Everybody Jammin' Up on Those Tings: Challenges for the Internet of Insecure Things

Kevin Butler

Forum on Internet of Things: Smarter Living in the Caribbean
Port of Spain, Trinidad & Tobago
28 April 2017

IoT: The Promise

- Many industries can be transformed by IoT - smart homes, smart cities, cars, agriculture, data collection
- Estimates: 5 billion devices deployed in 2015, 24 billion devices deployed in 2020
  - Global market of US **$13 Trillion**

IoT: The Current Reality

https://www.youtube.com/watch?v=n5lj63-nc5g

OK Google...

The “Smart” Home

ADD TO COMPARE

5.8 cu. ft. Flex Duo™ with Dual Door Freestanding Gas Range

NX58K7850SG/AA

COLOR

★★★★½ (11) Write a review

- Flex Duo ™ with Dual Door - Ultimate cooking flexibility
- Wi-Fi Connectivity - Remotely monitor and control your cooktop and oven
- Possibly maybe burns your house down while you're away
- Powerful Cooktop - Cook faster with 57K BTU on 5 burners simultaneously

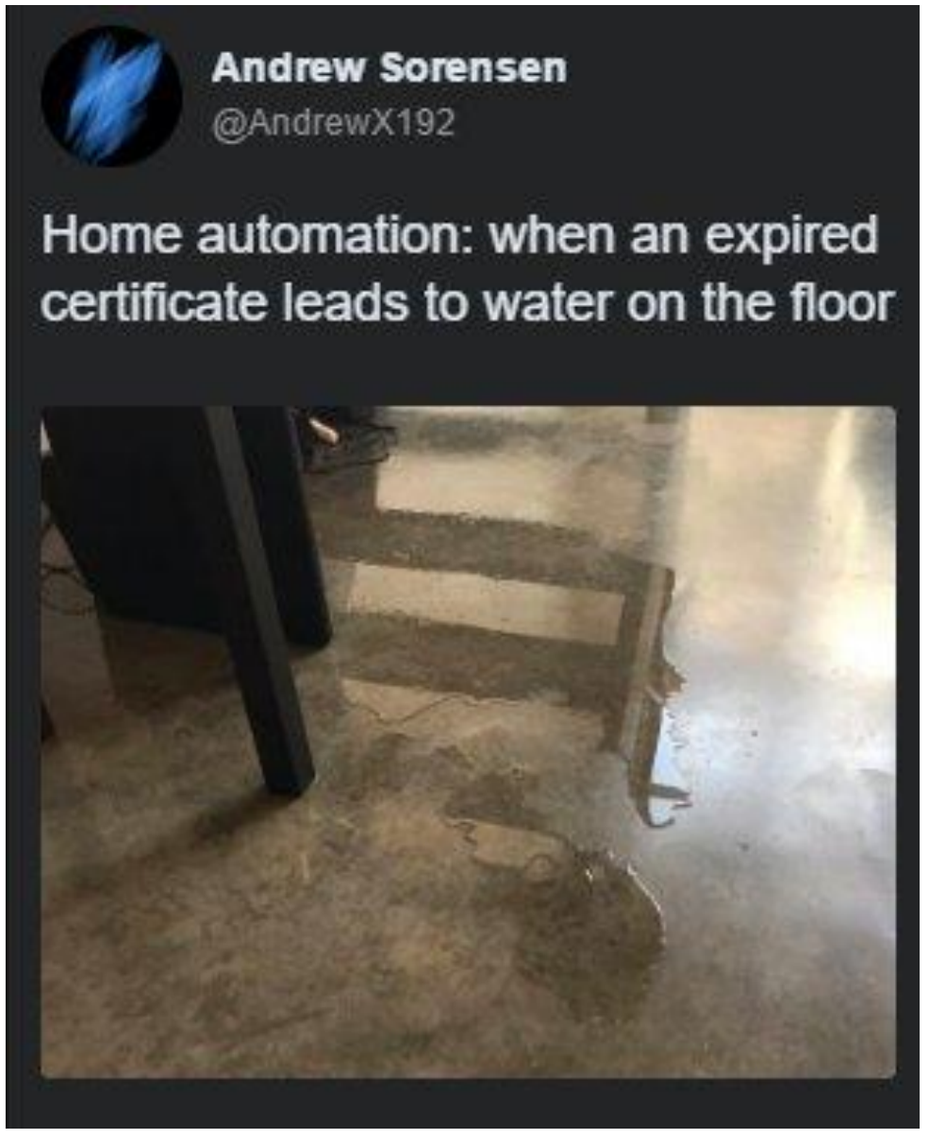
SUGGESTED PRICE: **$2,199.00**

Find Online or Locally

It's unclear which libraries Miele used to craft the Web server, which means without a fix from the vendor – *for a **dishwasher*** – the best option is to make sure the appliance isn't exposed to the Internet.

And because Miele is an appliance company and not a pure-play IT company, it doesn't have a process for reporting or fixing bugs.

The “Smart” Home



The “Smart” Home

garadget

2d

Martin,

The abusive language here and in your negative Amazon review, submitted minutes after experiencing a technical difficulty, only demonstrates your poor impulse control. I'm happy to provide the technical support to the customers on my Saturday night but I'm not going to tolerate any tantrums.

At this time your only option is return Garadget to Amazon for refund. Your unit ID 2f0036... will be denied server connection.

Global Consequences

- Mirai botnet: took control of millions of Internet-connected home automation devices
  - Used these devices to conduct a massive DDoS attack against Internet infrastructure, rendering many Internet services (e.g., PayPal, Twitter, Amazon) unusable for hours
    - Patches were available but not deployed by users
    - In some cases software updates wouldn't work for patching devices, requiring device return to manufacturer
- "Bricker-bot" attacks: permanent DoS attacks designed to destroy devices that they infect
  - Erase code and data, corrupt storage, sever network connection

Why are Things Insecure?

There are fundamental problems with the way IoT devices interact with each other and with the larger network.

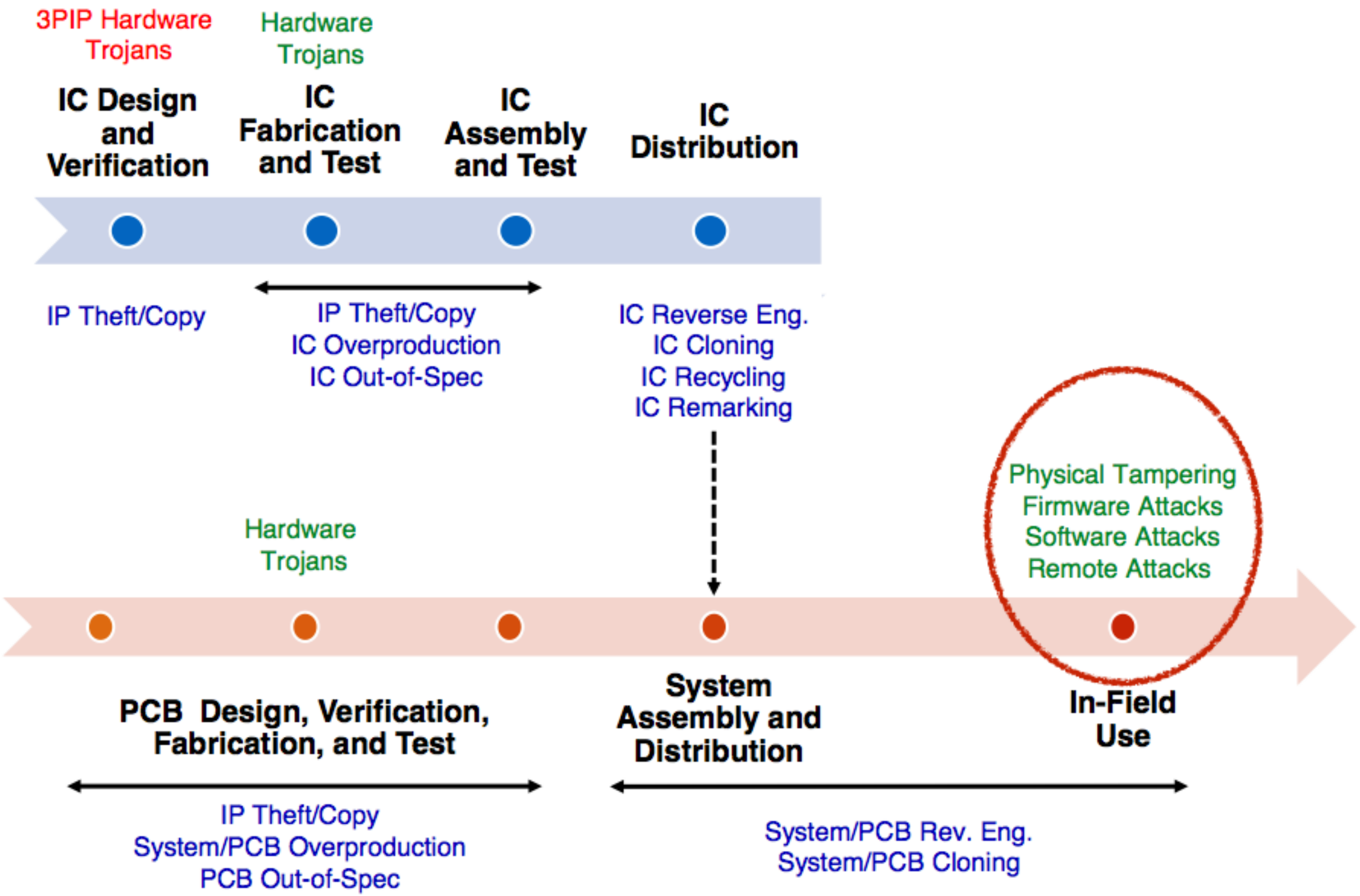
1. There is *insufficient authentication* of IoT devices and controllers.

