Internet of Things: Security Issues and Challenges

"Your next car will need a firewall."

– Title of article by Martin Bryant, The Next Web, April 7, 2016

Agenda

- What is the “Internet of Things?”
- How does security change with IoT?
- General notions of security and privacy
- Examples of current state of IoT security
- What research have people done in this area?

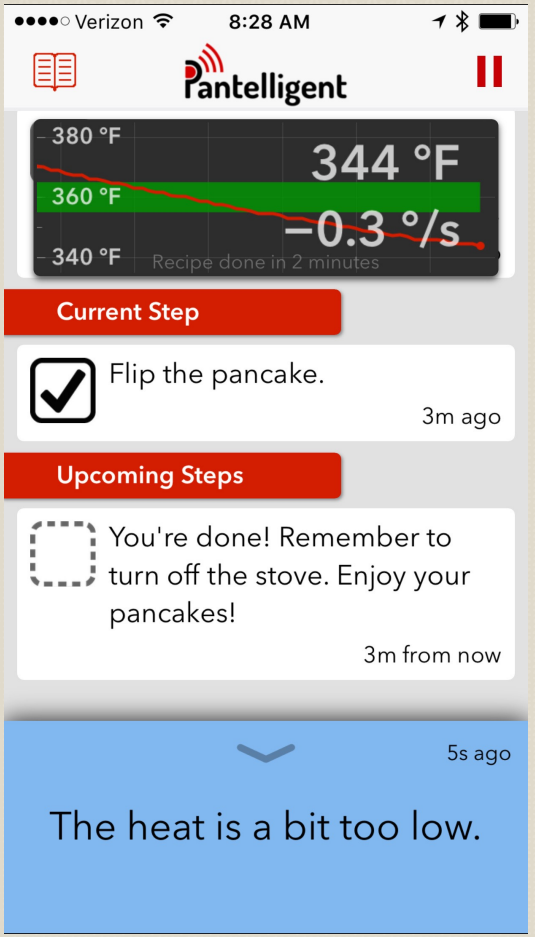
IoT Everywhere

- Healthcare
- Education
- Banking
- Agriculture & Farming
- Transportation
- Manufacturing
- Retail

All critical infrastructure sectors

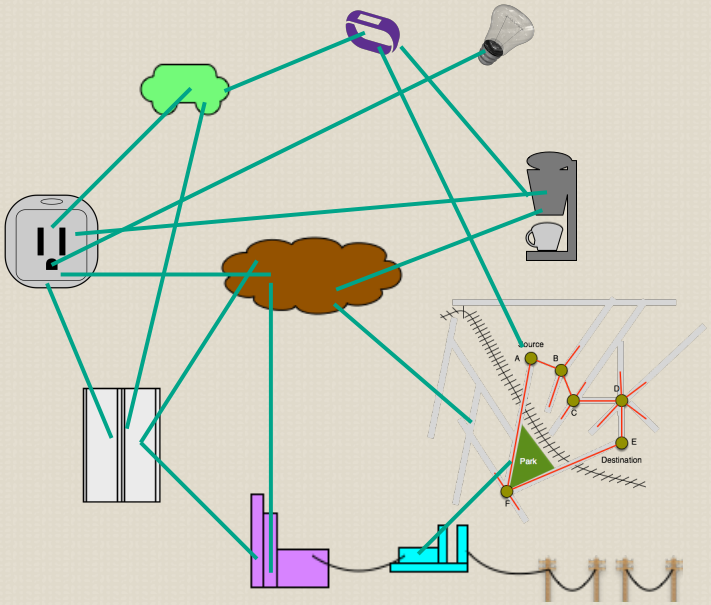
What is a thing?

- No unique definition of a “thing”
  - Networked **video cameras**
  - WiFi Routers
  - Speakers
  - Drones
  - Cars
  - Refrigerators
  - Coffee machines
  - **Smart locks**, shutters, toys, and light bulbs



