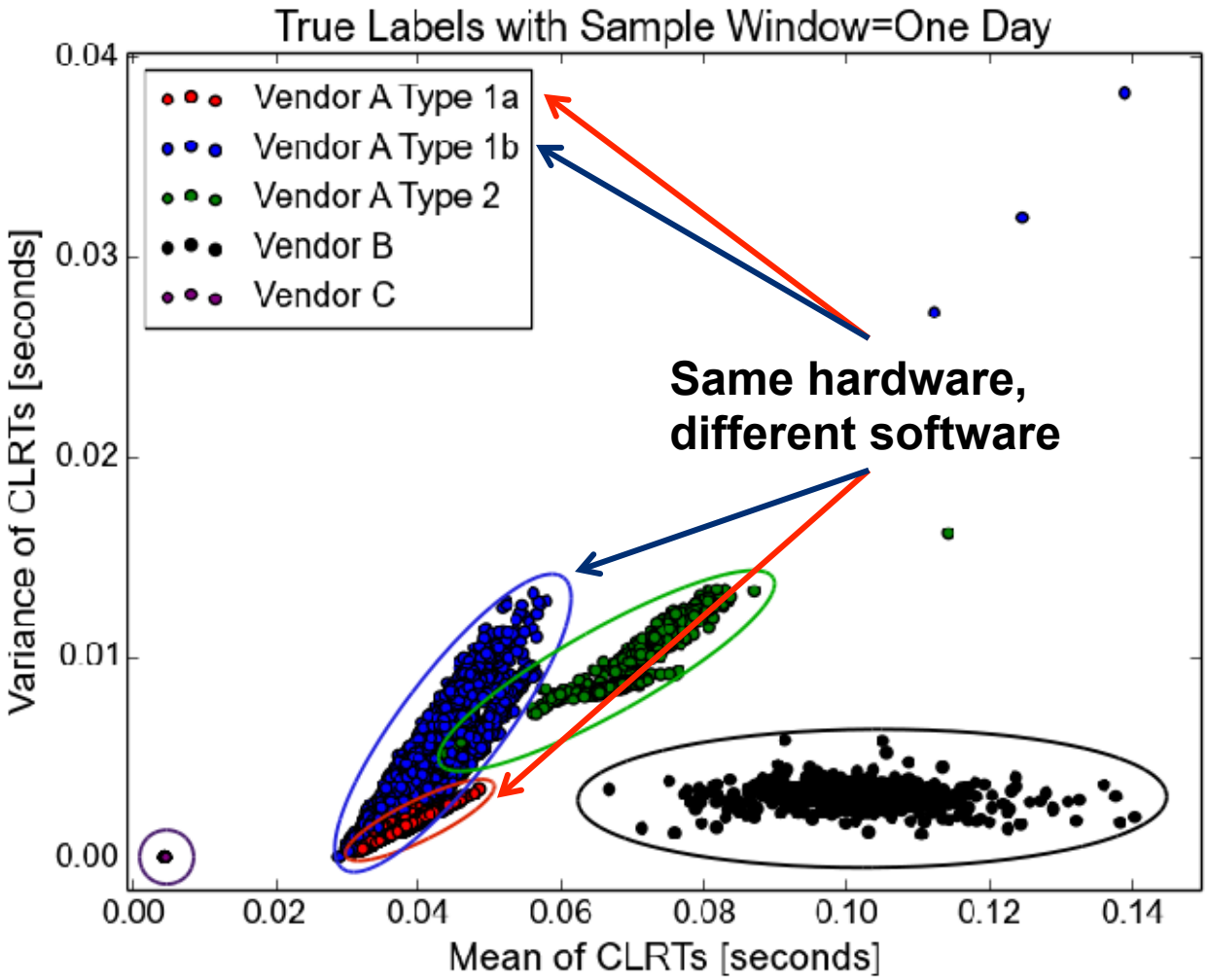
Cross-Layer Response Time (CLRT)

- Fingerprints devices from data acquisition traffic
- Estimates device processing time
  - Time between TCP ACK and SCADA response
  - Fast links (100Mbps) with slow devices, slow and regular traffic