2. IoT devices are *not designed with hardware, firmware, and software security* as a first-class design goal.

3. Insufficient attention has been paid to *user privacy*.

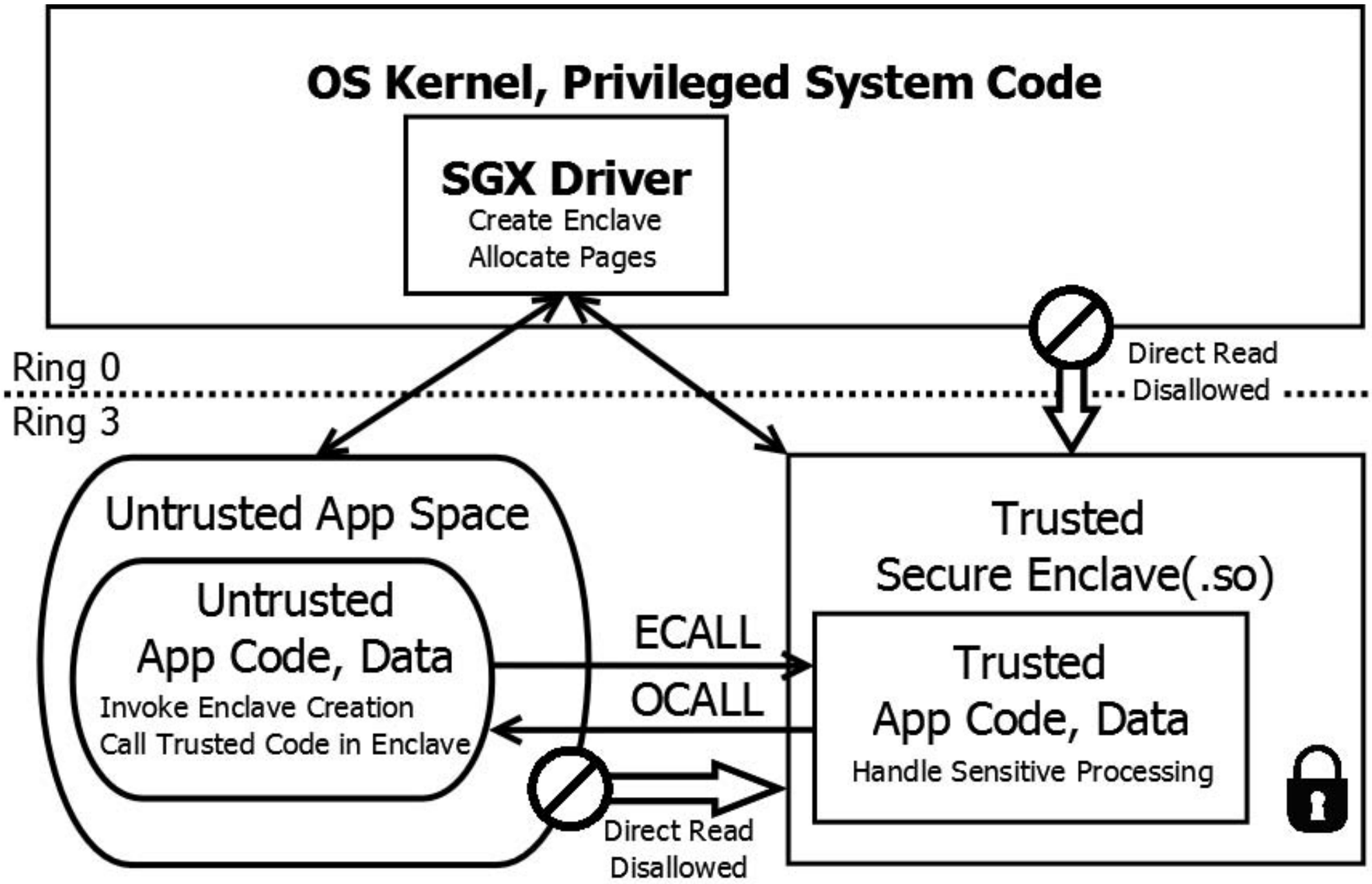
4. Devices have *always-on connectivity* to the Internet, making them reachable by anyone on Earth

Device Verification



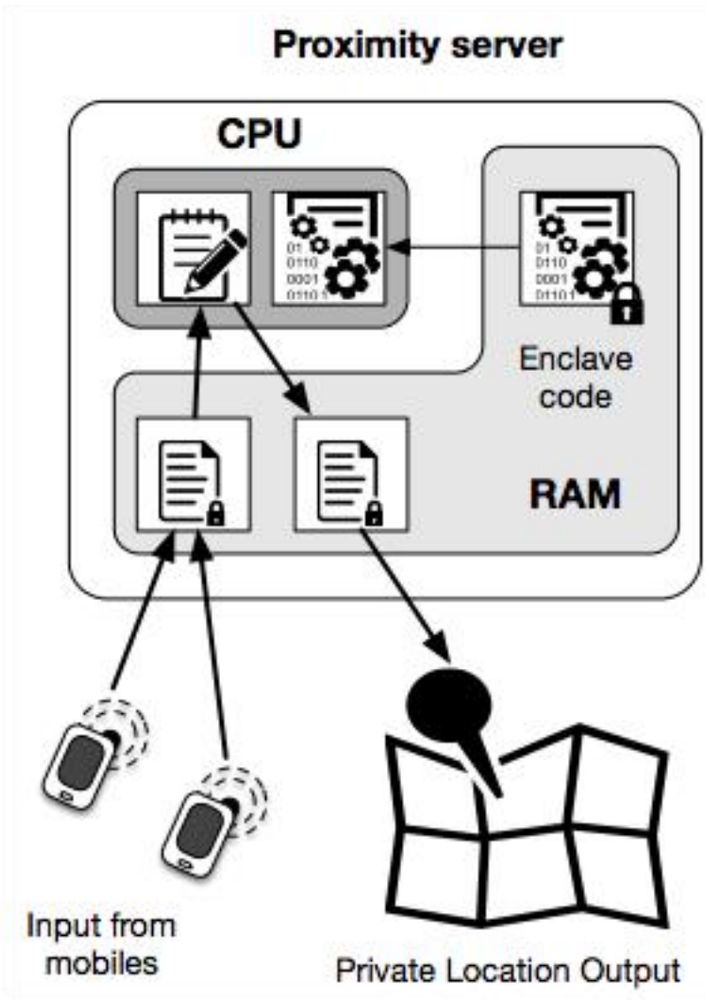
Hardware-Supported Privacy

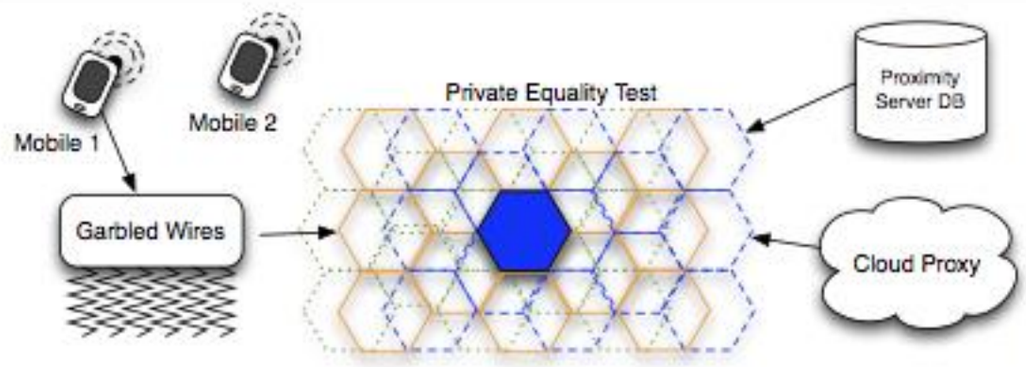
New technologies: TrustZone (ARM), SGX (Intel) allow new ways of securely isolating and attesting code and data



