# IoT Security | What, Why, How

Earlence Fernandes

*Your car is a computer with wheels and an engine*

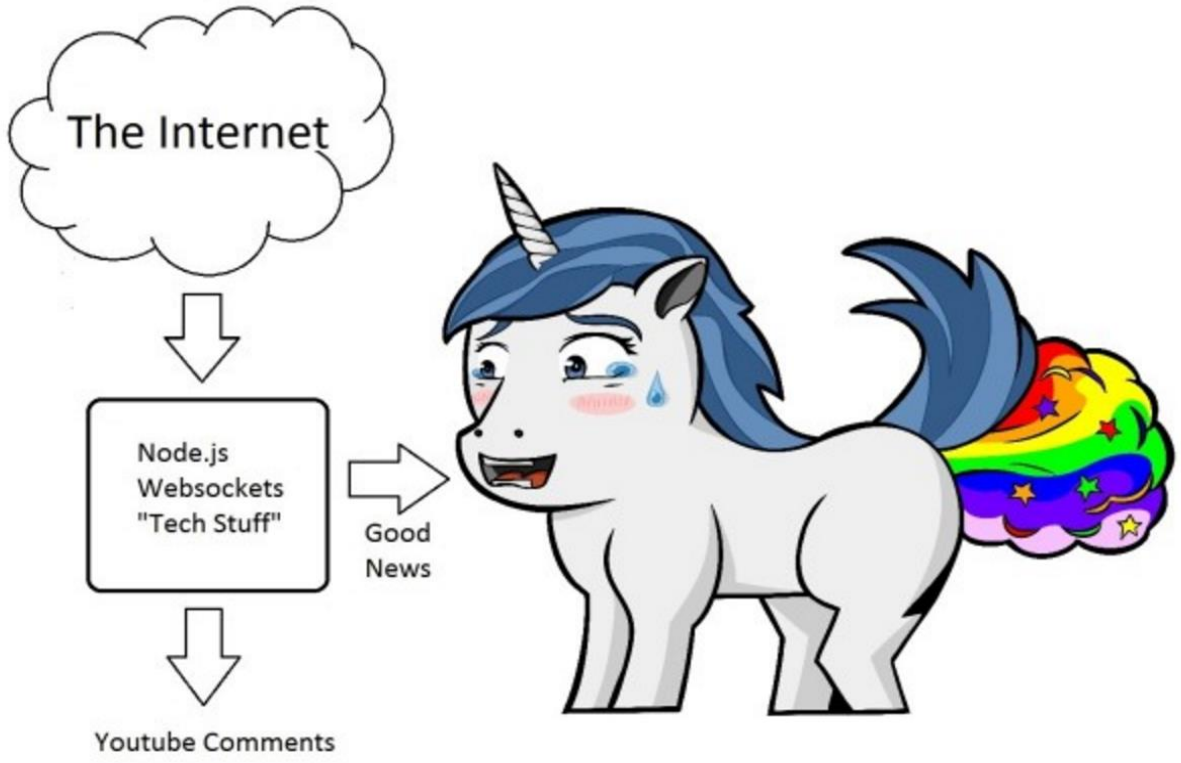
*Your refrigerator is a computer that keeps food cold*

*Your ATM is a computer with money inside*

-- Bruce Schneier to the US House Committee on Energy and Commerce
2016

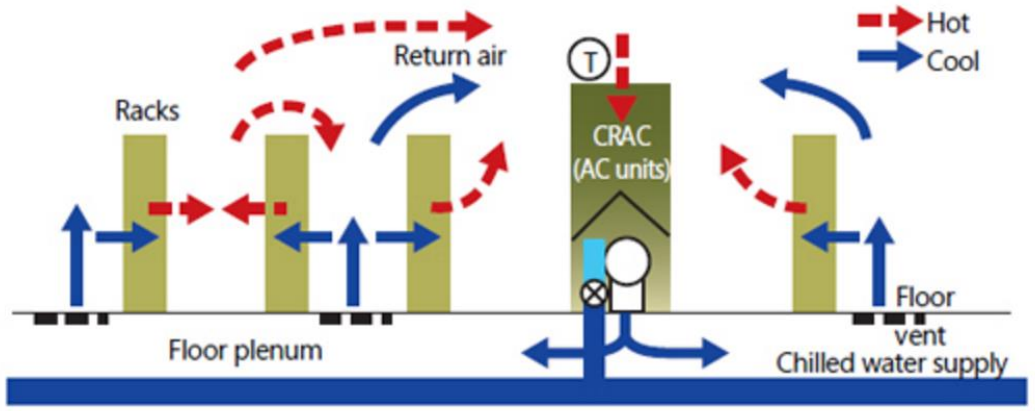
# World, saved: Tootz the IoT unicorn farts rainbows at good news

*Posted on April 19, 2016* in CONNECTED DEVICES




Tootz integrates with twitter, Facebook, twitch and gmail but will connect to more services in the future.  It is Powered by USB or battery for fully untethered fun.

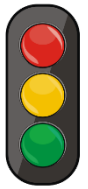
# Automated Data Center Cooling Management

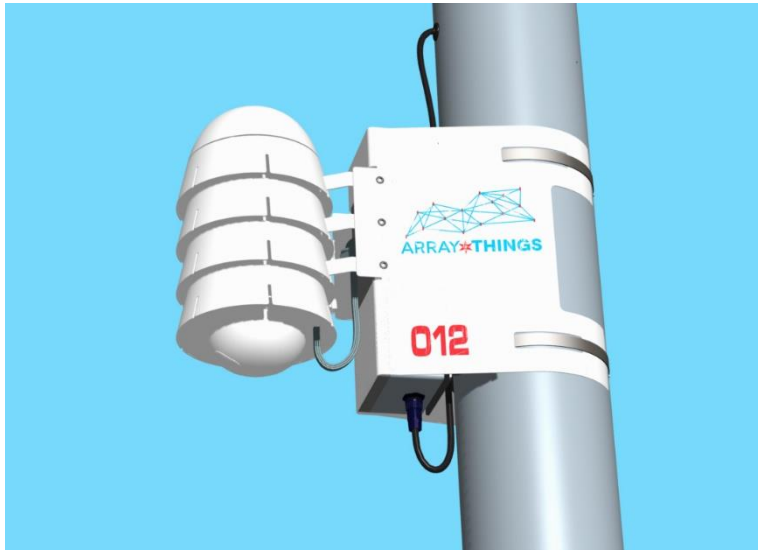



Courtesy: Microsoft Genome Project
https://msdn.microsoft.com/en-us/library/dd393313.aspx