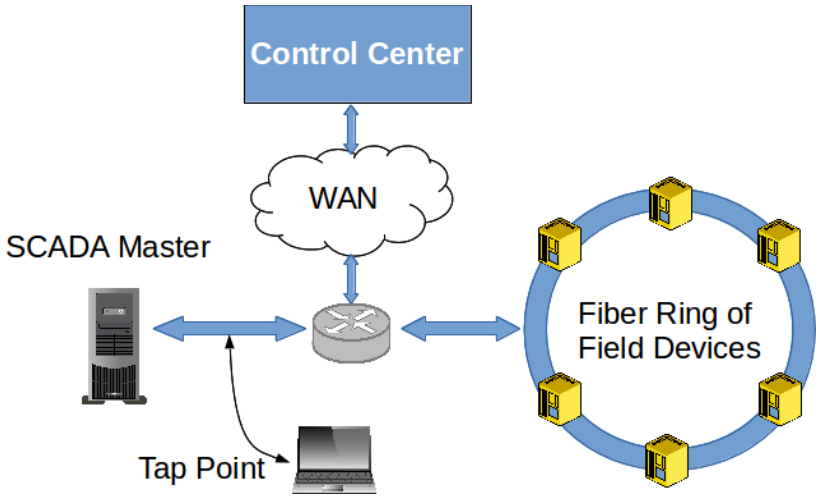


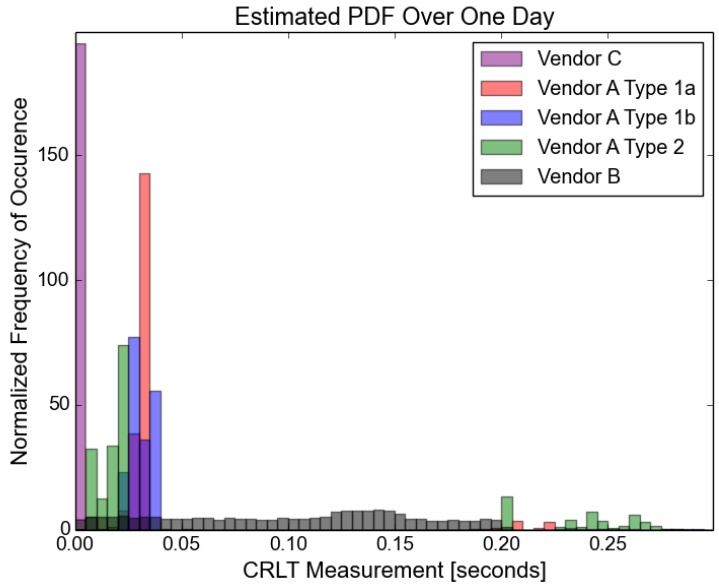
Adversary cannot simply respond faster to beat IED, must match the CLRT fingerprint

CLRT Clusters



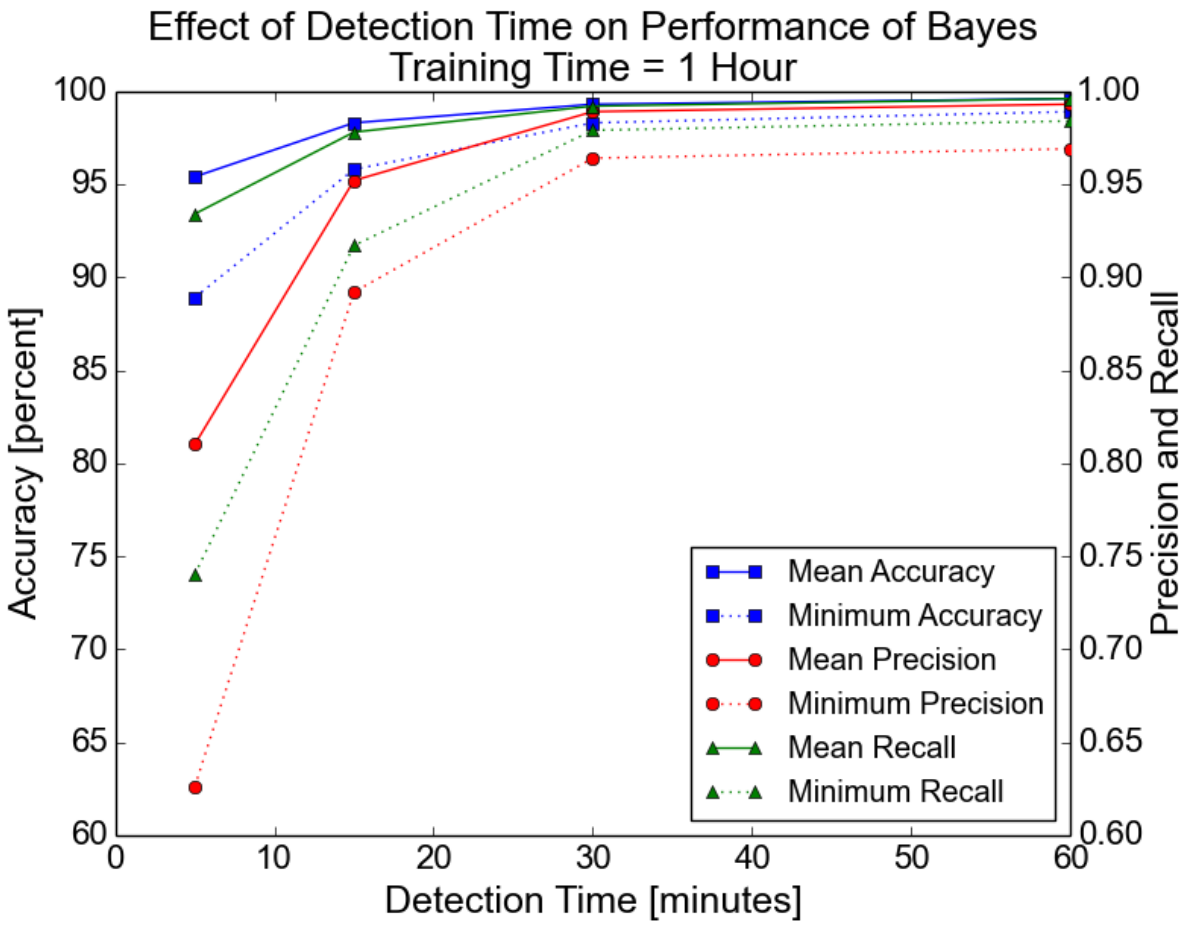
Cross-Layer Response Time





- Network Architecture
  - 100Mbps fiber links
  - Path distance ranged from 1 switch at 10 yards, to roughly 30 switches around 10 miles away
    - Devices still had same signature no matter the distance