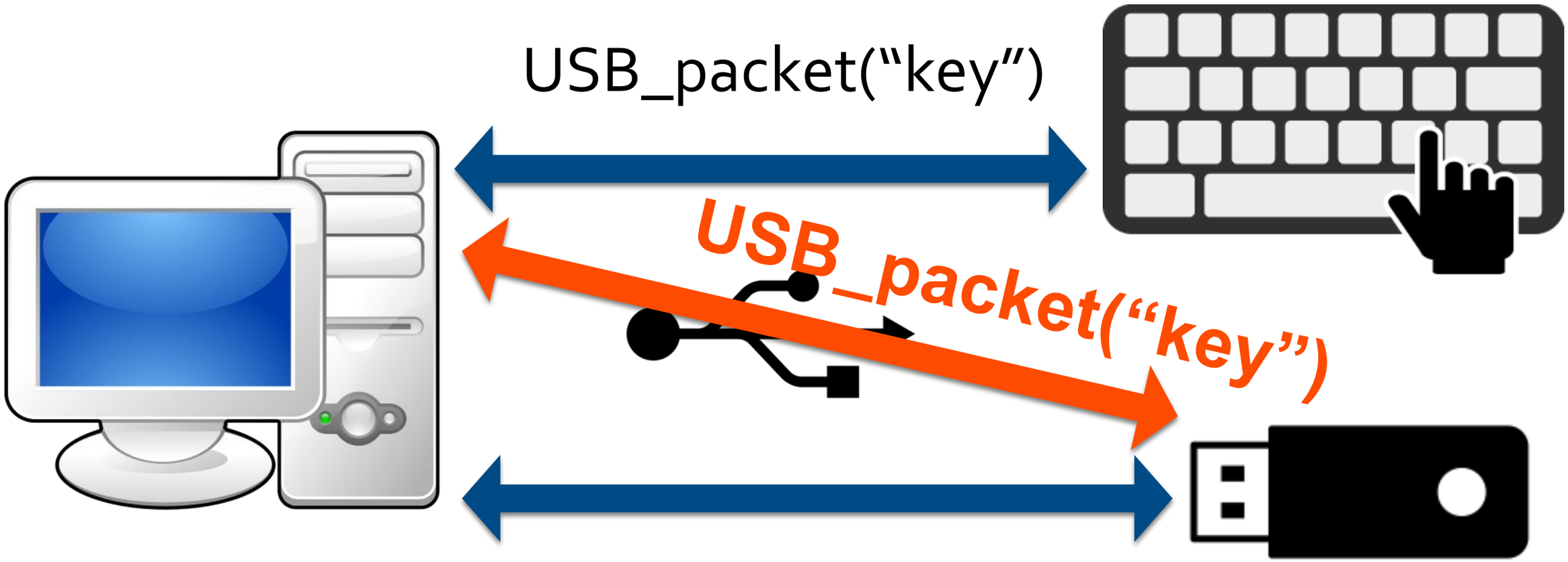
Hardware-Supported Privacy

- Understanding how secure enclaves can be used to support private computation: supporting secure location services



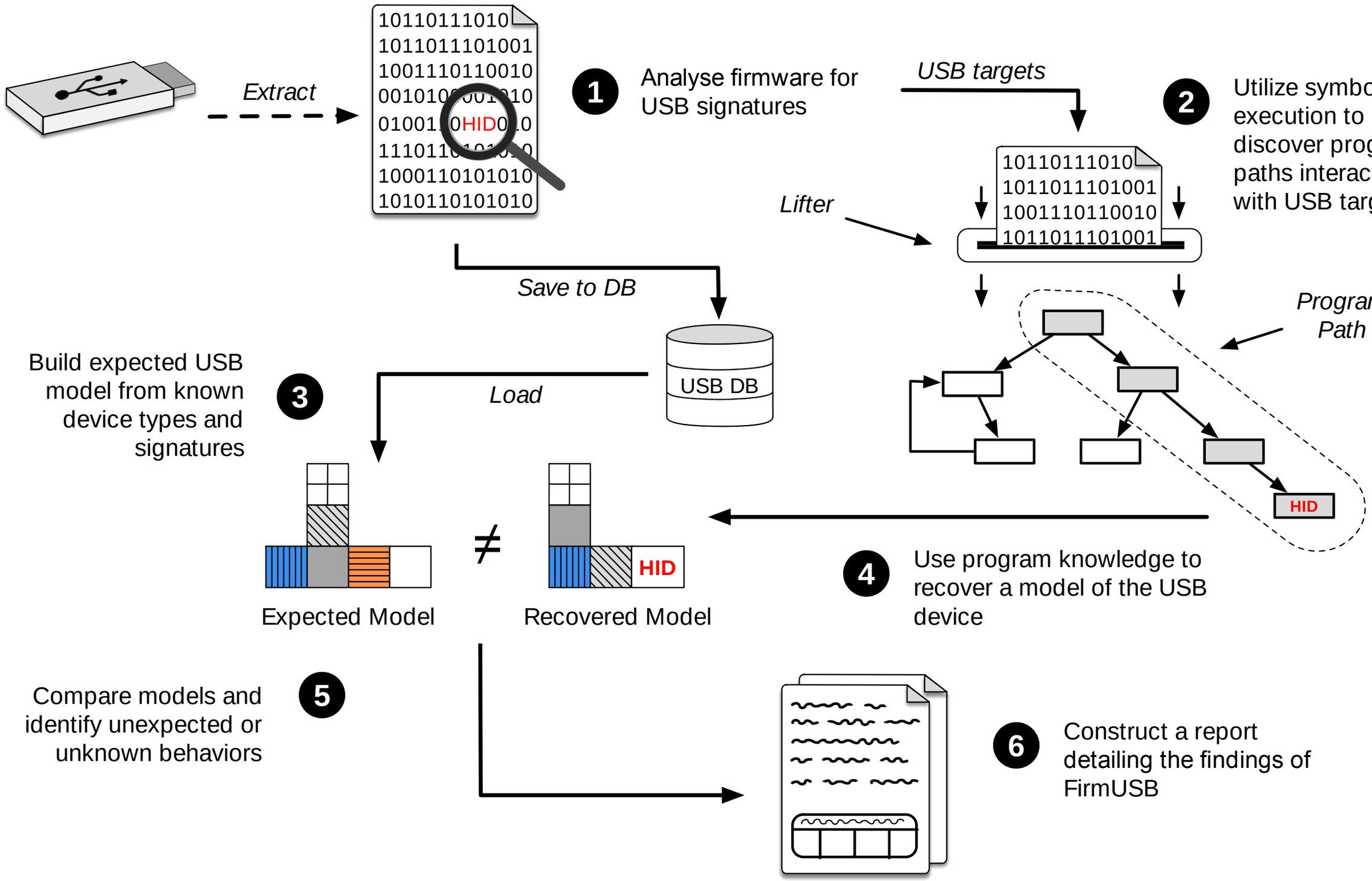


Vetting Devices?



Can we vet the device to ensure that it will never expose malicious functionality in the first place?

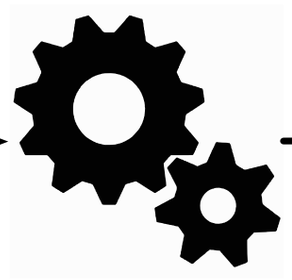
Current Initiative: FirmUSB



Current Initiative: FirmUSB

```
int add() {
  unsigned char i, a = 0;

  for(i = 0; i < 100; i++)
    a += 1;

  return a;
}
```

Source Code



Compiler

```
7f 64 7e 00
0e 8f 05 ed
14 ff 70 f8
ff 8e 82 8f
83 22
```

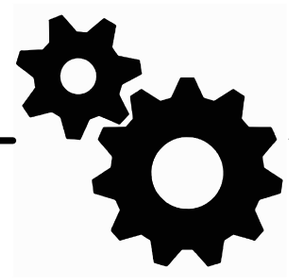
Binary Firmware

Disassembly and CFG recovery

```
00 | ------ IMark(0x66, 1, 0) ------
05 | t24 = Get(R6)
06 | t23 = Add8(t24, 0x01)
07 | Put(R6) = t23
08 | ------ IMark(0x67, 2, 0) ------
12 | t28 = i8051g_memory(0x00000005, 0x00)
13 | STle(t28) = Get(R7)
14 | ------ IMark(0x69, 1, 0) ------
17 | t30 = Get(R5)
18 | ------ IMark(0x6a, 1, 0) ------
19 | t31 = Sub8(t30, 0x01)
20 | PUT(A) = t31
21 | ------ IMark(0x6b, 1, 0) ------
22 | Put(R7) = t31
23 | PUT(ip) = 0x0000006c
24 | ------ IMark(0x6c, 2, 0) ------
25 | t34 = CmpNE8(t31, 0x00)
26 | if (t34) { PUT(ip) = 0x66; Ijk_Boring }
NEXT: PUT(ip) = 0x0000006e; Ijk_Boring
```