# Smart Cities

amsmartcity TRAFFICLINK






# Demand Response; Increased Renewables Usage


# Data-Driven Agriculture

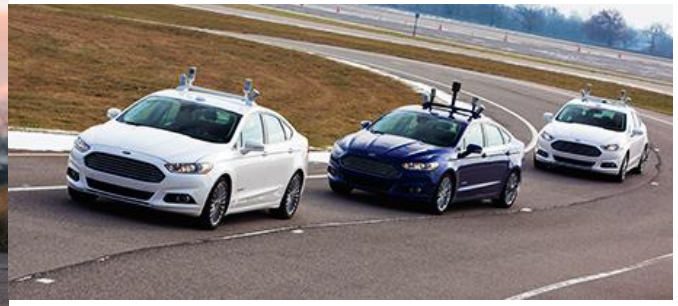
FarmBeats Platform, NSDI 2017

## Hospital Efficiency and Effectiveness

Track meds for elderly

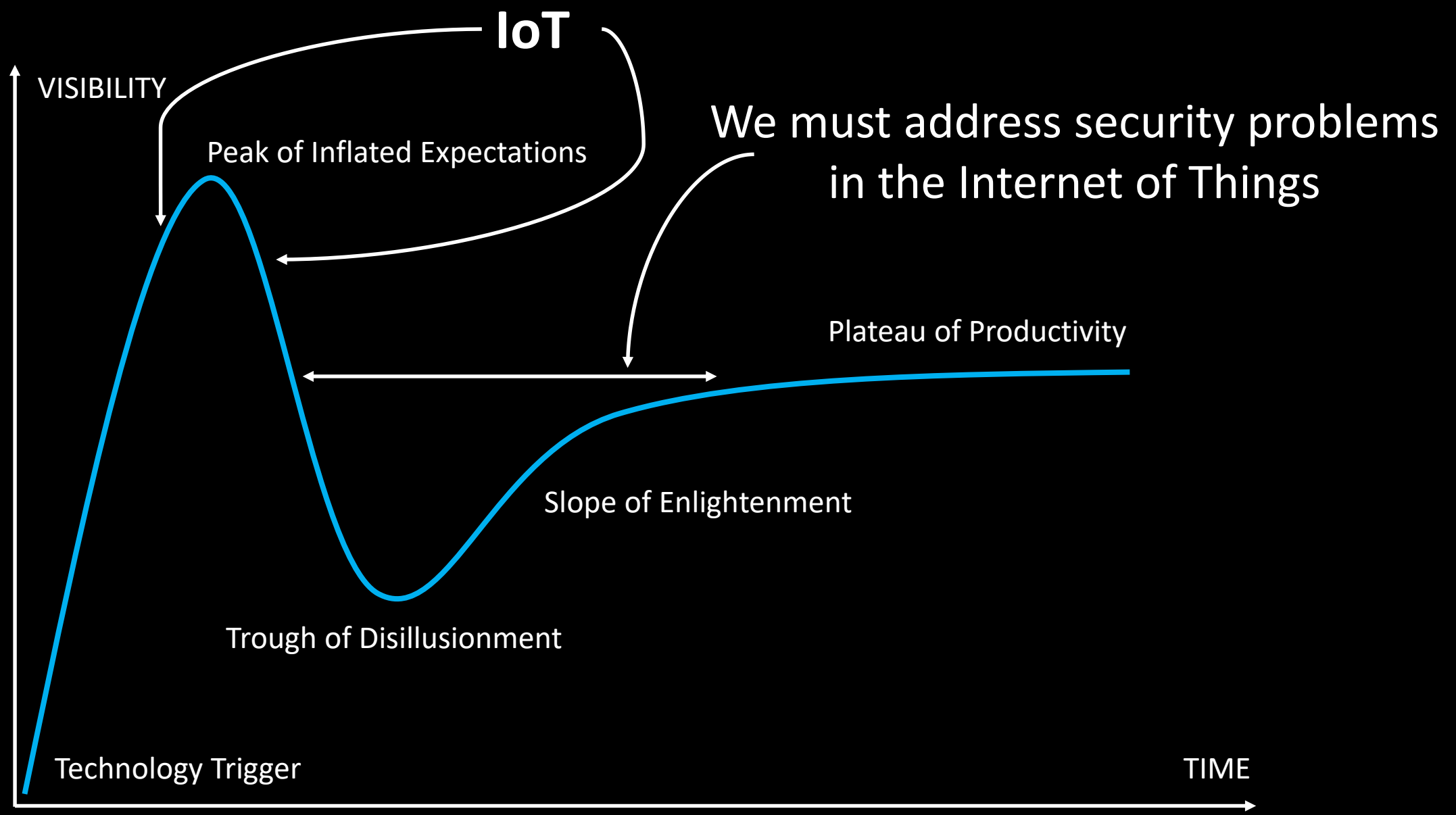
Realtime location

## Autonomous Vehicles



## Wearables


## Industrial Internet



IoT
VISIBILITY
Peak of Inflated Expectations
We must address security problems in the Internet of Things
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

# Attacks on the Internet of Things

theguardian

opinion sports soccer tech arts lifestyle fashion business travel environment

## DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

Mirai disabled heating for buil 200,000 residences in lost power for 3 hours

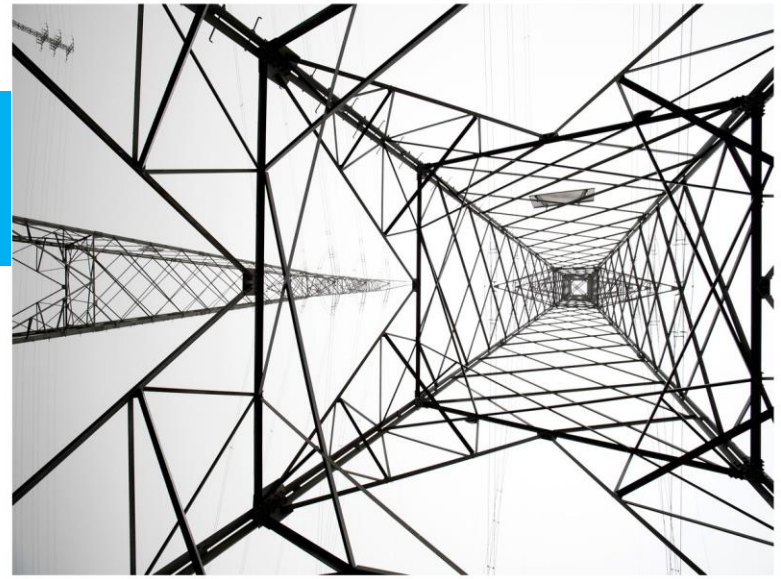
Mirai botnet used IP Cameras/DVRs to launch DDoS