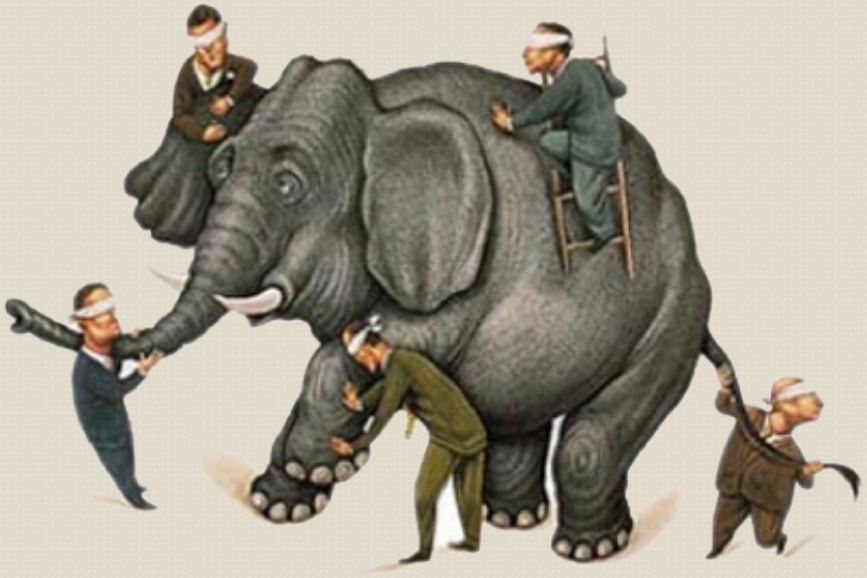
What is the “Internet of Things?”

- Every “thing" has an IP address
  - Maybe or maybe not?
- IoT =? Smart Environment
  - Smart cities
  - Smart grid
  - Smart health
  - Connected life



Blind Men and the Elephant

- Design of low-power embedded communicating devices
- Scalable infrastructure for connectivity
- Software platforms
- Applications
- Smart end-to-end analytics

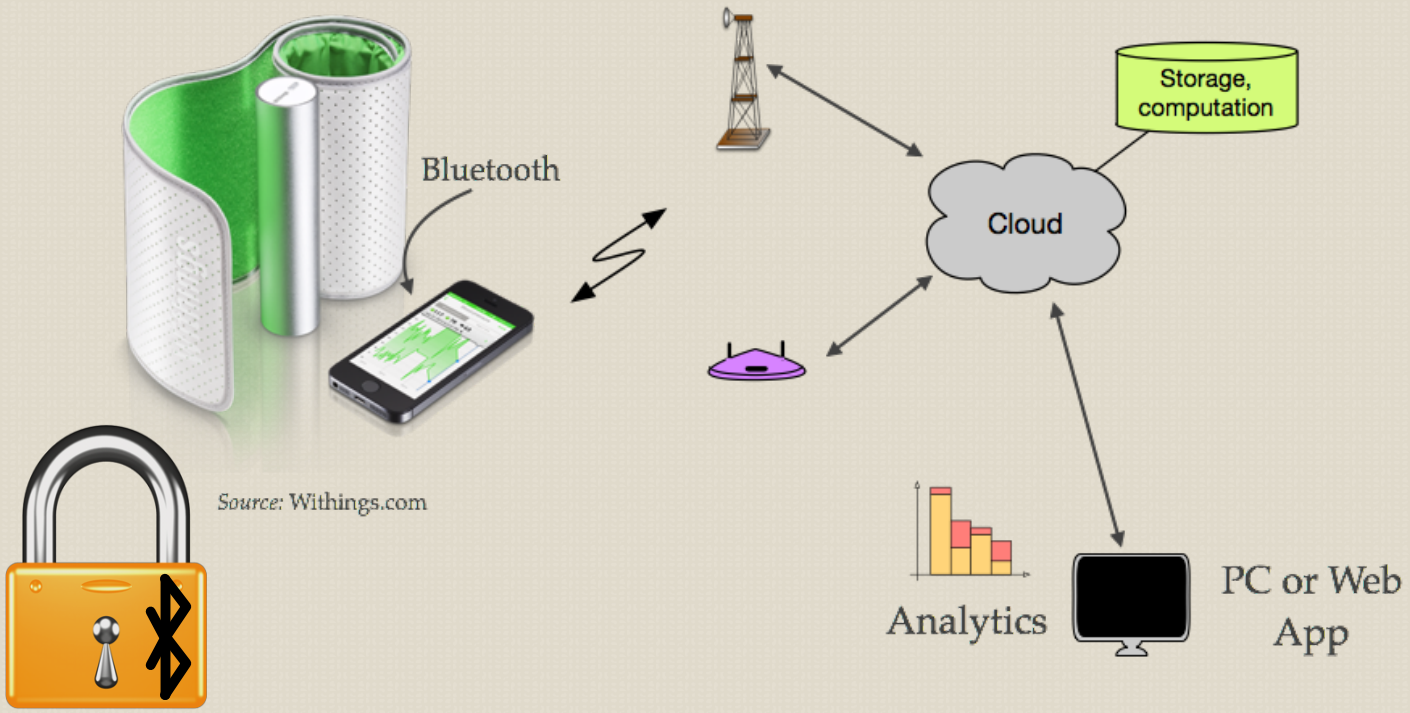


Picture Source: http://4.bp.blogspot.com/-gL2fYhYZP68/UHBFQjzWoQI/AAAAAAAAEsE/12-xXmcAHY4/s1600/blindmenandelephant.jp

How about the “Internet” of Things?