VEX IR of basic block 0x66

Lifter

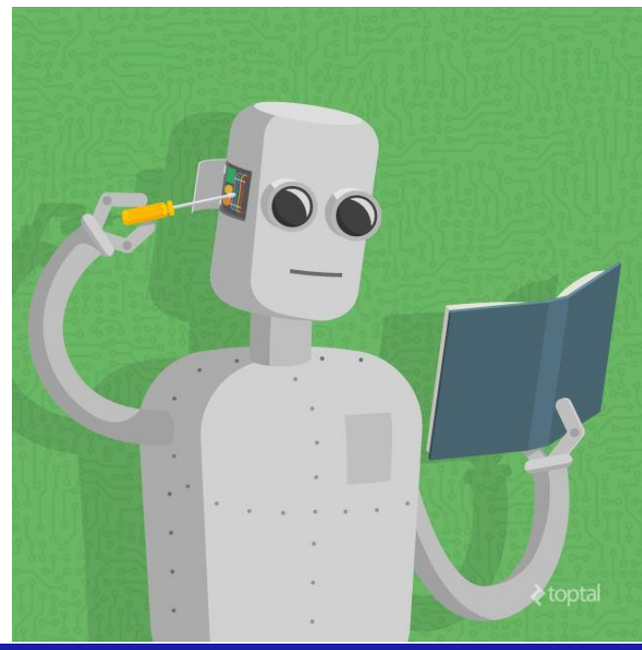


```
0x62: mov  R7, #0x64
0x64: mov  R6, #0x00

0x66: inc  R6
0x67: mov  (0x5), R7
0x69: mov  A, R5
0x6a: dec  A
0x6b: mov  R7, A
0x6c: jnz  $-8

0x6e: mov  R7, A
0x6f: mov  (0x82), R6
0x71: mov  (0x83), R7
0x73: ret
```

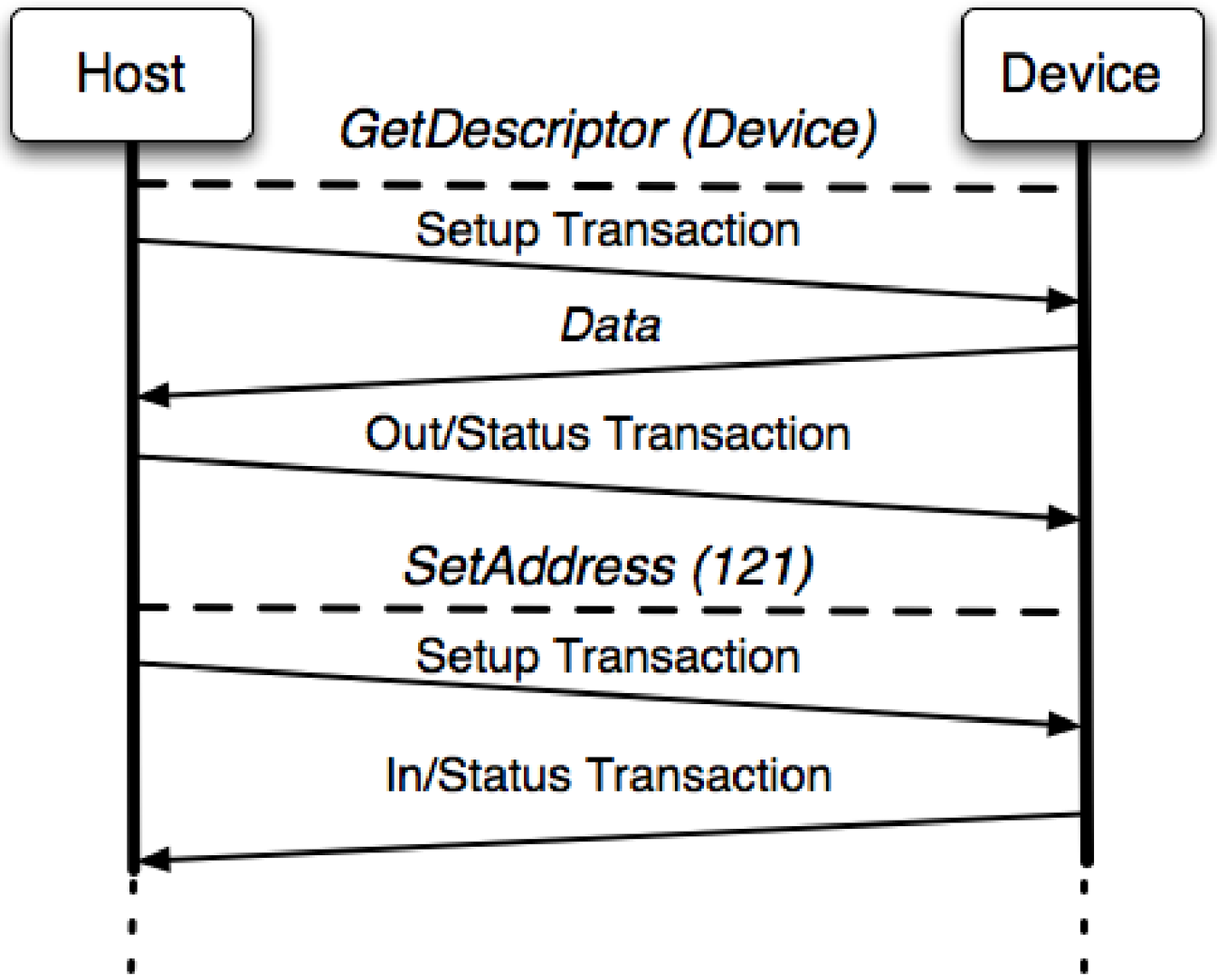
8051 Assembly CFG

Machine Learning and Security

- Recently an area of great interest
  - Means of sifting signal from noise
  - Methods of use: accelerometers, finger movements on smartphones, browsers
- How can machine learning techniques help?
  - Identification, authentication, attestation?
  - In IoT environments?



Case Study: USB Fingerprints

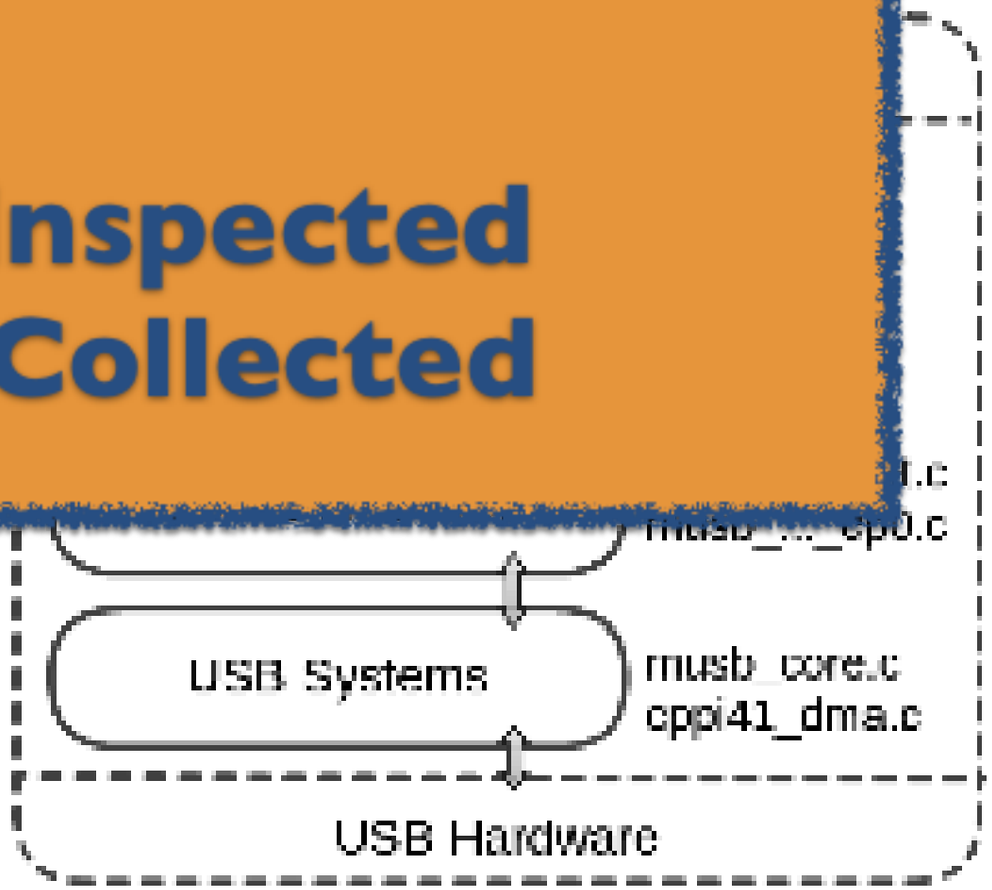


- Enumeration can be forced on any powered-on USB board that is configured to run in host mode.