WIRED Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

BUSINESS CULTURE DESIGN GEAR SCIENCE

KIM ZETTER SECURITY 03.03.16 7:00 AM

## INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



# Attacks on the Internet of Things

MOTHERBOARD

CULTURE

## Hackers Killed a Simulated Human By Turning Off Its Pacemaker

JASON KOEBLER
Sep 7 2015, 12:45pm

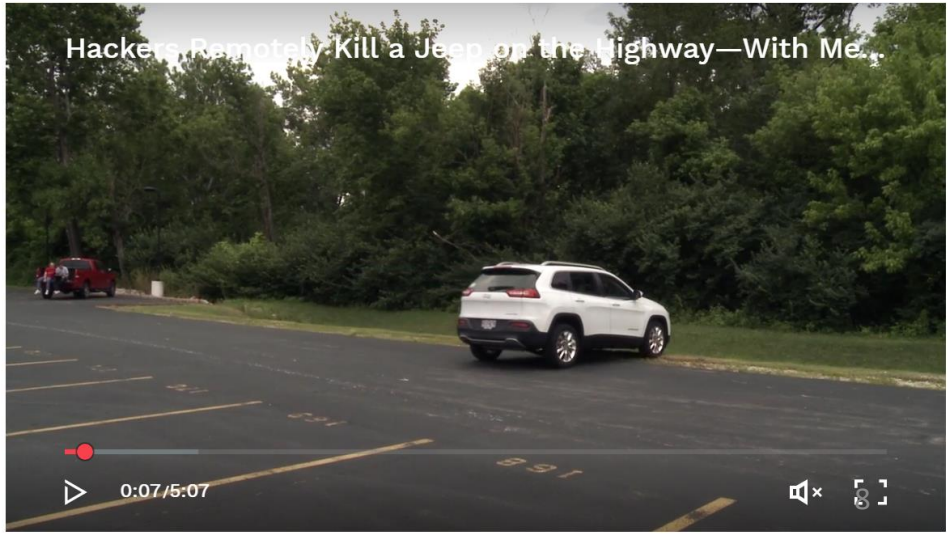
**Some humans are already hackable, and, yes, you can do some serious damage by compromising medical implants.**

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It

RE | DESIGN | GEAR | SCIENCE

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



# Attacks Closer to Home

Remotely determine prime time for Burglary [1,2]

OR

Flooding [1]

## Devices



## Protocols

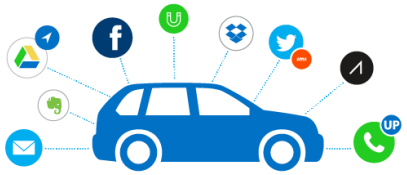


[1] Denning et al., Computer Security and the Modern Home, CACM'13
[2] FTC Internet of Things Report'15

How might we tackle the IoT security problem?

What are the new intellectual challenges?

# The Internet of Things Stack




Application Domains

Interoperability, Sensing Mgmt, Data Analysis, Control

IoT Platforms/ System Software




Connectivity Protocols/ Network

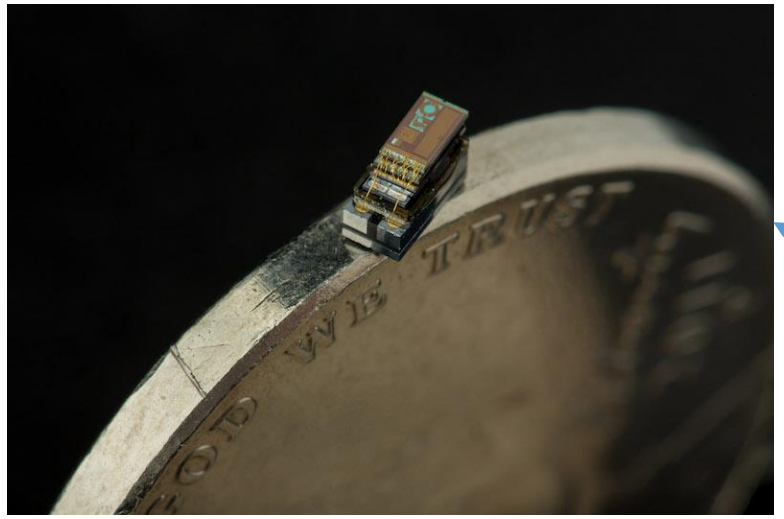


Devices/ Hardware

Usability Issues

# Device/Hardware Layer Challenges

Michigan Micro Mote (M3)



Smart Cards/RFID Tags

**apply**

**apply**

Resource Constraints
(Energy, Hardware Features, Computation, …)

Privilege Levels, Memory Management Unit,
Trusted Execution (SGX, TrustZone, …),
Secure Randomness, Secure Clocks, …

How can we measure the passage of time? [1]

[1] A. Rahmati et al., Time and Remanence Decay in SRAM to implement secure protocols on embedded devices without clocks, USENIX Sec 2012

# Device/Hardware Layer Challenges

- Core notions of hardware security mechanisms: Similar to other computing paradigms
- Resource Constraints of IoT devices => Affect higher-layer security properties
- Higher-layer security properties => Tuned to manage resource constraints

Hardware-Software Co-Design Approach

# Network Layer Challenges

Power Line Communication

Z-WAVE

ZigBee®

Bluetooth SMART

NFC™

Visible Light Communication

## Connectivity Protocol Diversity

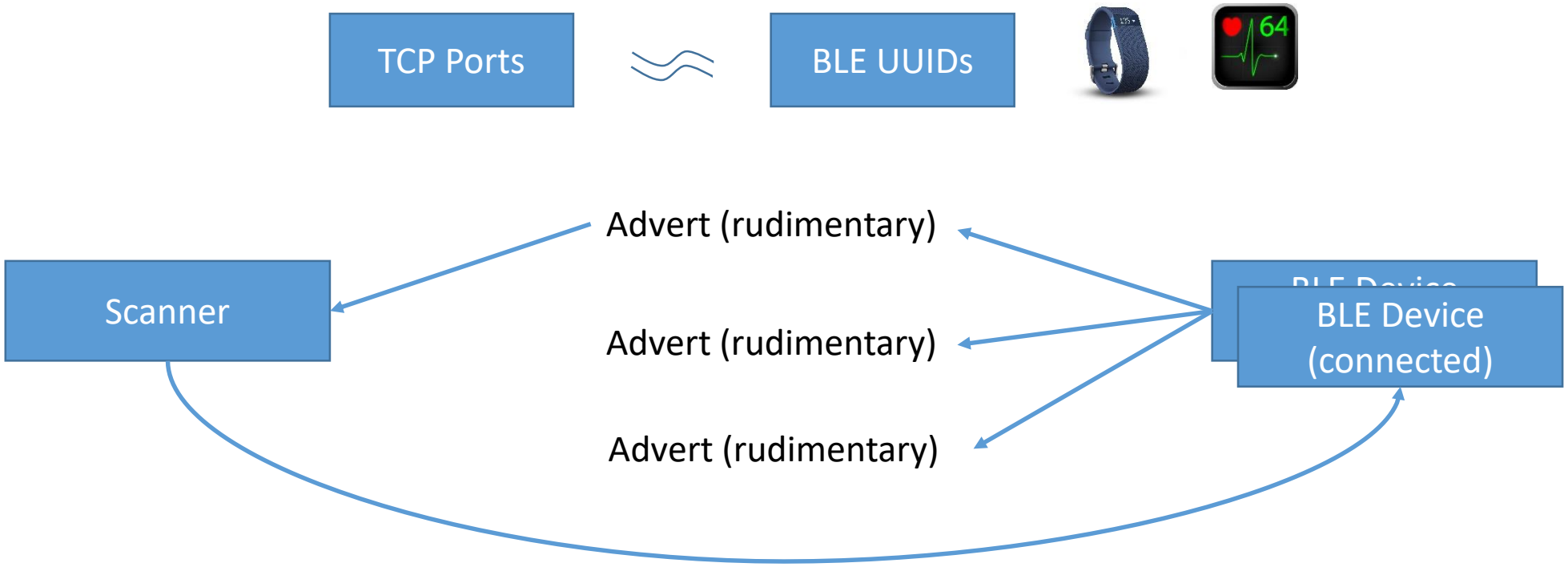
Technology Infancy

Environmental Constraints
(e.g., no additional infrastructure)