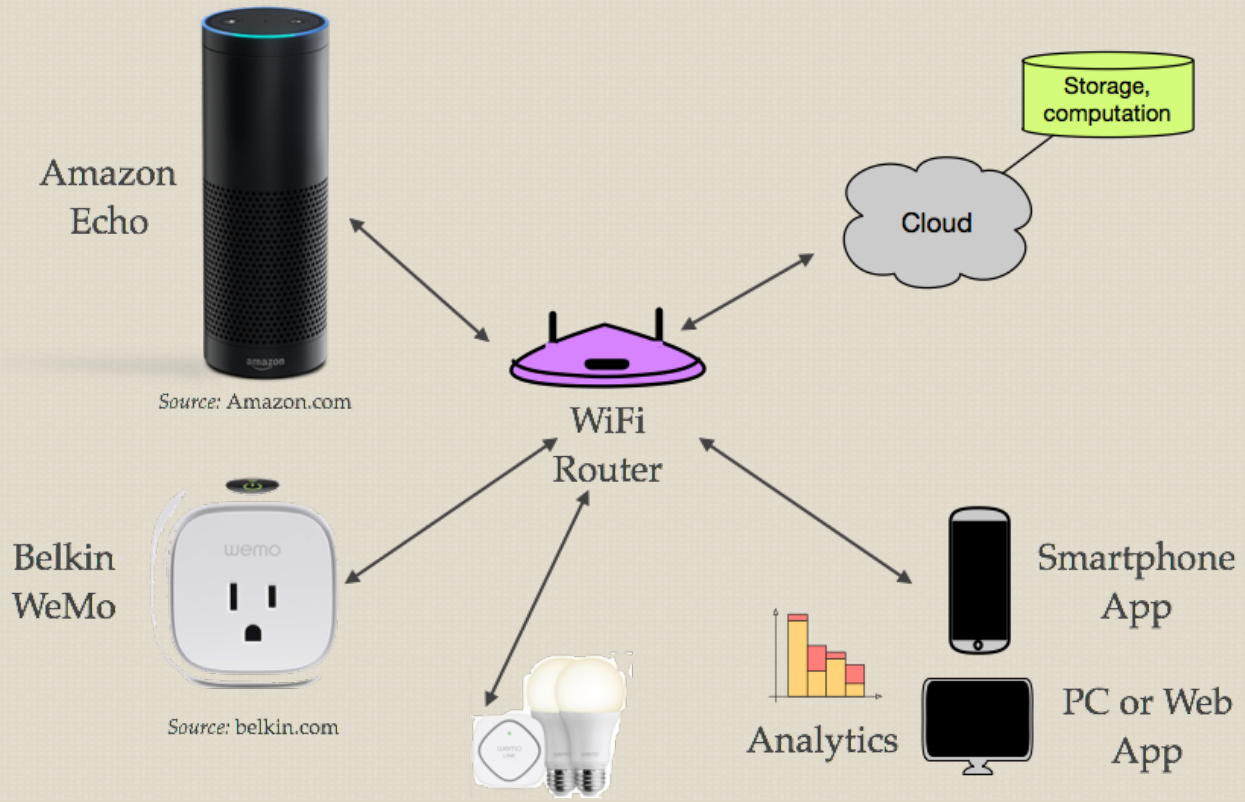
- Given: “Things” are connected
- How?
  - Does every “thing” talk with every other “thing”?
- Various paradigms for the network and connectivity
  - High-level view
  - Some details

Example (1)