Cross-Layer Response Time



Accuracy

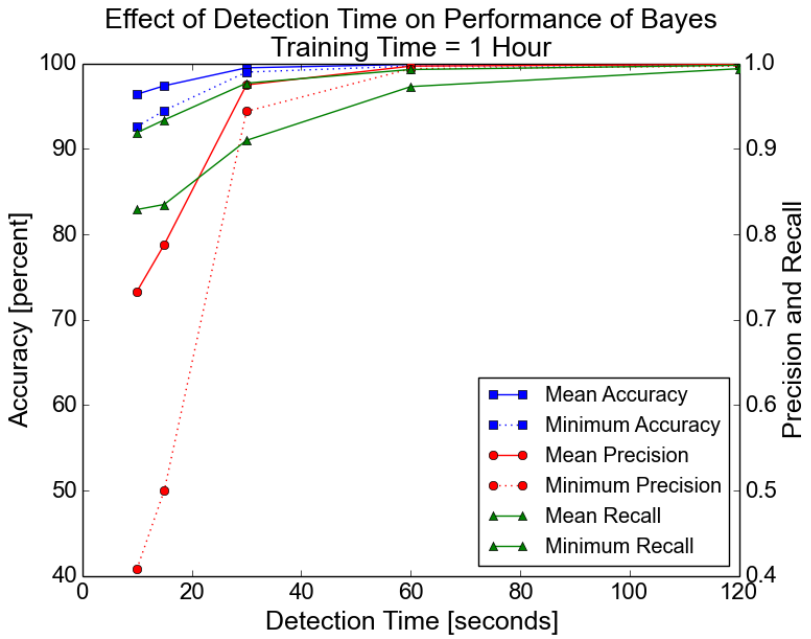
Precision

Recall

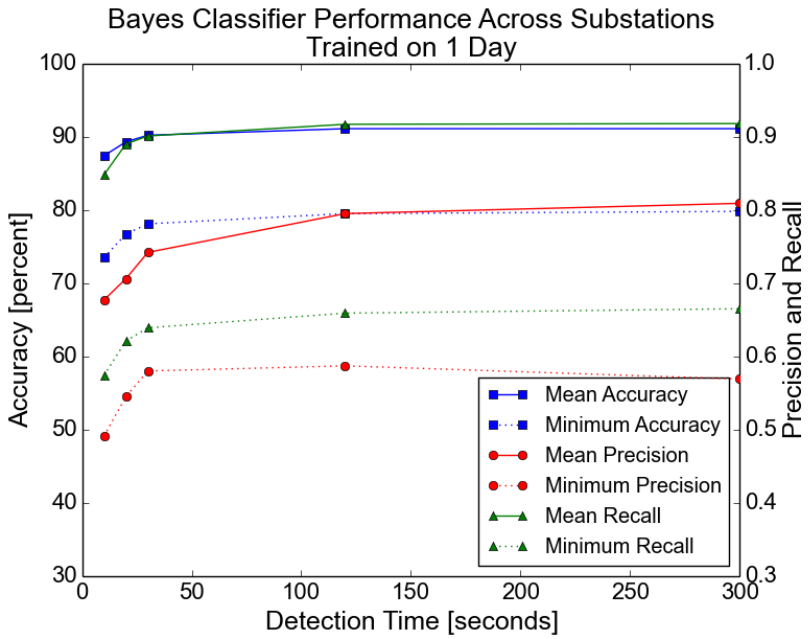
Detection time – Time to gather samples before making a decision

Cross-Layer Response Time

- Network architecture found to have minimal effect



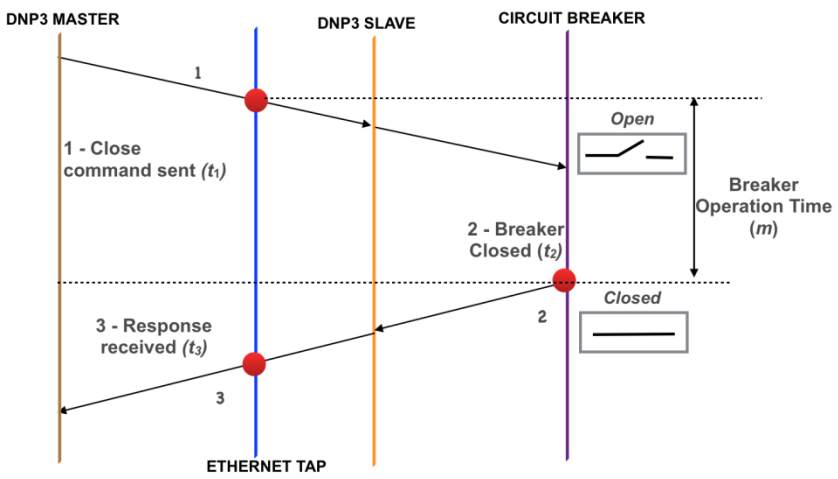
Training Data – Original dataset
Testing Data – Upgraded network



Training Data – Original dataset
Testing Data – Different substation

Physical Fingerprinting

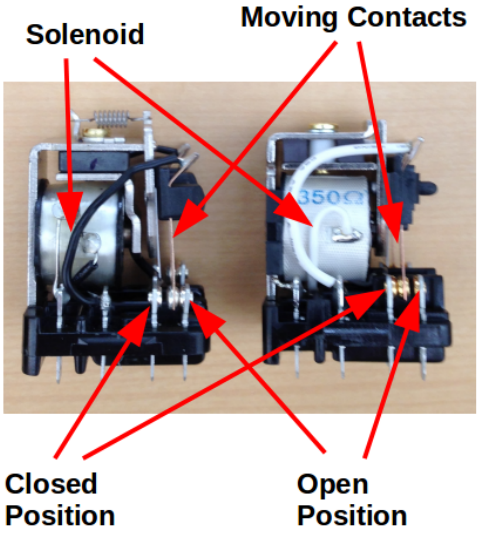
- Fingerprint devices from control traffic
- Estimate physical operation time
  - Time between command packet and event timestamp
- Black Box and White Box Methods