Resource Constraints (e.g., energy)

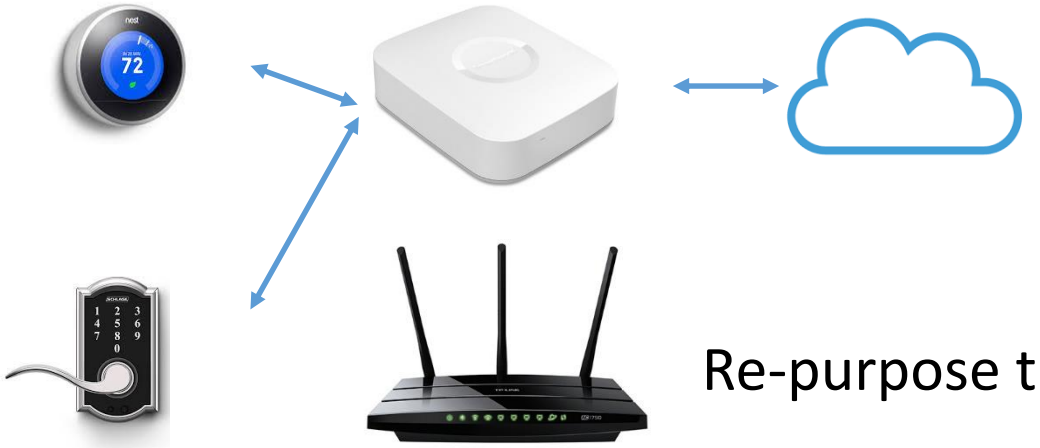
## Affects Network Security Practices

# Case Study: Port Scanning




As each protocol has its own notions of how two peers communicate with each other, it is unclear how network security practices such as port scanning translate to networks of devices that use various IoT protocols

# Repurposing Networking Tech. In New Ways



The hub-model of Smart Homes

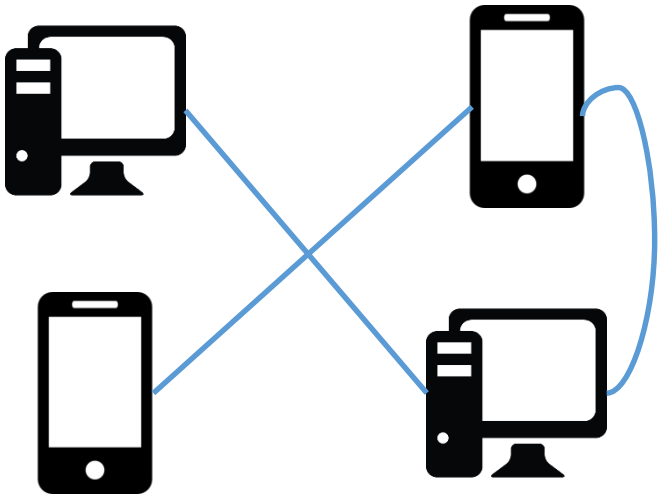
Re-purpose the WiFi Router [1]

How do we make sure that only a WiFi-enabled a presence detector and nothing else affects a WiFi door lock?

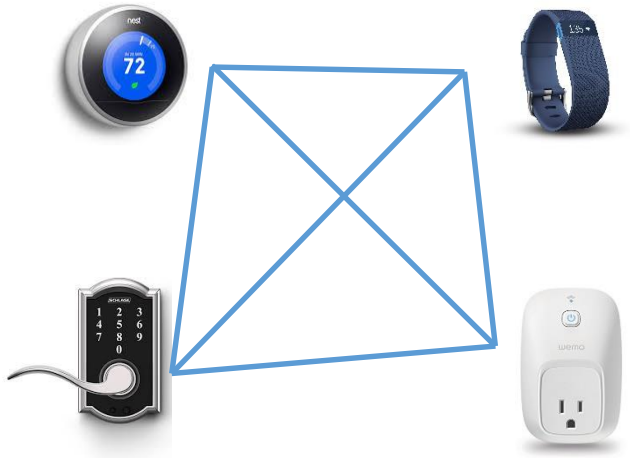
Can we patch security vulns at the network layer for unpatchable IoT devices?

[1] A. Simpson et al., Securing vulnerable home iot devices with an in-hub security manager, University of Washington, Technical Report UW-CSE-17-01-01, Jan. 2017

# Physical Principles for Network Anomaly Det.



Typical Network
General Purpose Computing Devices =>
Errors in Anomaly Detectors




IoT Network
Specialized Computing Devices =>
Possibly Less Errors

Physical devices/processes evolve as per physical laws.

Can we leverage this knowledge to build a model and then use it to reduce errors in anomaly detectors?

# IoT Platform Layer Challenges

Process Isolation Access Control Information Flow Control Updates Authentication

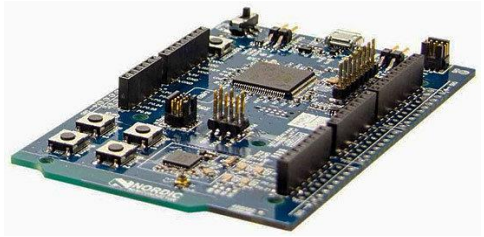
# IoT Platform Layer Challenges

Process Isolation Access Control Information Flow Control Updates Authentication

Ultra-Resource Constrained Devices. E.g., sensors in a bridge, 64K RAM

Hail Dev Module

IMIX Dev Module



nRF51-DK Dev Module

Language Type Safety + Memory Protection Units = Tock OS [1]

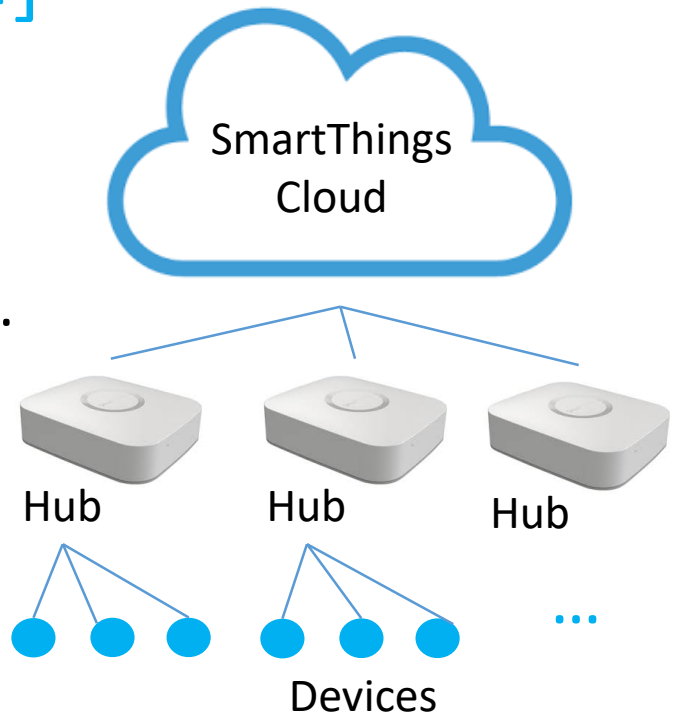
[1] A. Levy et al., Ownership is theft: Experiences building an embedded OS in Rust, in PLOS'15