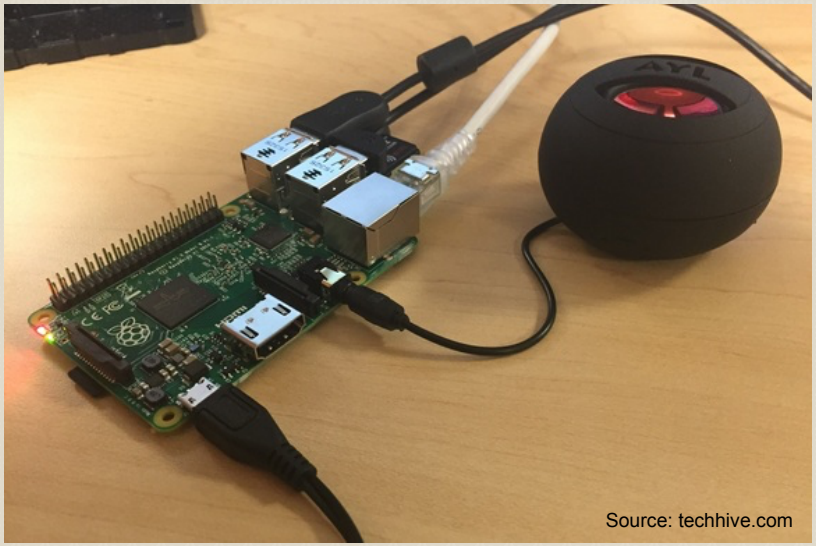


Source: Withings.com

Example (2)


Amazon
Echo
Source: Amazon.com
Storage,
computation
Cloud
WiFi
Router
Belkin
WeMo
wemo
Source: belkin.com
Smartphone
App
Analytics
PC or Web
App

DIY IoT



Source: techhive.com

SEEED Windows 10 IoT Core Grove Kit

Exclusive kit for Windows 10 IoT Core & Raspberry Pi 3
Easy to use: Solder-less, breadboard-less
Coming Summer 2016

Source: pcworld.com

Source: arduino.cc

Commercial IoT “Solutions”

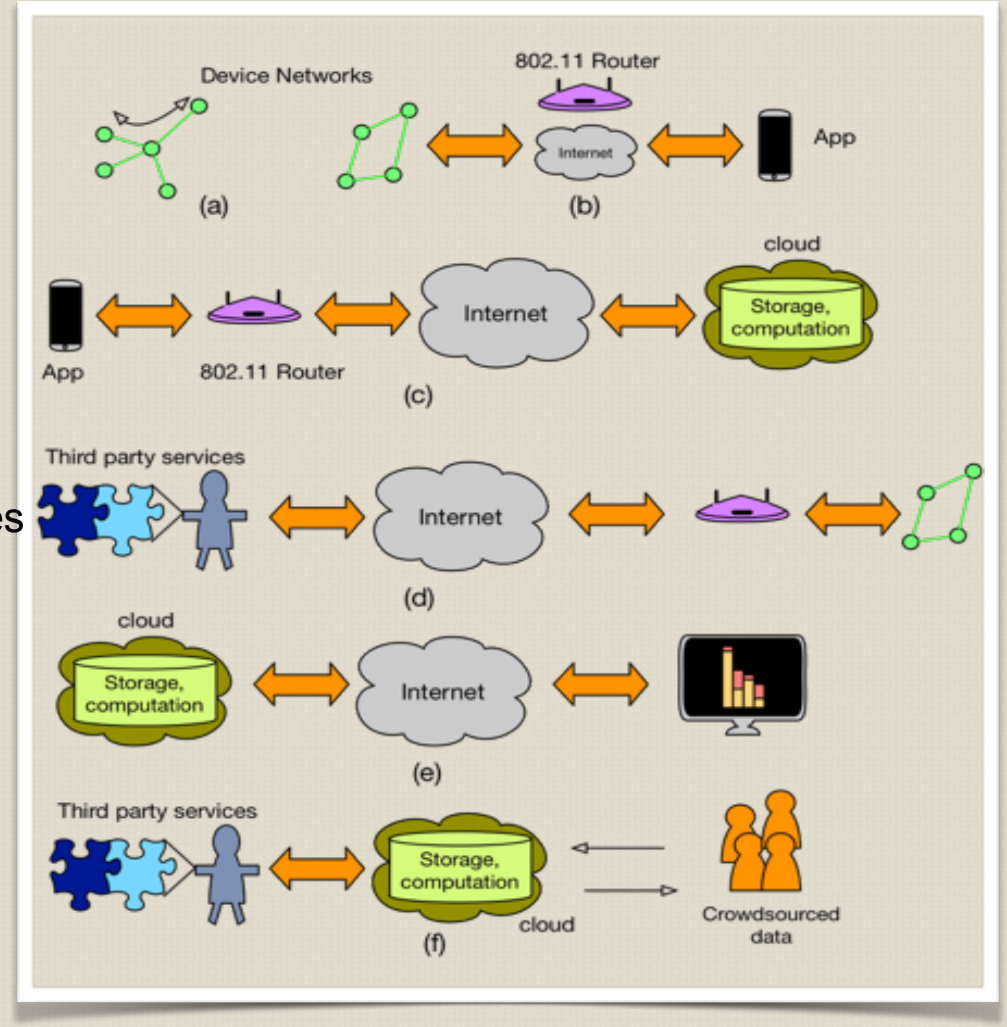
- Apple’s HomeKit
  - Control IoT devices using iOS and apps
- Cisco’s Fog Computing
  - Move analytics and computation closer to the edge
- Google’s NEST
  - Automation and smart devices
- IBM’s NodeRed and Bluemix
  - Processing and analytics of various data pipes
- Intel’s IoT platform
  - Software, hardware, reference stack targeting developers
- Microsoft’s nitrogen.io
  - Smart device front-ends using Node.js libraries and the Azure cloud platform