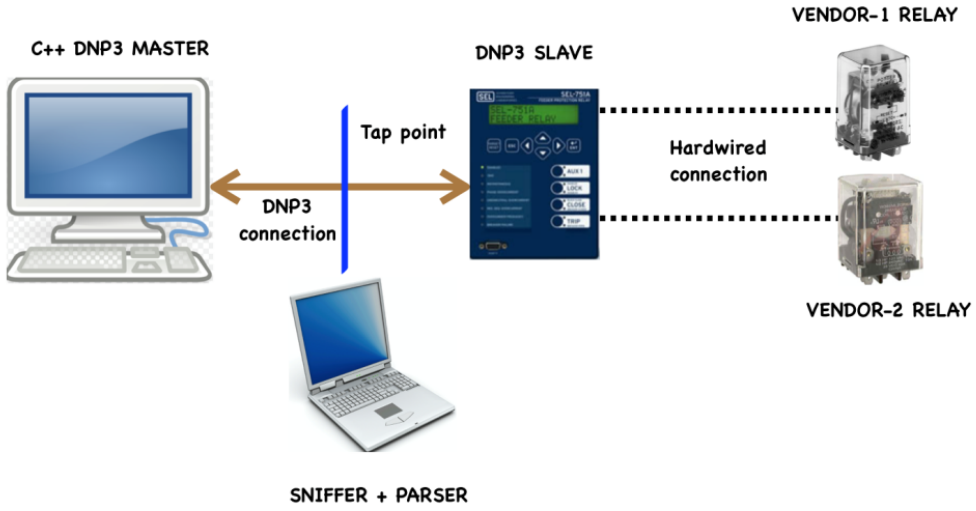
Adversary must guess what event timestamp to respond with

Physical Fingerprinting Setup

- Relays – Typically used to open or close higher voltage circuits with a lower voltage signal. Common device in ICS and analogous to large scale circuit breakers

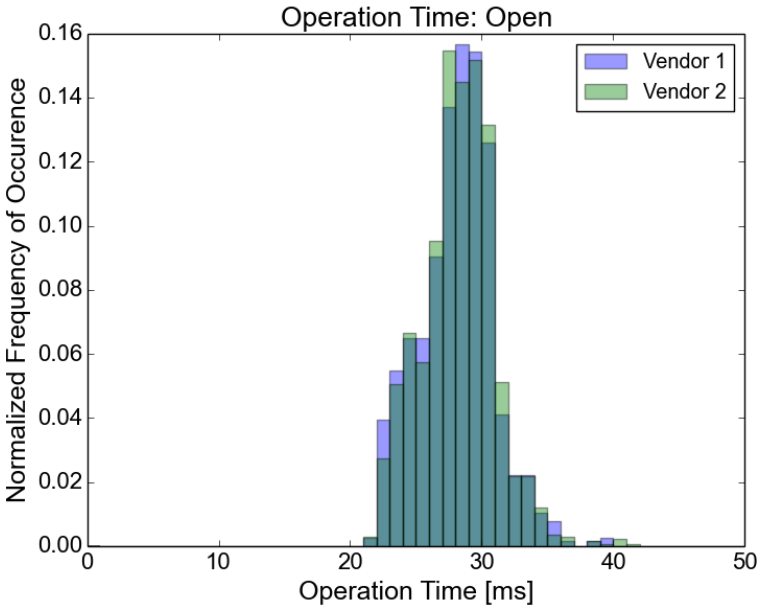


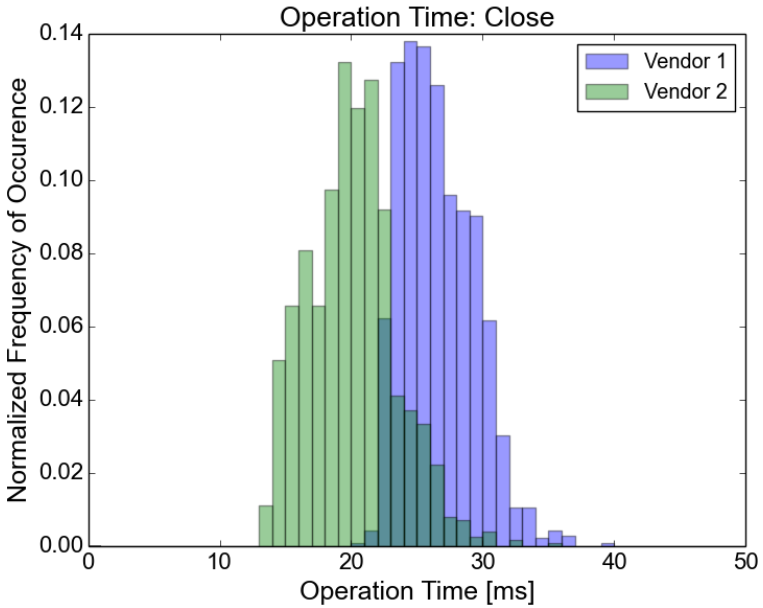
Relays used in testbed, nearly identical specifications