# IoT Platform Layer Challenges

Process Isolation | Access Control | Information Flow Control | Updates | Authentication

# Analysis of SmartThings [1]

- **What is SmartThings?**
  - Home automation platform
  - Wirelessly control door locks, motion sensors, music players, …
  - Supports third-party apps



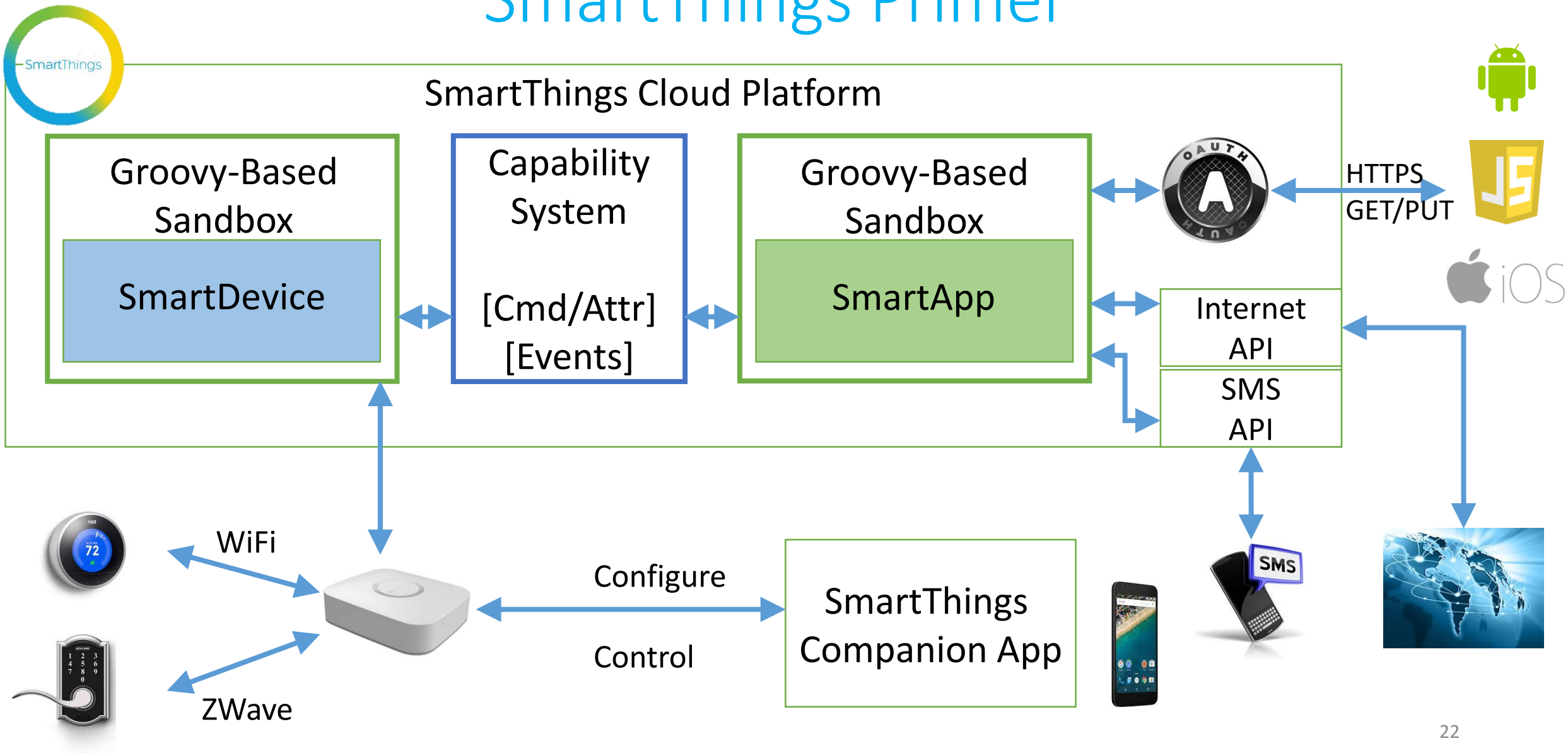

- **Why SmartThings?**
  - Relatively Mature (2012)
  - 521 SmartApps
  - 132 device types
  - Shares design principles with other existing, nascent frameworks

Access Control

Event-Based Programming

[1] E. Fernandes et al., Security Analysis of Emerging Smart Home Applications, S&P 2016

# SmartThings Primer

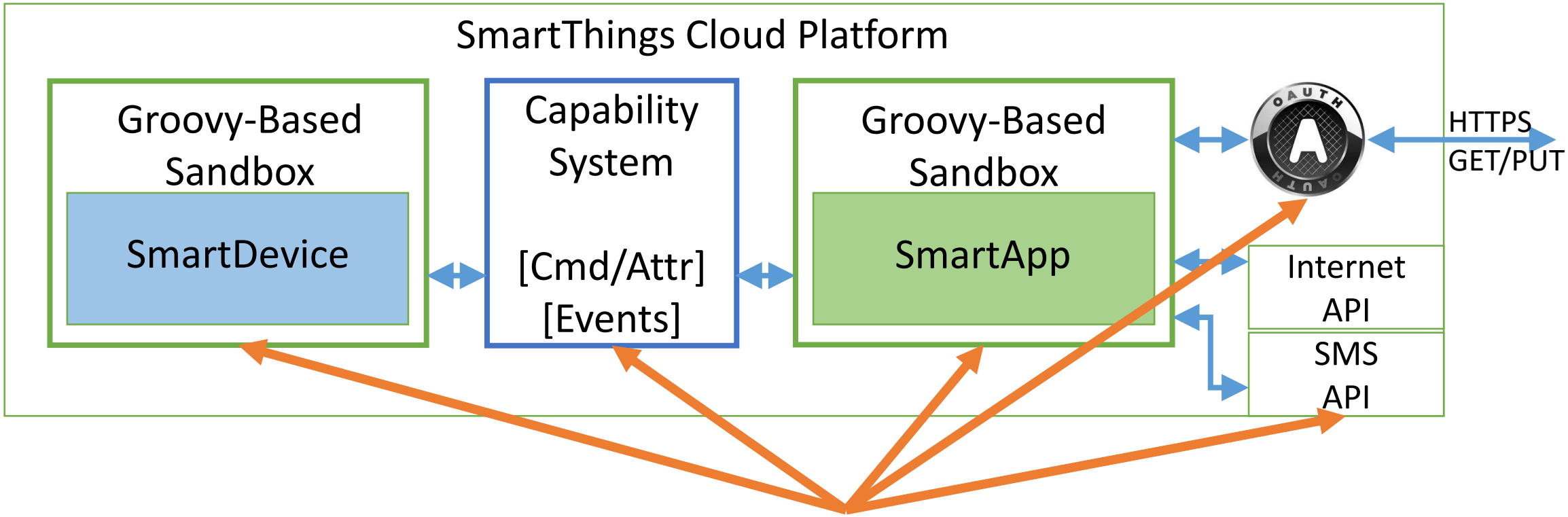


# What makes this analysis challenging?


- Design Documents & Technical Reports
- Platform Analysis Toolchains
  - Dynamic Instrumentation
  - Static Analysis of Platform Code