Example (3)

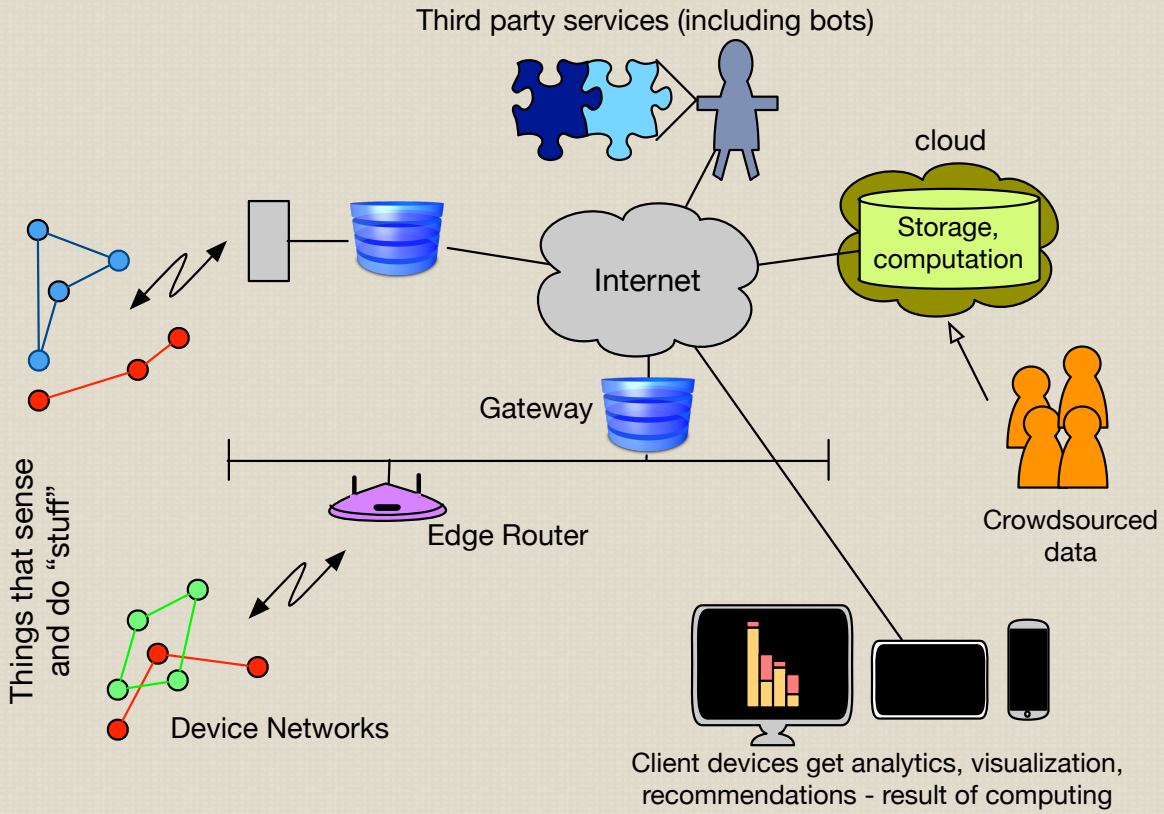
- Similar to previous notions of sensor networks
  - Crop monitoring for loan collateral
  - Temperature sensing in a mall
  - Remote healthcare monitoring
- Differences
  - Back-end intelligence and analytics
  - Some crowd-sourcing