Testbed setup

Physical Fingerprinting Results





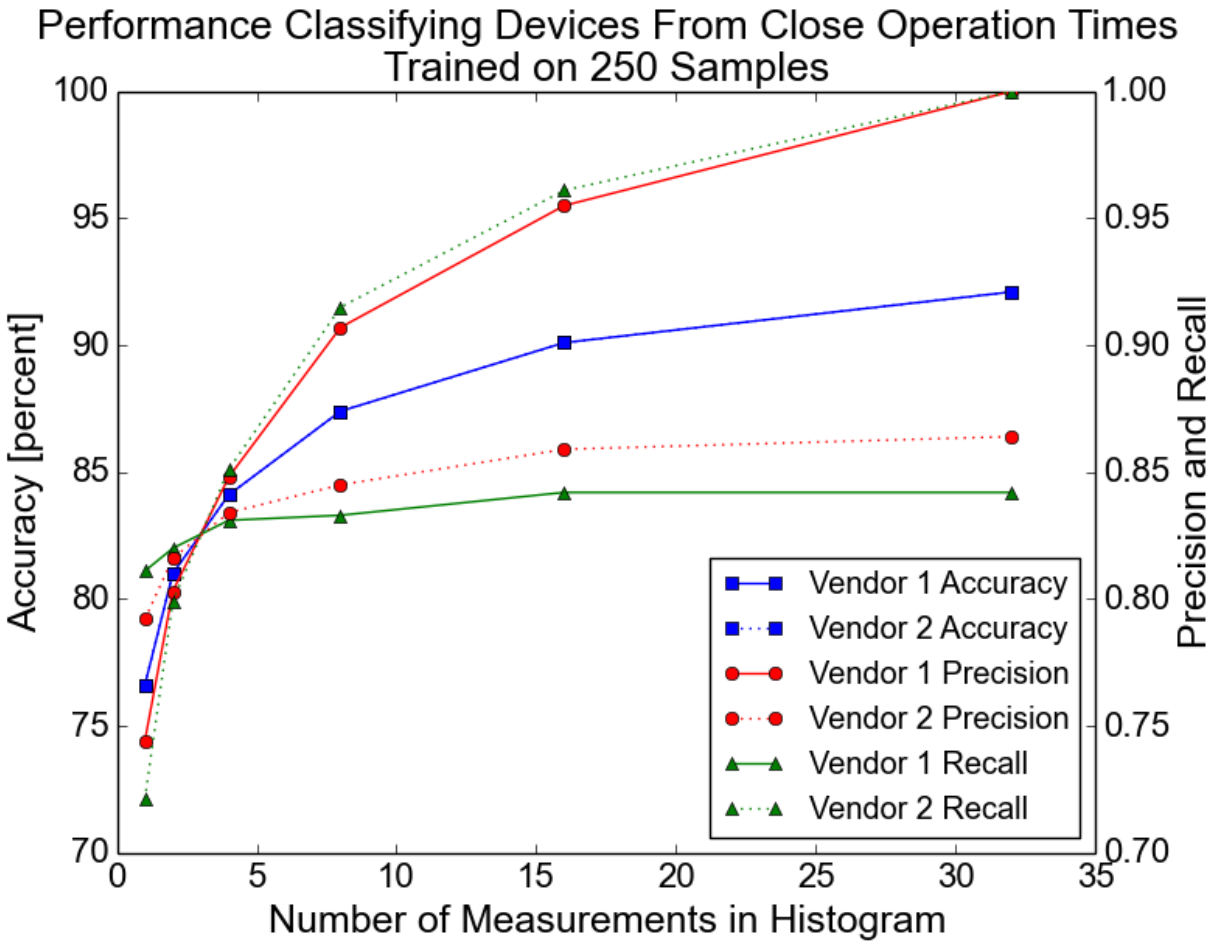
No obvious differences between Open operations due to nearly identical ratings.

Clear differences in Close operations allow for device fingerprinting.

Georgia Institute of Technology

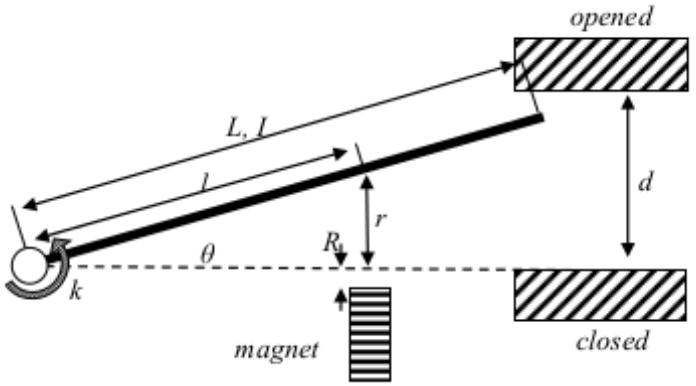
CAP Communications Assurance & Performance Group

Physical Fingerprinting Results



White Box Modeling

- Black Box Modeling sometimes infeasible
  - Operate infrequently, no physical access
- Construct physical model and estimate parameters



White Box Modeling

Current in coil

$$\alpha(t) = 1 - e^{-t/\tau}$$

Magnetic field

$$\phi(t) = \frac{2}{\pi}\tan^{-1}(\beta\alpha(t) - \gamma)$$

Permanent magnet force

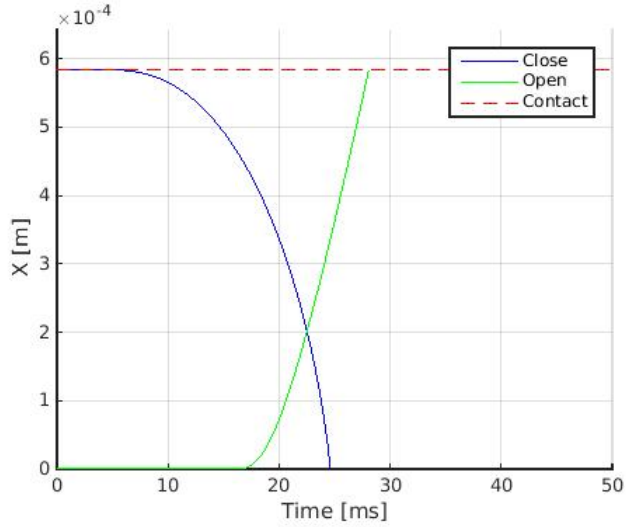
$$F_p = \frac{c_p\mu_0}{(r+R)^2}\phi(t)$$