- No public design documents
- Closed source: cannot use existing analysis toolchains
- Cloud platform has limited public interface

# Analysis Methodology & Threat Model



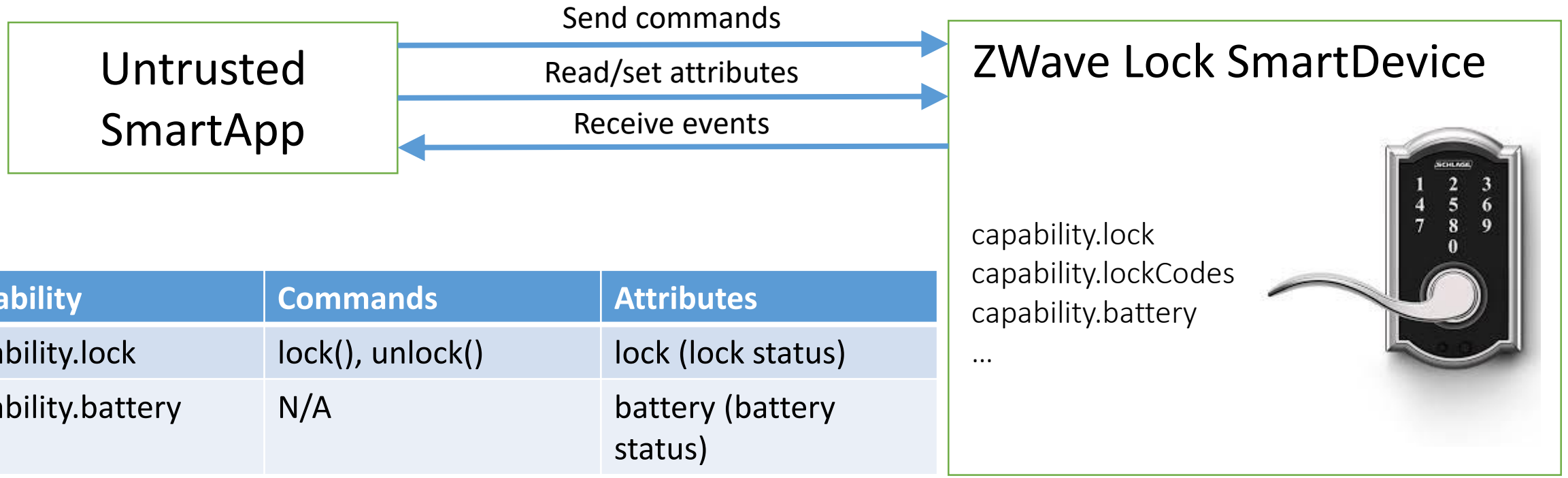

Black-box API Testing w/ Apps + Crash-Log Analysis (along 5 principles)

Static Code Analysis of SmartApps (our toolchain, our dataset)

# Security Eval. of SmartThings: Our Results

| Security Analysis Area | Finding |
|---|---|
| Overprivilege in Apps | Two Types of Automatic Overprivilege |
| Event System Security | Event Snooping and Spoofing |
| Third-party Integration Safety | Incorrect OAuth Can Lead to Attacks |
| External Input Sanitization | Groovy Command Injection Attacks |
| API Access Control | No Access Control around SMS/Internet API |
| **Empirical Analysis of 499 Apps** | **> 40% of apps exhibit overprivilege of atleast one type (55%, 43%)** |
| **Proof of Concept Attacks** | **Pincode Injection and Snooping, Disabling Vacation Mode, Fake Fire Alarms** |

# Capability System



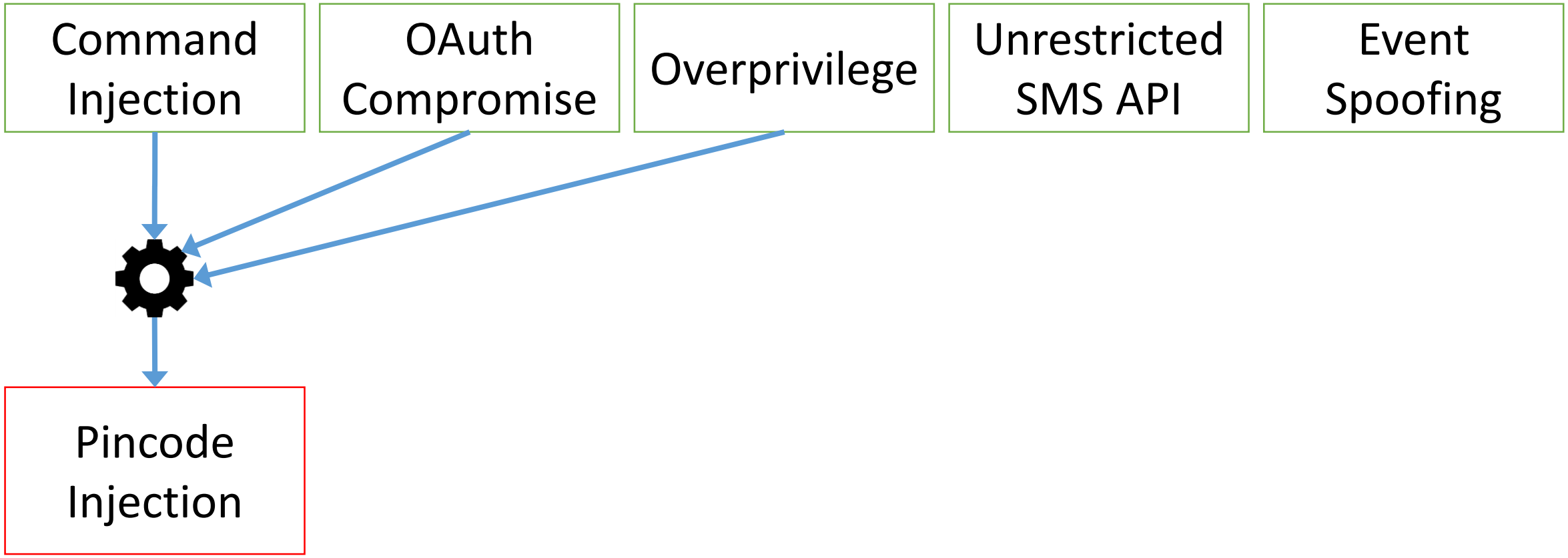

| Capability | Commands | Attributes |
|---|---|---|
| capability.lock | lock(), unlock() | lock (lock status) |
| capability.battery | N/A | battery (battery status) |