Six Pathways

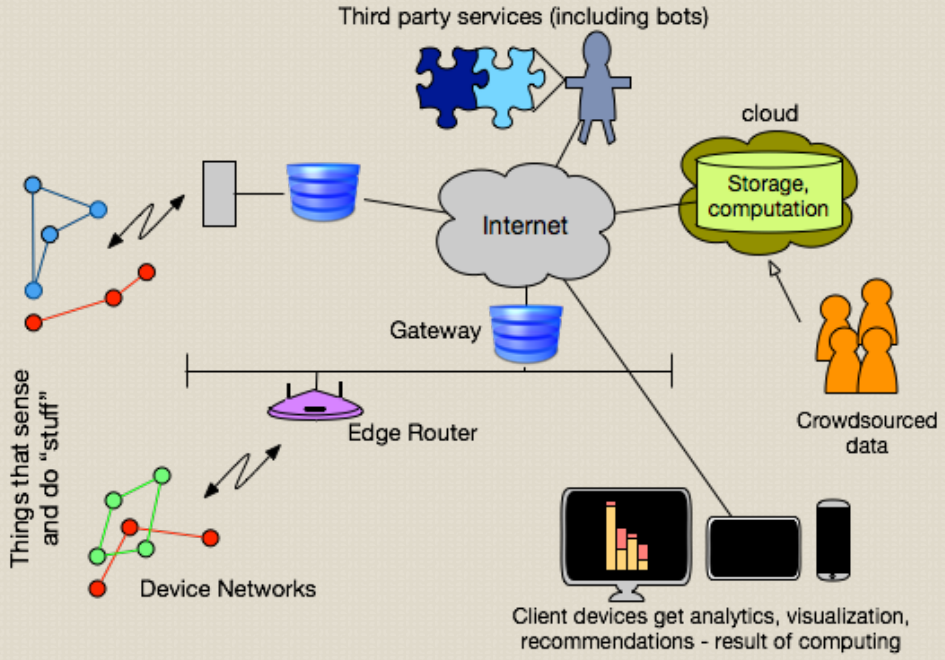
- Device Network
- App & Things (Devices)
- App & Cloud
- Device and Third-Party Services
- Analytics and Presentation
- Third-Party Services