Coil Force

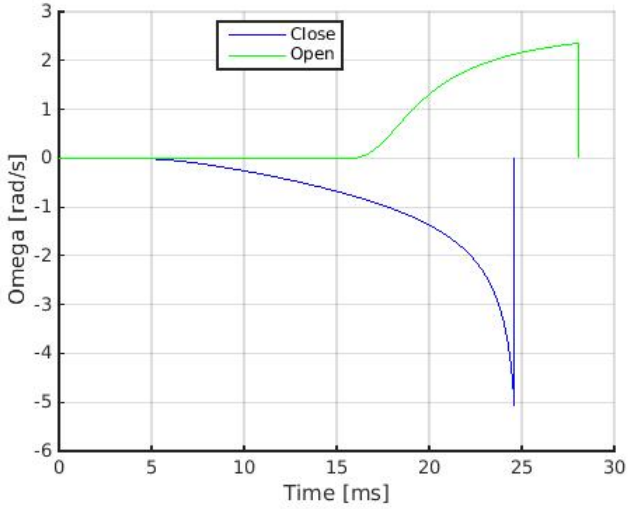
$$F_c = \frac{c_c\mu_0}{(r+R)^2}\alpha(t)$$

Equation of motion

$$\ddot{\theta} = I^{-1}(F_p l\cos\theta + F_c l\cos\theta + k\theta)$$

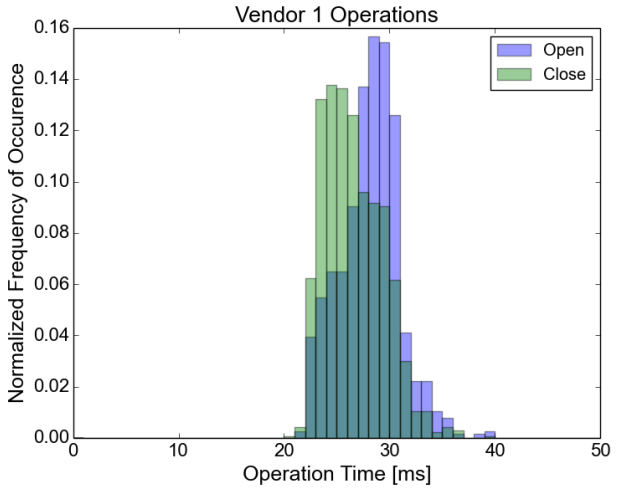


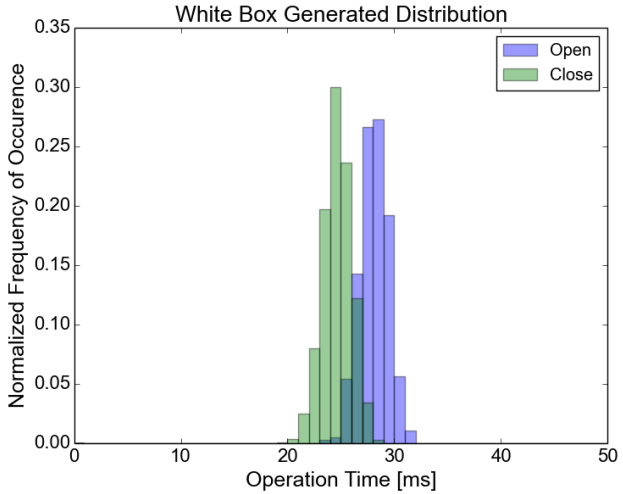
Armature displacement

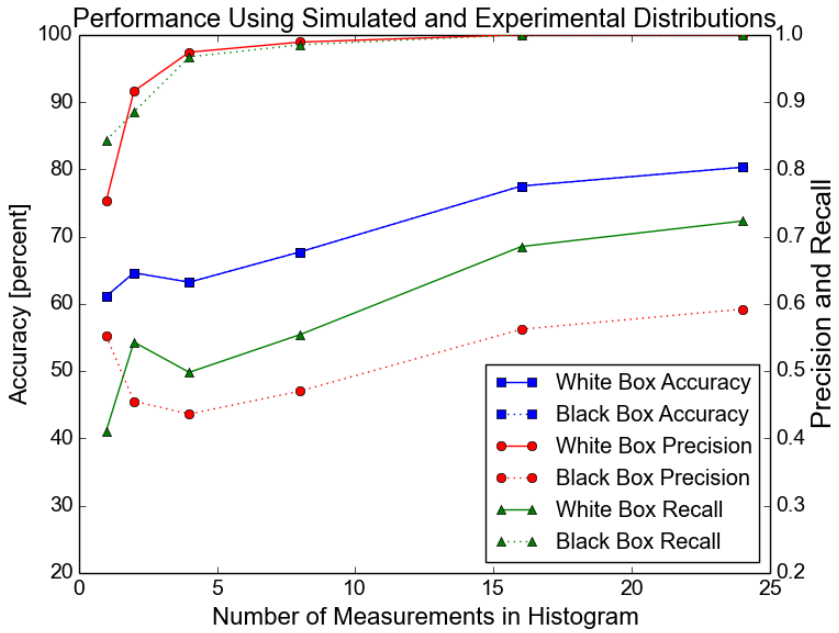


Armature angular velocity

White Box Modeling Results







Reduced accuracy, but could be refined as true samples become available

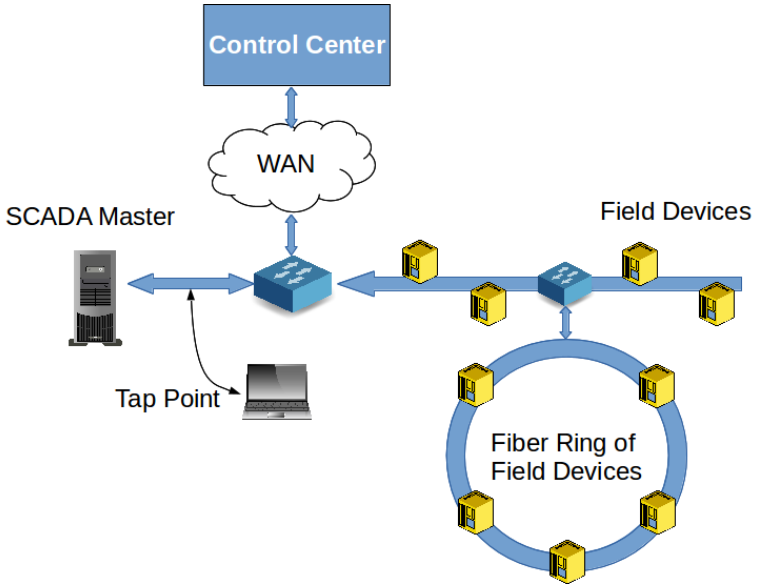
Discussion

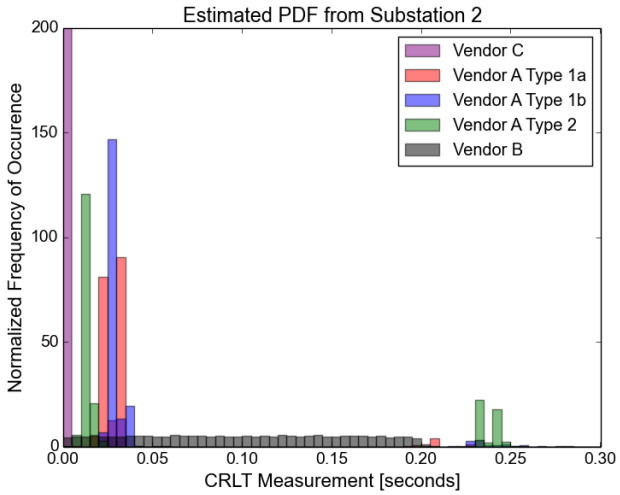
- Assumptions
  - TCP Quick ACKs for CLRT and timestamps for physical
- Accuracy: 99% and 92%