USB Fingerprinting

Total Data Corpus:

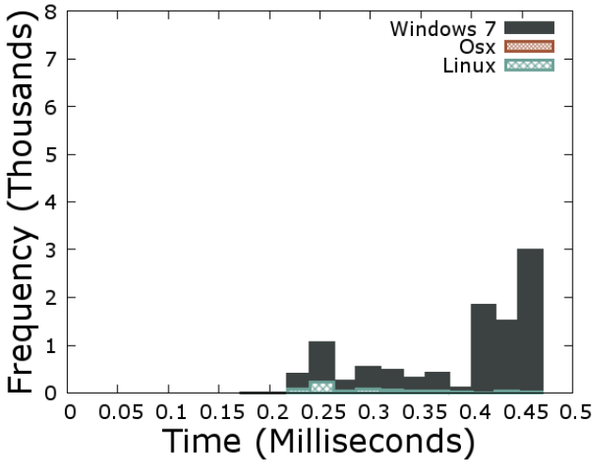
256 Machines Inspected
32,150 Traces Collected



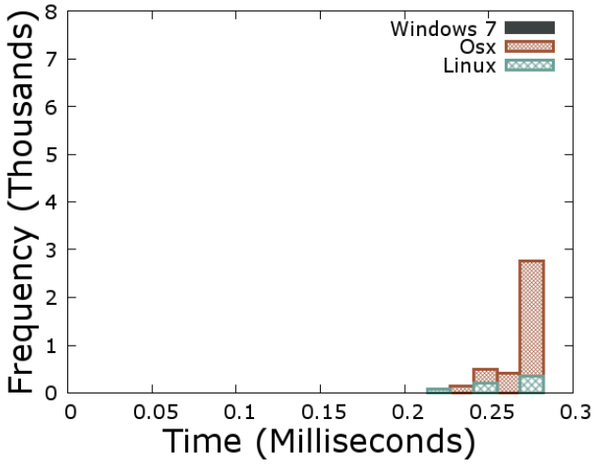
Feature Extraction

Trace Data was processed to extract timing data, producing features that included:

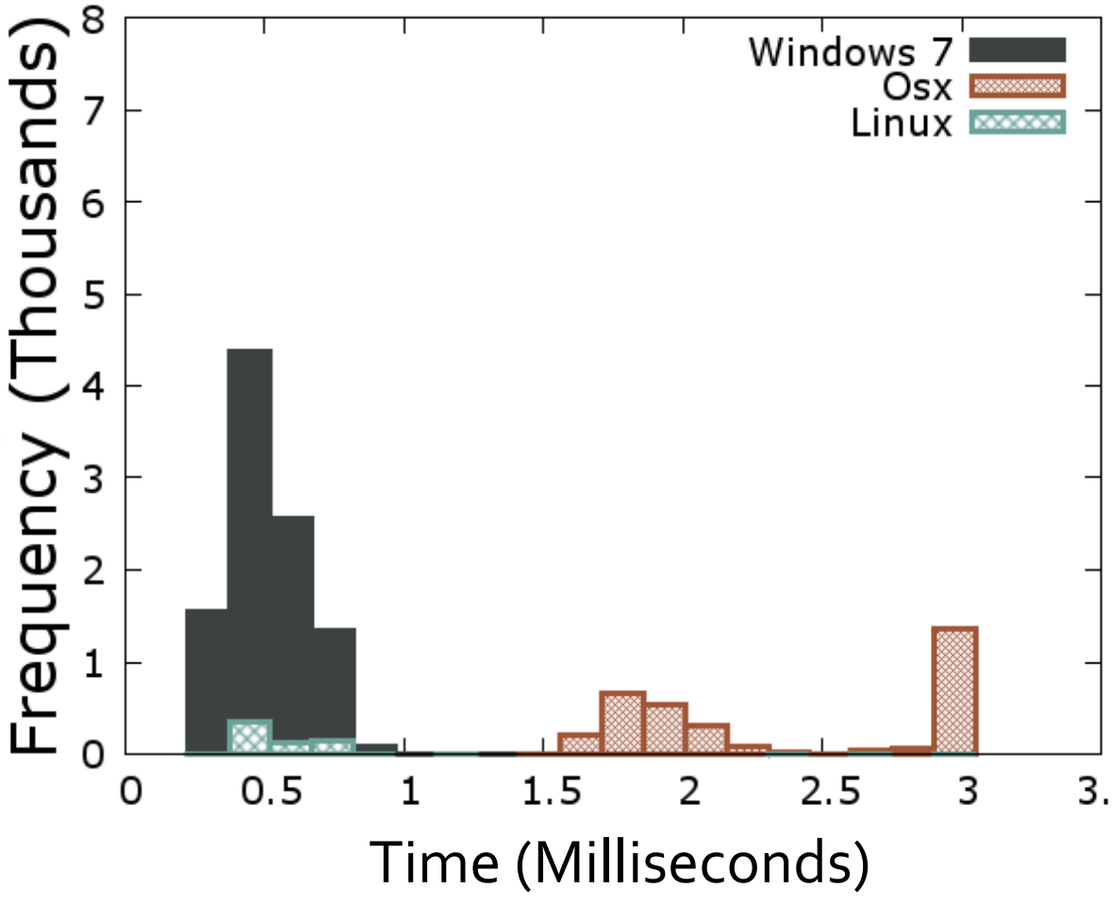
Individual Control Transfers



GET_DESCRIPTOR (Language)

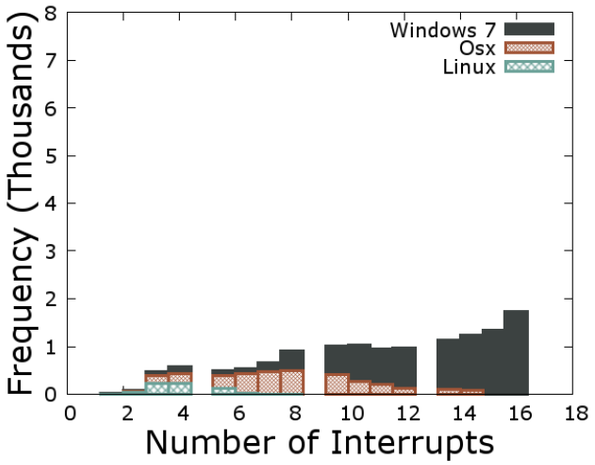


GET_DESCRIPTOR (Manuf.)

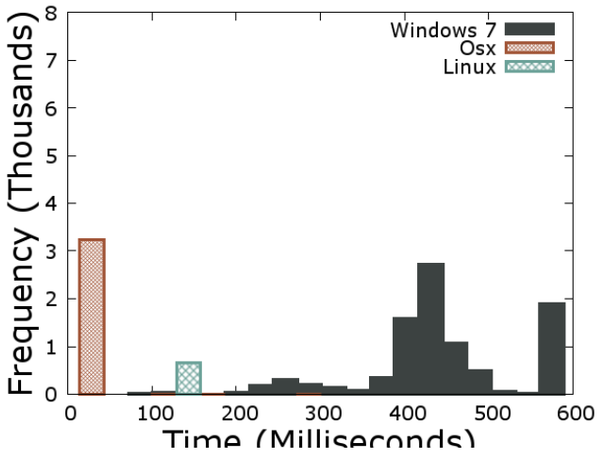


GET_DESCRIPTOR (Serial)

Trace-level Statistics



Num. of Idle Packets



Length of Enumeration

Classification Results

	Example Label	Accuracy
OS Major	“OSX”	100%
OS Minor	“OSX 10.8”	94%
Make	“Apple iMac”	97%
Model	“Apple iMac 13”	90%

Supervised learning with random forest classifier over vectors of 152 features derived from data, train on 66% of data and evaluate on 34%