Usability
Simpler Coarser Capabilities

Ease of Development
Expressive Functionality

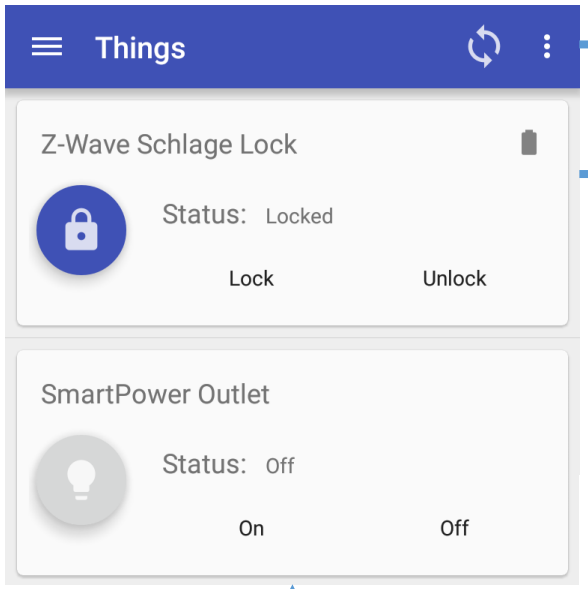
Security
Fine-Grained Capabilities

# Exploiting Design Flaws in SmartThings




Popular Existing SmartApp with Android companion app; Unintended action of setCode() on lock

# Backdoor Pincode Injection Attack




HTTP PUT

HTTP GET


WebService SmartApp

client_id
client_secret

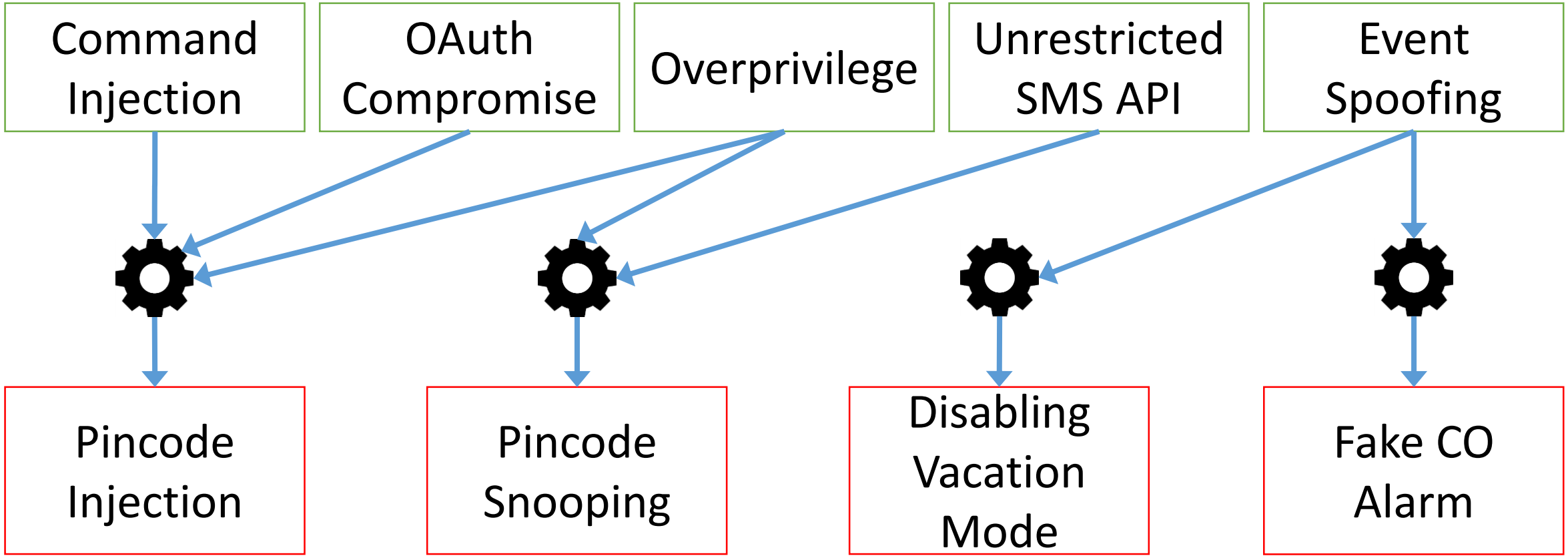
```
mappings {
   path("/devices/:id") { action:
   [ PUT: "updateDevice" ]
}

def updateDevice()
{
   def cmd = request.JSON.command
   def args = request.JSON.arguments
   // code truncated
   device."$cmd"(*args)
}
```

```
{
   command: setCode,
   arguments: [3, '3456']
}
```

Dynamic Method

# Exploiting Design Flaws in SmartThings



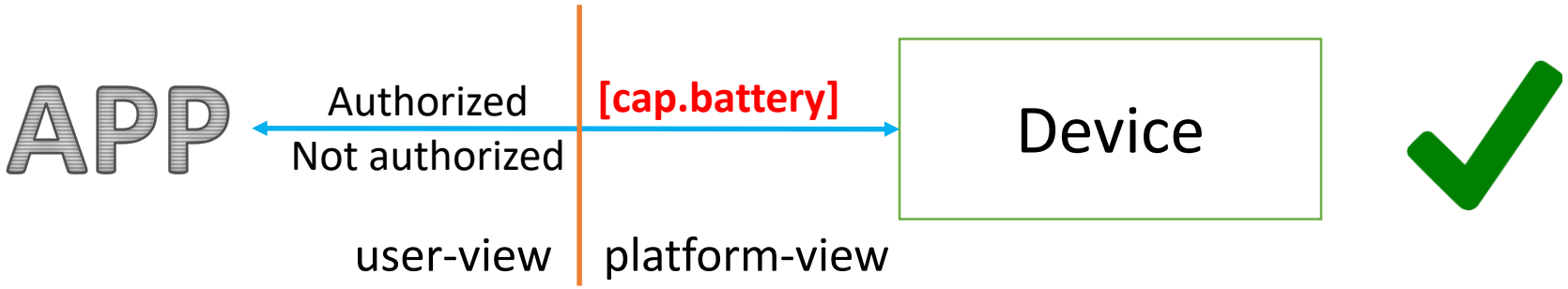

Popular Existing SmartApp with Android companion app; Unintended action of setCode() on lock

Stealthy malware SmartApp; ONLY requests capability.battery

Malware SmartApps with no capabilities;

Gives impression of reduced reliability

# What did we learn from the attacks/analysis?




- App-Device bindings can be more precise without changing UX
  [Coarse SmartApp-SmartDevice Binding Overprivilege]
  - Fixing of event system overprivilege is a by-product

- Risk-based Capabilities/Permission => Fundamental Risk Asymmetry

- Permissions are only useful as a first line of defense for IoT platforms, can we do better?