  - Not high enough for stand-alone IDS, but can complement traditional IDS
- White Box Modeling
  - Reduced accuracy and requires some expertise, combine with “gray box” modeling to overcome
- Strength Under Mimicry Attack
  - Skilled adversary would evade detection, countermeasures could randomize requests, send extra

Conclusion

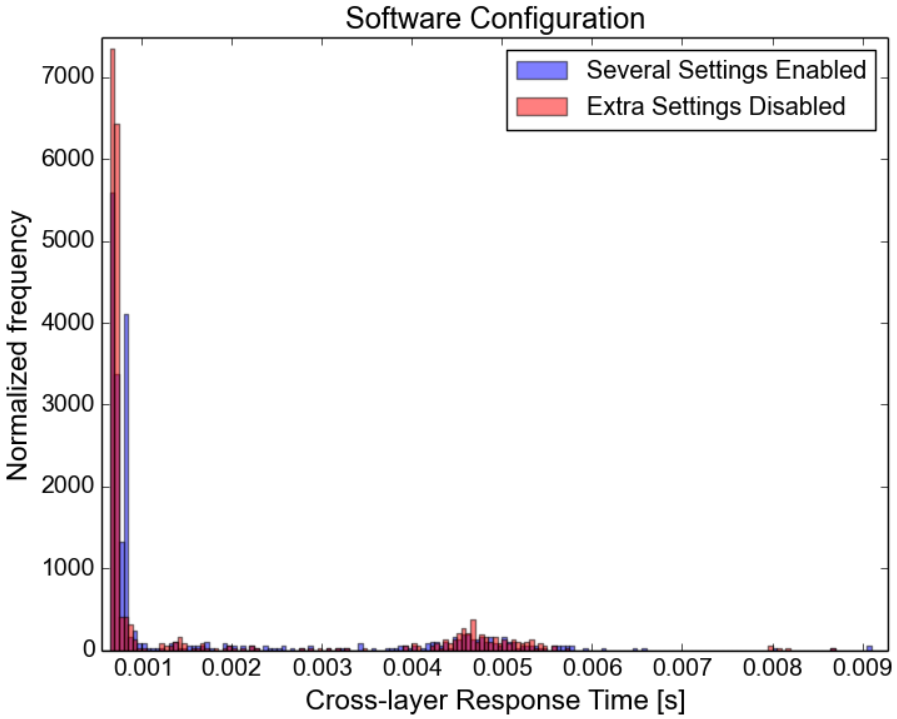
- Novel passive fingerprinting techniques for ICS
  - Data acquisition and control
  - 99% and 92% classification accuracy
  - Inventory and complementing traditional IDS
  - Resistant to simple mimicry attacks
- New class of fingerprinting – White Box Models
- Future work
  - Internet of Things, developing white box methods