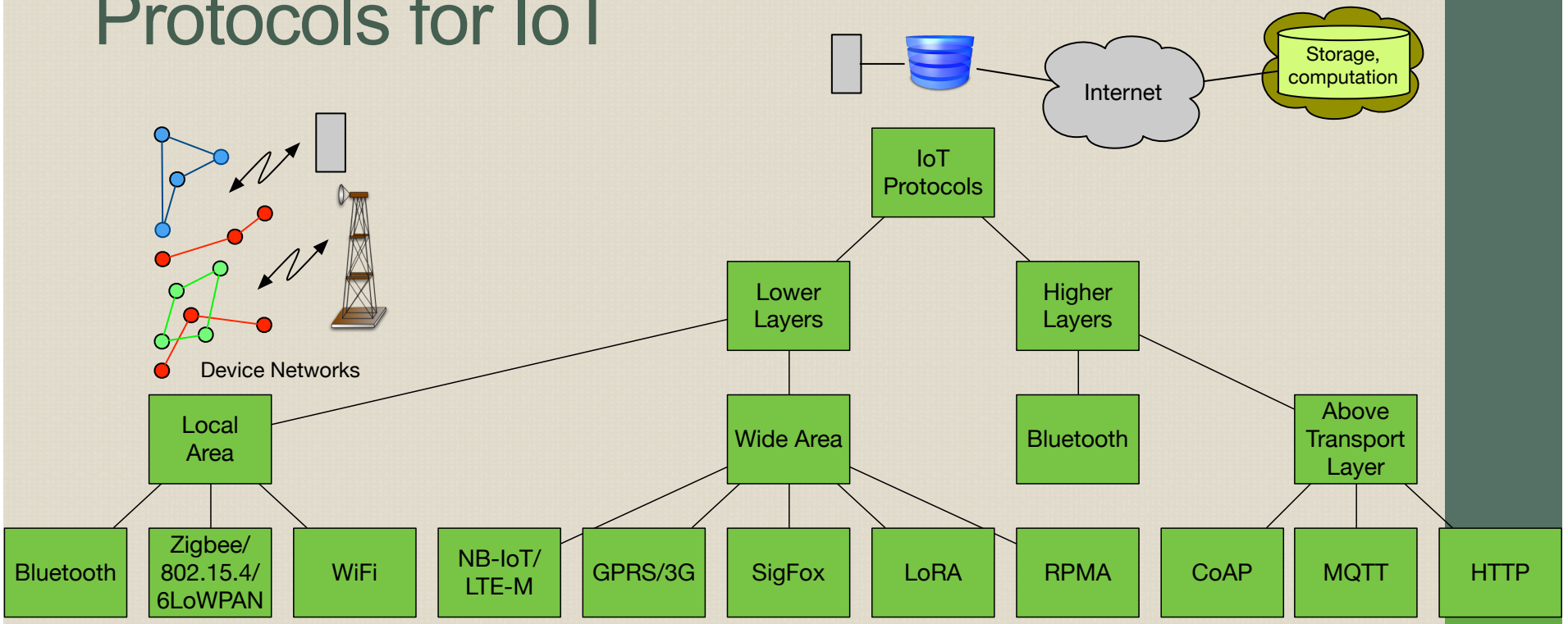
Summary: High-Level Architecture



Security Threats at a High Level



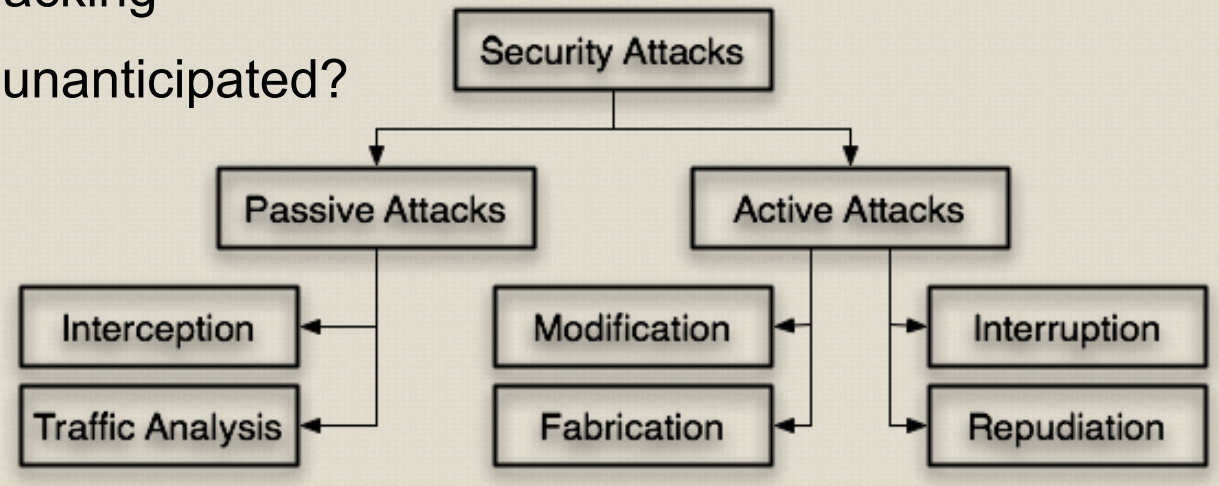
Protocols for IoT



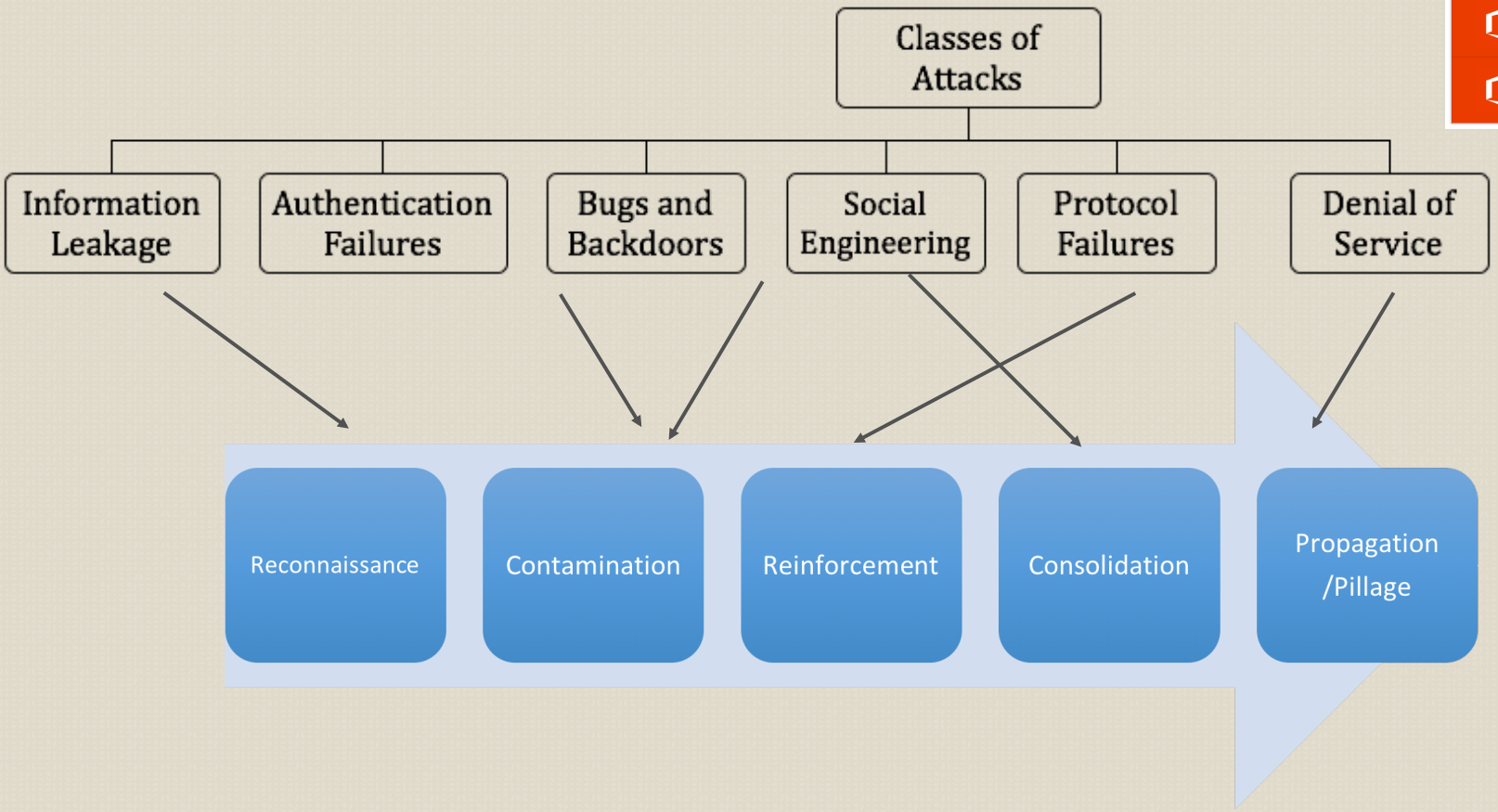
- Too numerous to have an exhaustive list