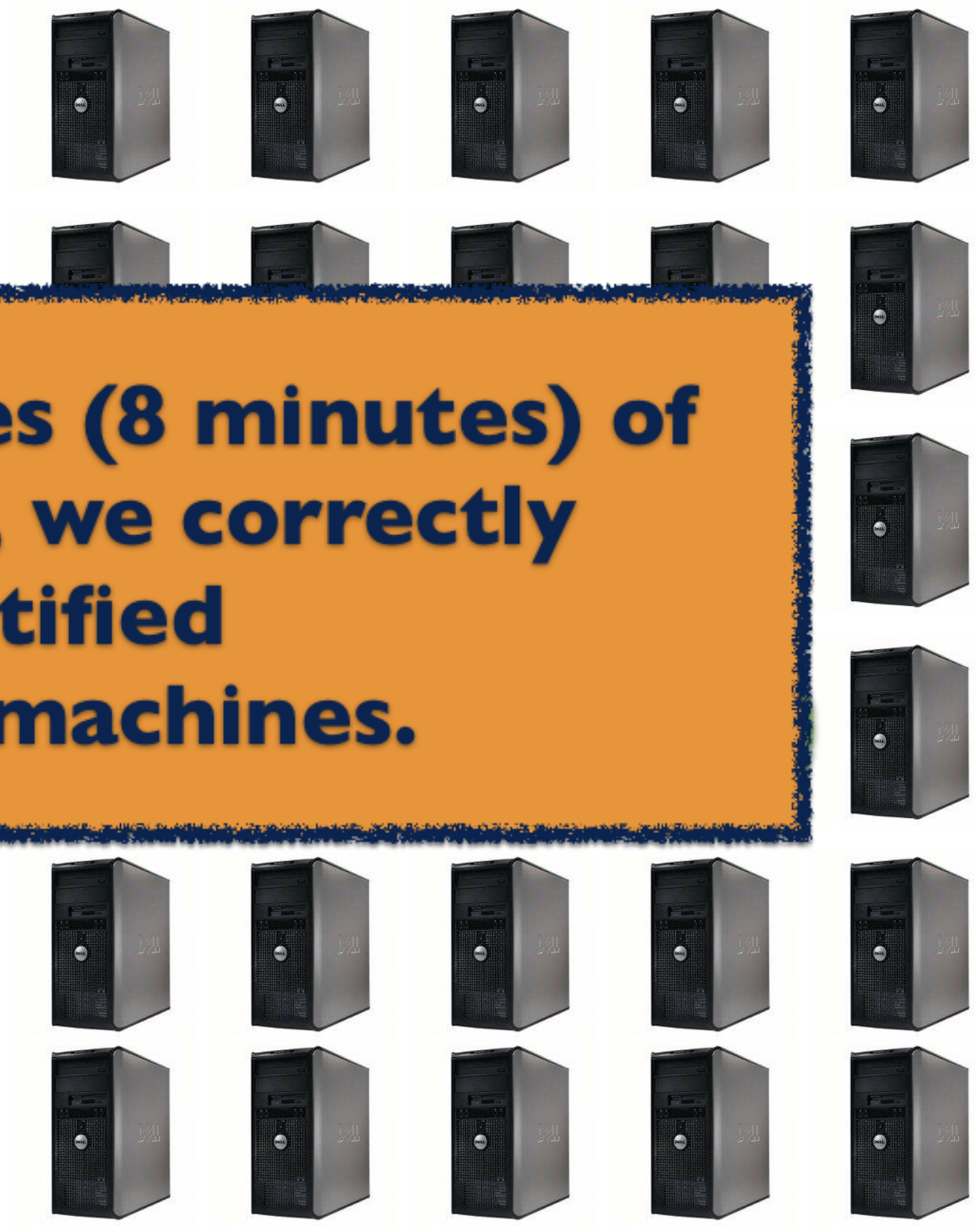
Individual Host Identification

- Field of 30 identical Dell Optiplex 745s.
- Labeled 1 PC “Target”, all others “Outlier”.
- Polled the classifier for hundreds of predictions.
- Performed χ^2 independence test on the distribution of predictions.
- Tested each PC as Target once.

Individual Host Identification

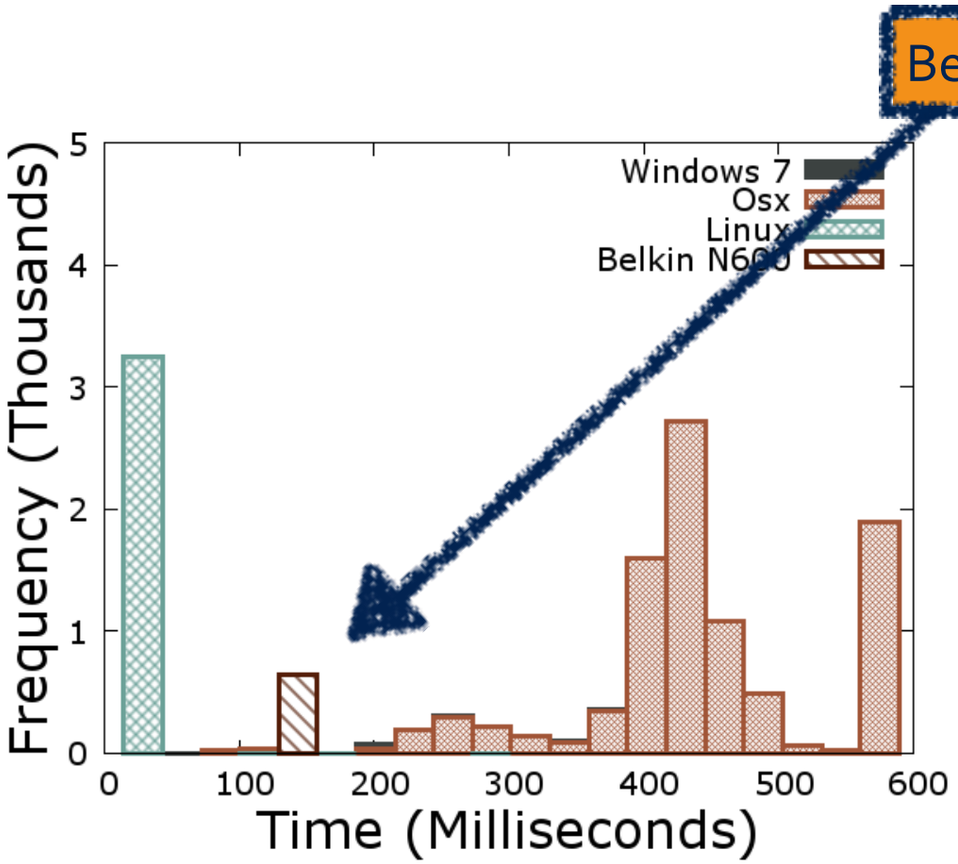
- Field of 30 identical Dell Optiplex 745s.
- La
  ot
- Pc
  hu
- Pe
  test on the distribution of predictions.
- Tested each PC as Target once.

Given 250 traces (8 minutes) of observation, we correctly identified 21 of 30 machines.

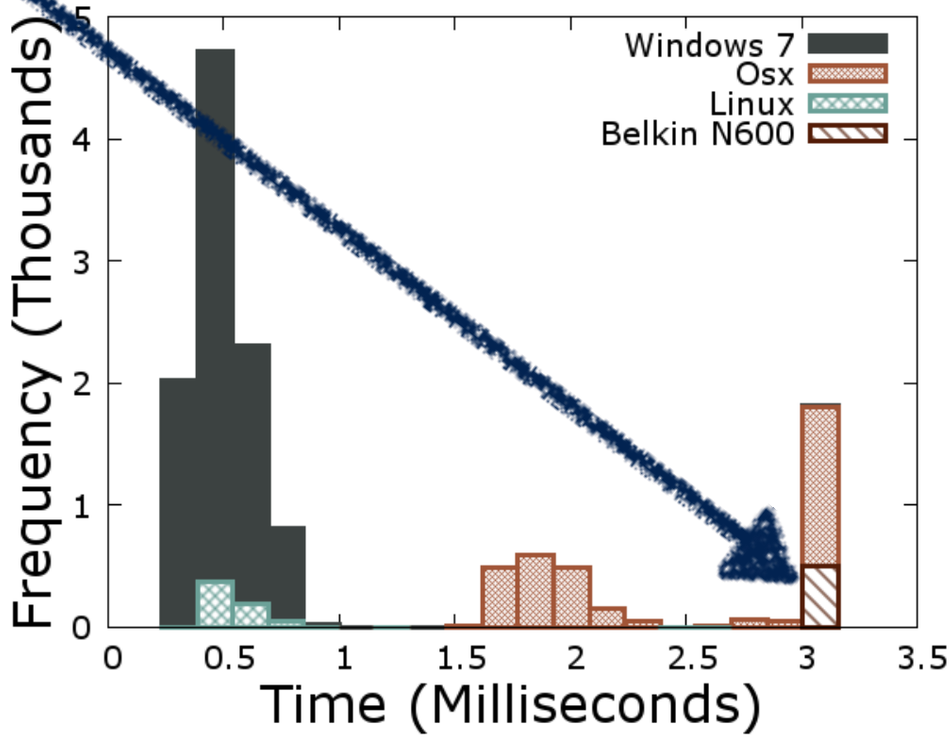


Embedded Devices

- We fingerprinted a router, distinguishing it from the rest of our data corpus.



Duration of Enumeration

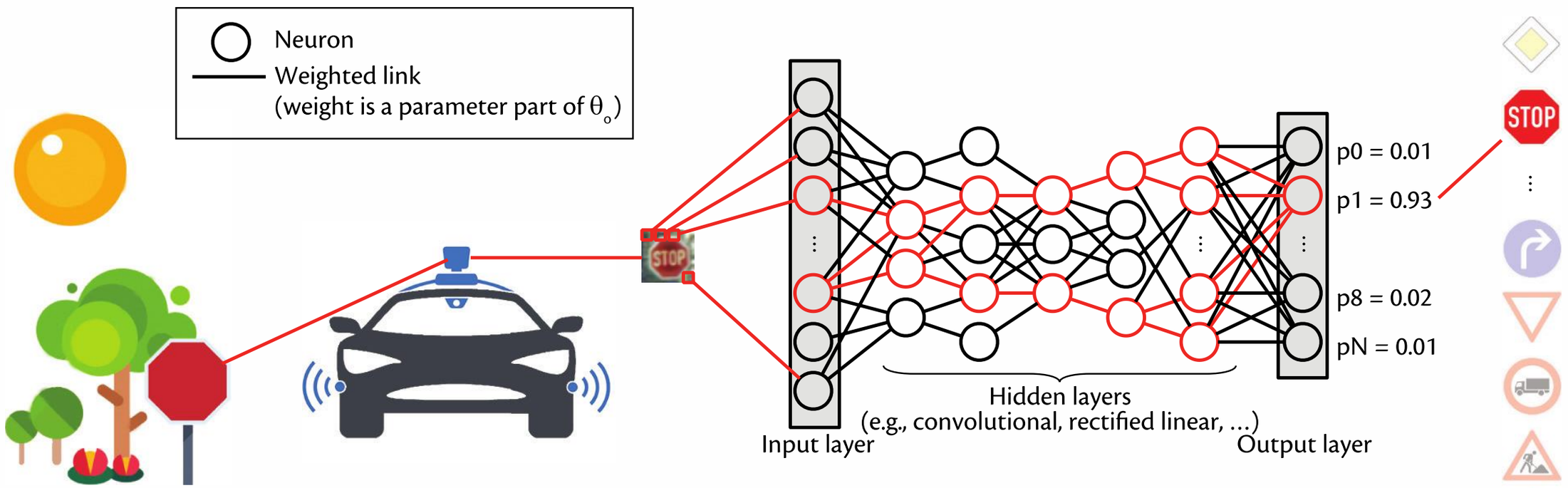


GET_DESCRIPTOR (Serial)