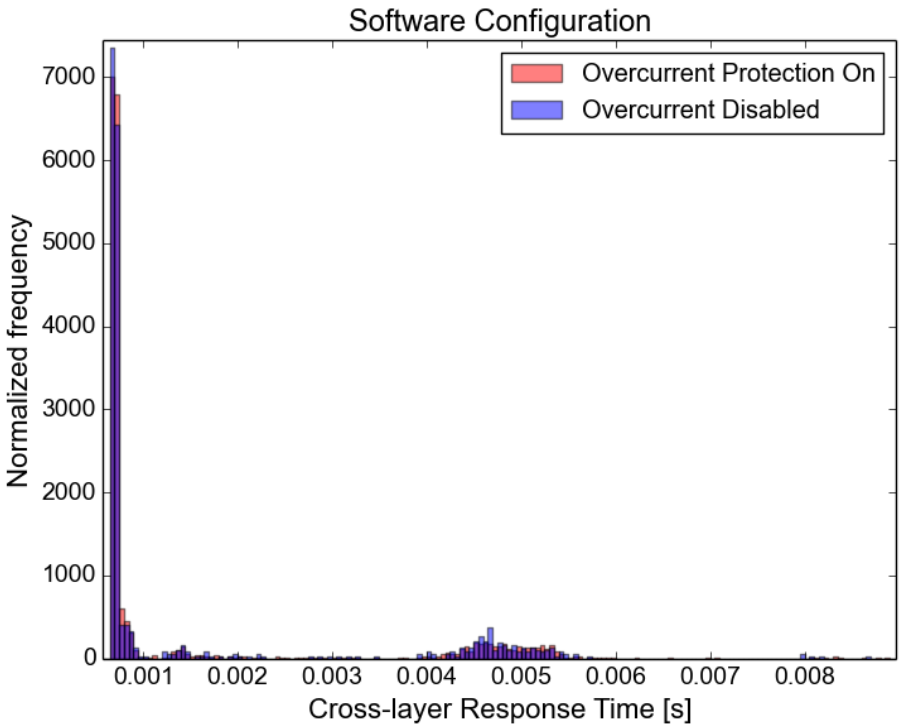
Backup – Across Substations



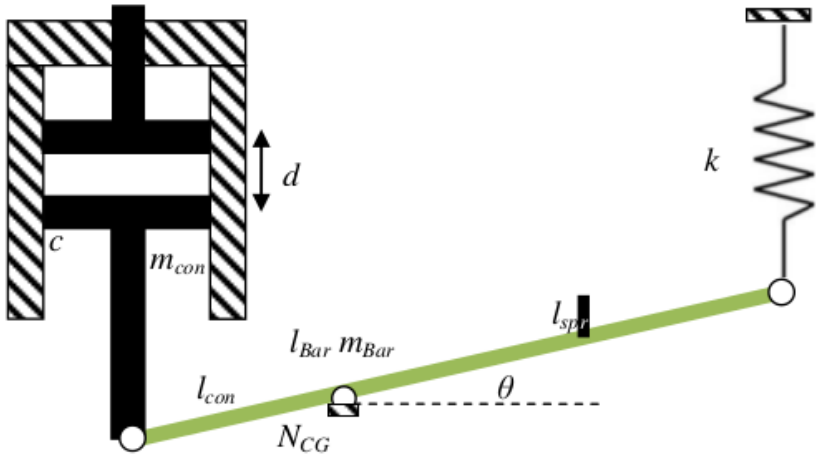


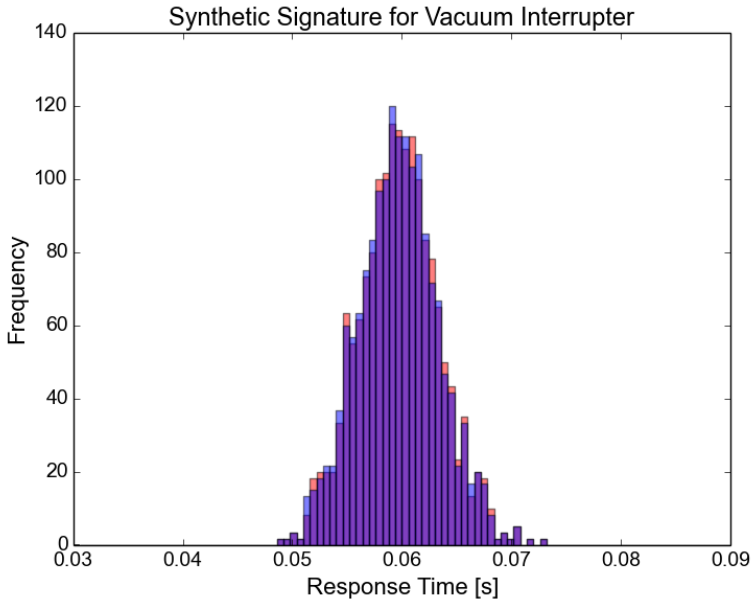
Backup - Software





Backup – White Box





Backup – Mimicry Attacks

- Weak Adversary
  - Simulate compromised PLC
  - BeagleBone Black at 300MHz, 512MB RAM
- Strong Adversary
  - Simulate on-site attacker
  - Desktop with 3.4 GHz quad-core i7, 16GB RAM
- Goal
  - Given the target distributions, masquerade as target device while responding to read requests

Backup – Mimicry Attacks