# IoT Platform Layer Challenges

Process Isolation | Access Control | Information Flow Control | Updates | Authentication

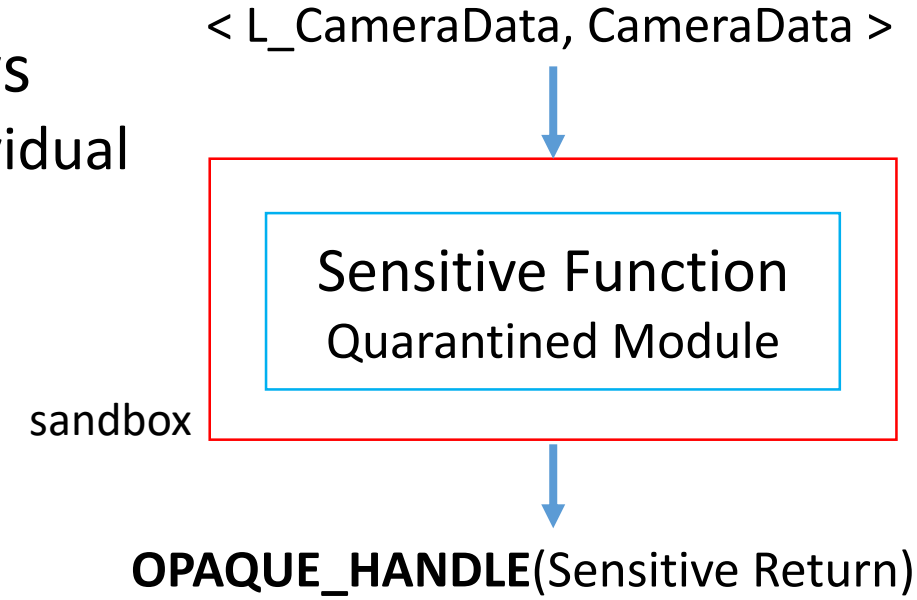
# FlowFence [1]

## flow tracking is a first-class primitive

- Restructure apps in terms of information flows
  - Apps request point-to-point flows instead of individual permissions

    Camera data only used to activate door lock

- Language-level primitive to isolate and flow-track sensitive code




✓ Dynamic labeling scheme

✓ Programmer-defined tracking granularity

✓ Supports existing tools, languages, IDEs; no changes to OS

[1] E. Fernandes et al., FlowFence: Practical Data Protection for Emerging IoT Application Frameworks, USENIX Security 2016

# A Spectrum of Information Flow Tracking

Architecture Level
(Instructions, Gates)
Resource Overhead; Special Hardware
RIFLE, Execution Leases, …

OS-Based DIFC
(Page/Process Level Tracking)
May Overtaint; Coarse-Control
HiStar, Asbestos, Flume, …

Language-Based DIFC
(Type Systems, Variable-Level Tracking)
Dev. Learning Curve; Limited Control over External Resources
Jif, Jeeves, …

Challenge: Applying flow tracking principles to a specific domain

"Component-Level" DIFC
(Well-defined component-level tracking)
Combines PL & OS Techniques
Laminar, COWL, Aeolus …

```
definition(
    name: "DemoApp", namespace: "com.testing",
    author: "IoTPaper", description: "Test App",
    category: "Utility")

//query the user for capabilities
preferences {
  section("Select Devices") {
    input "lock1", "capability.lock", title:
        "Select a lock"
    input "sw1", "capability.switch", title:
        "Select a switch"
  }
}

def updated() {
  unsubscribe()
  initialize()
}

def installed() {
  subscribe sw1, "switch.on", onHandler
  subscribe sw1, "switch.off", offHandler
}

def onHandler(evt) {
  lock1.unlock()
}

def offHandler(evt) {
  lock1.lock()
}
```

Trigger

Process

Action

Device Independence

Runtime Binding of Actual Resource/Device

SmartThings

openHAB
empowering the smart home

IFTTT

Ur et al., Practical Trigger-Action Programming in the Smart Home, CHI'14

# IoT Platform Layer Challenges

Process Isolation | Access Control | Information Flow Control | Updates | Authentication

Updates should be careful and planned => Economic Impact or Worse

## Cyber Incident Blamed for Nuclear Power Plant Shutdown

*By Brian Krebs*
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

TOOLBOX
Resize Print
E-mail Reprints

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

# IoT Platform Layer Challenges

Process Isolation | Access Control | Information Flow Control | Updates | Authentication

Updates should be careful and planned => Economic Impact or Worse

IoT devices in the field could be intermittently powered => How to update during power losses?

IoT devices may not be updateable fundamentally [1] => no infrastructure was built by manufacturer

[1] T. Yu et al., Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things, HotNets-XIV.

# IoT Platform Layer Challenges

Process Isolation | Access Control | Information Flow Control | Updates | Authentication


Weak Passwords
Default Password (Mirai)
Password Re-use

Client Side Password Strength Estimators
e.g., https://github.com/dropbox/zxcvbn

GIZMODO

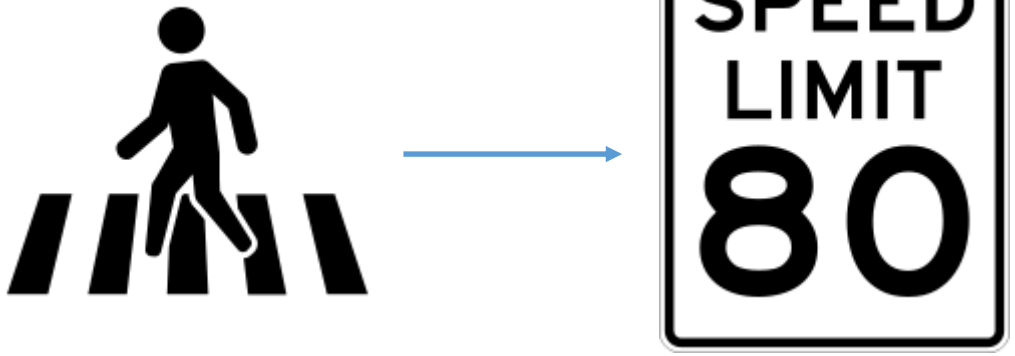
**TV Report on Accidental Amazon Orders Triggers Attempted Amazon Orders Across San Diego**

Hudson Hongo
1/08/17 8:33pm · Filed to: ALEXA

106.9K 108 8

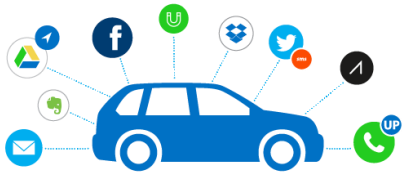
# Application Layer Challenges

- Physical Co-Relations
  - E.g., Garage door closes, nearby speaker picks up acoustic pattern
  - E.g., Vehicle speed increases, change in engine vibration patterns
- Machine Learning [1] for Control
  - E.g., Robots
  - E.g., Autonomous Vehicles




[1] N. Papernot et al., Towards the science of security and privacy in machine learning, CoRR, vol. abs/1611.03814, 2016.

# The Internet of Things Stack




Application Domains






IoT Platforms/ System Software




Connectivity Protocols/ Network



Devices/ Hardware

Usable Security Issues

# IoT Security | What, Why, How

Earlence Fernandes
earlenceferns@gmail.com

IoT Security Research: A Rehash of Old Ideas or New Intellectual Challenges?
E. Fernandes, A. Rahmati, K. Eykholt, A. Prakash
arXiv 2017

https://web.eecs.umich.edu/~earlence/

Consider Submitting

https://iotsecurity.eecs.umich.edu

https://www.safethings.info/