Robust Identity for IoT

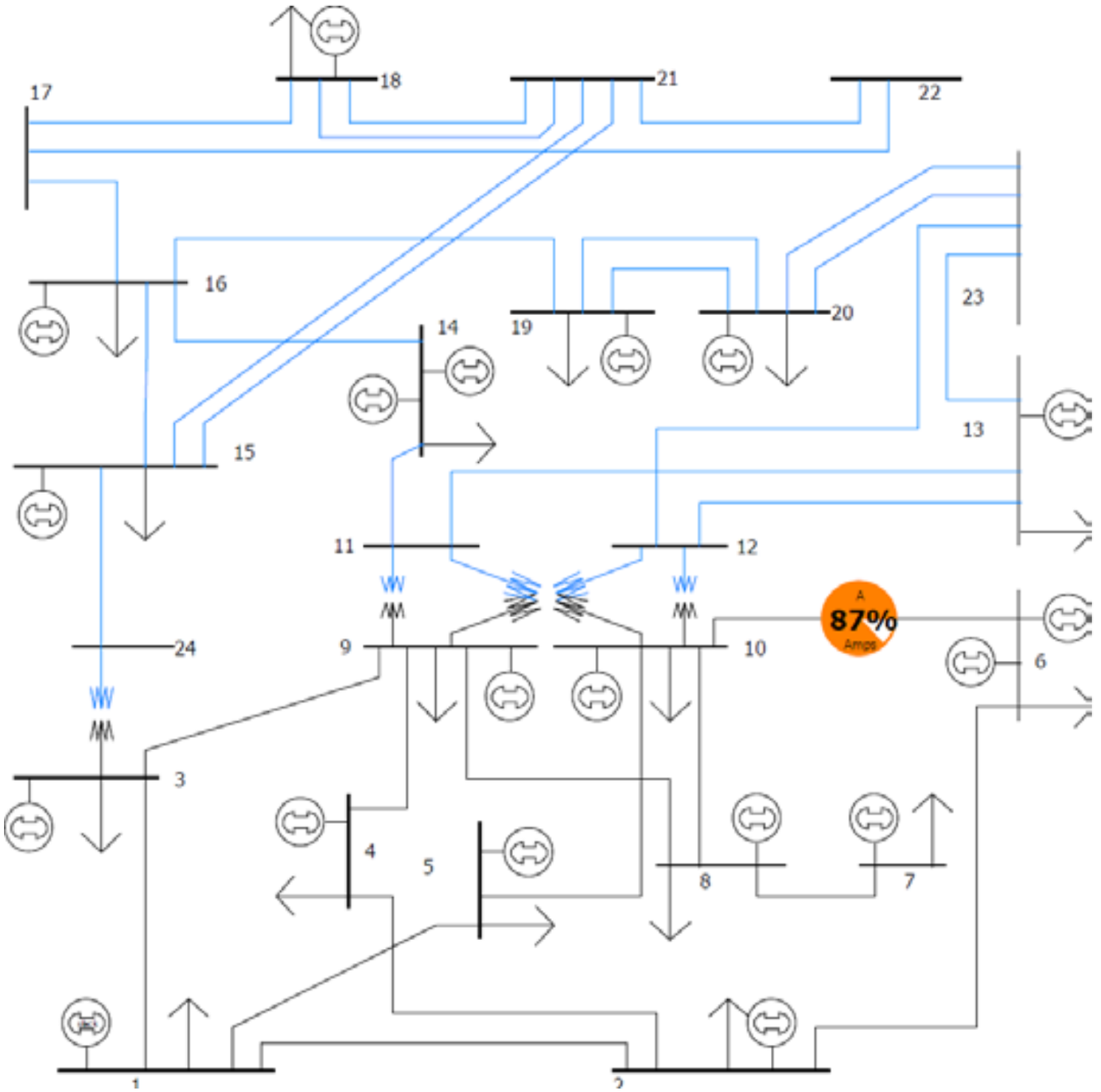
- **Workload characterization:** Can we determine what is running on the device based on signal emanation that we can collect?
- **Ensemble signal analysis:** examining JTAG interface and EM signals and combine existing machine learning techniques to strengthen fingerprint collection and support remote querying and attestation

Challenge: Adversarial Learning

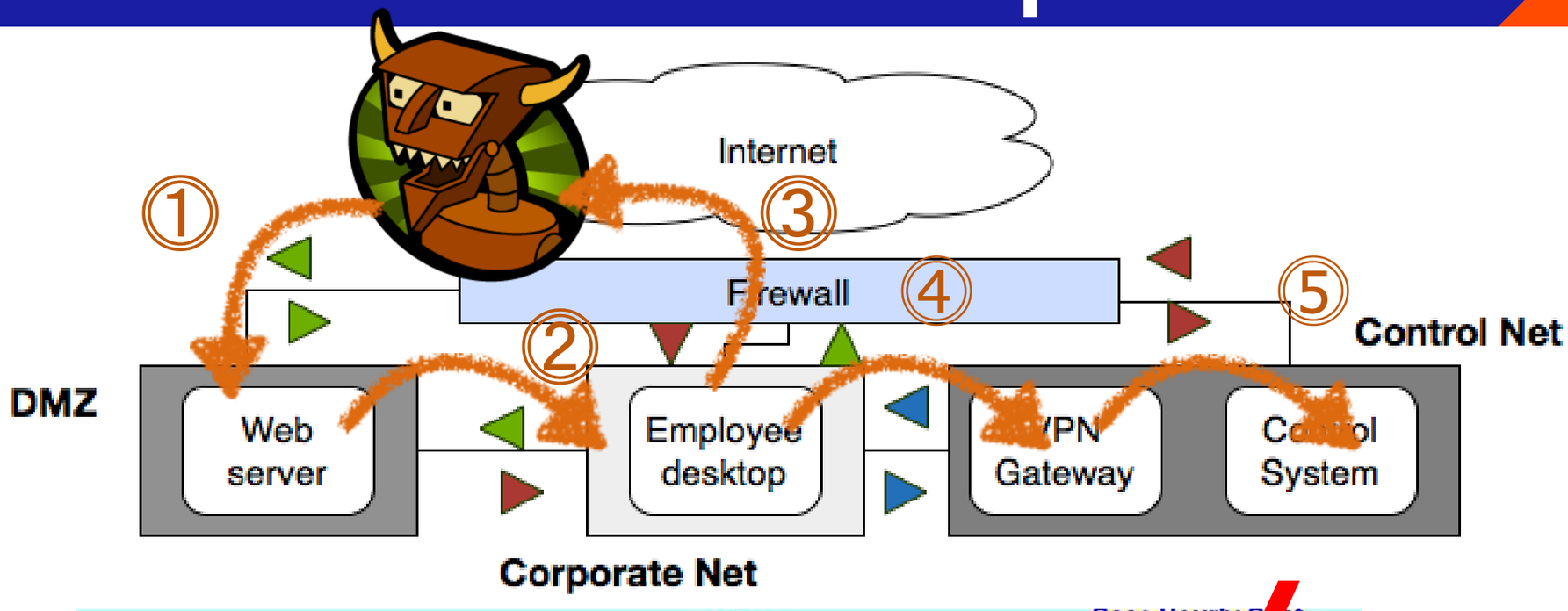


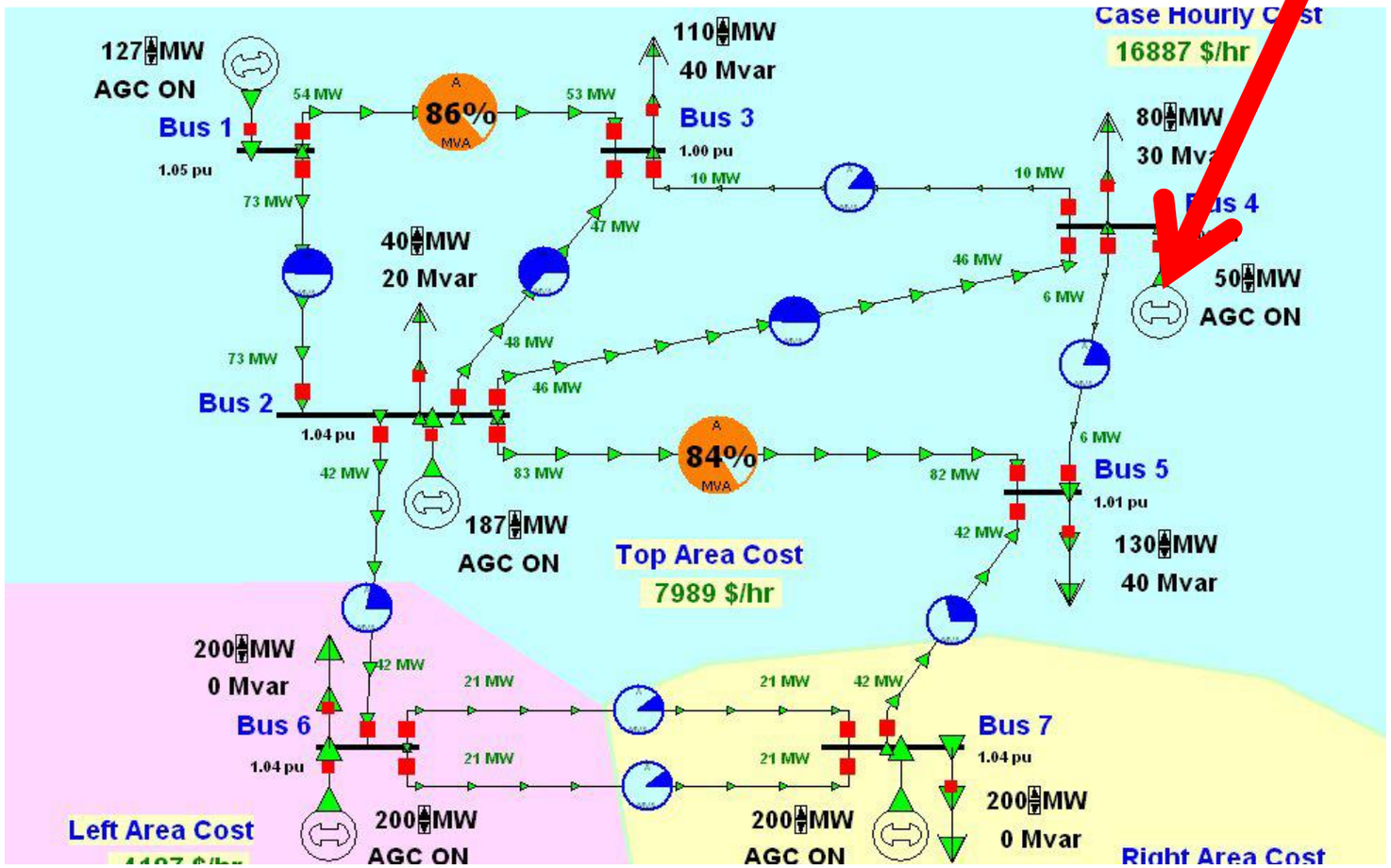
Cyber-Physical Systems

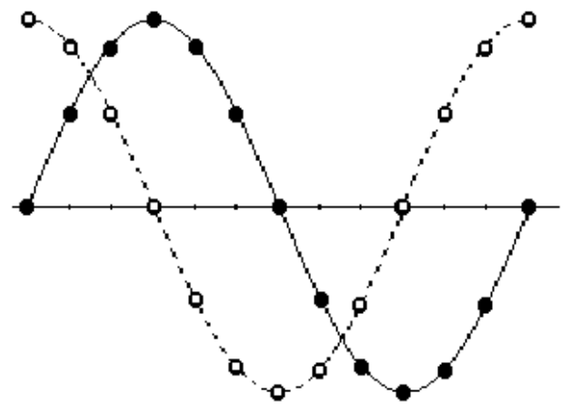
- Environments like the power grid, which can contain many IoTs, are different
- Not just the cyber element: also the physics of the system
- E.g., voltage and current relationship in power systems (Kirchoff's laws)
- Generators, loads, lines provide ***feedback loop***



CPS Network Exploit

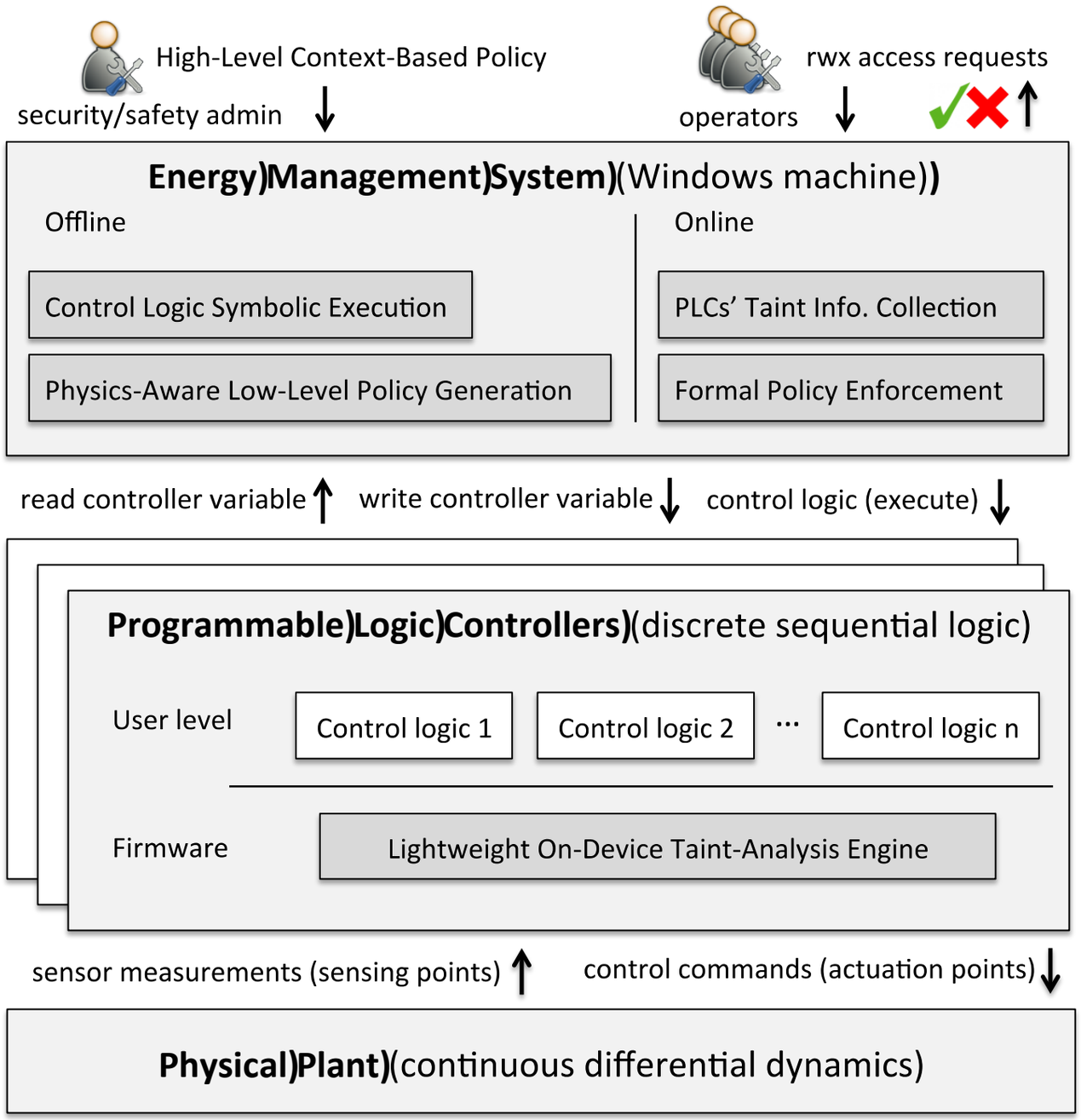






Our Solution: CPAC

- Model the physical system to device policies based on information flow
- Track the control flow through controller devices
- Real-time policy decisions based on sensing and control



Ransomware

- One of the newest and most pernicious types of malware, can affect both IoT devices and the controllers that they communicate with
- Encrypt critical data on these systems and deny service to them unless a ransom is extorted from victims
- Universities, hospitals, other critical infrastructure has been hit by ransomware
  - **638 MILLION** ransomware attacks in 2016 (**167X** the number seen in 2015)
  - ***$209 million paid*** in ransoms in Q1 2016 alone (Sonicwall report)
- ***Traditional anti-virus cannot keep up with this threat.***

CryptoDrop

Insight: Ransomware must transform data in unreadable blobs.

Insight: Regular files have known structure, encrypted files lack it.

Solution: Monitor changes to files instead of monitoring specific apps.

Contact me for more details.

Challenges to Consider

- **Deployment:** where will the devices be placed? How accessible will they be?
- **Remediation:** if a device is compromised, how can it be fixed? Who will do it?
- **Resilience:** In the event of a compromise, what are the ramifications? What layers of additional defense are there to protect assets?
- **Regulation:** What is the role of regulatory agencies when IoT devices are used in critical infrastructure environments? What about security and privacy of citizens in the home?
- What is the ***security model*** that systems are being designed with and how to ensure accountability to this model from design to implementation - in either the public or private sector environment?

Thank You!

Kevin Butler

butler@ufl.edu

http://www.kevinbutler.org