Attacks

- When threat becomes real
- Passive and active
  - Privacy Vs. Hijacking
- Anticipating the unanticipated?



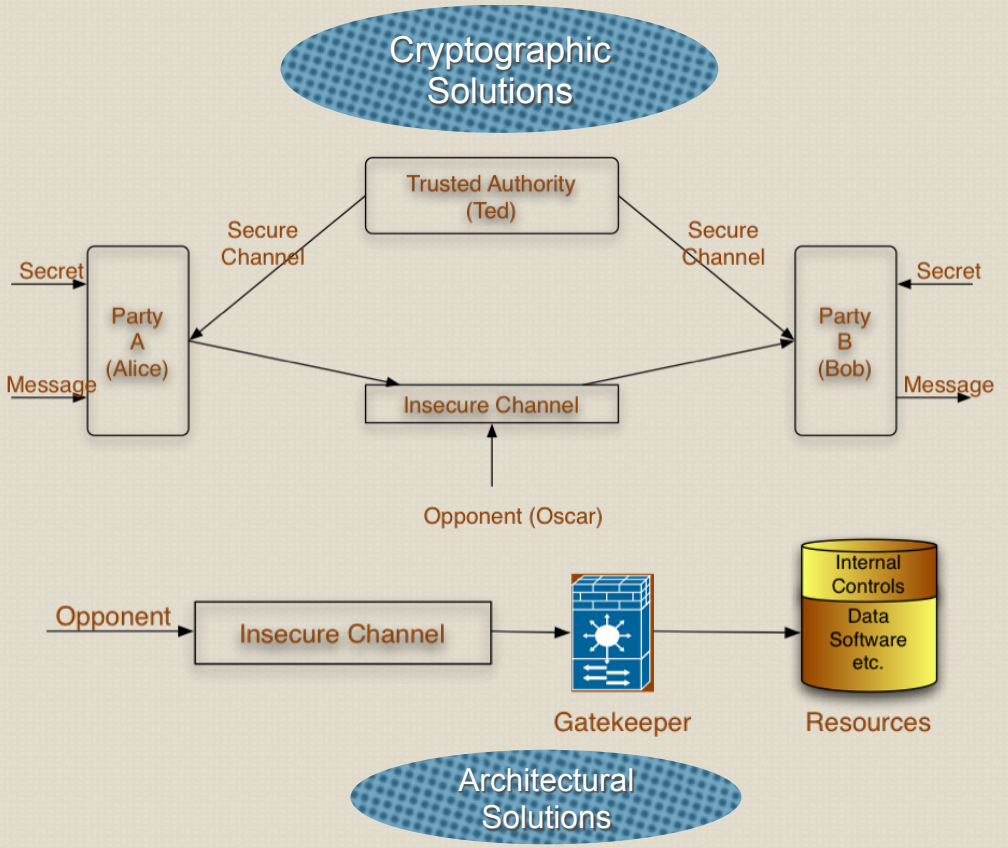
Classes of Attacks



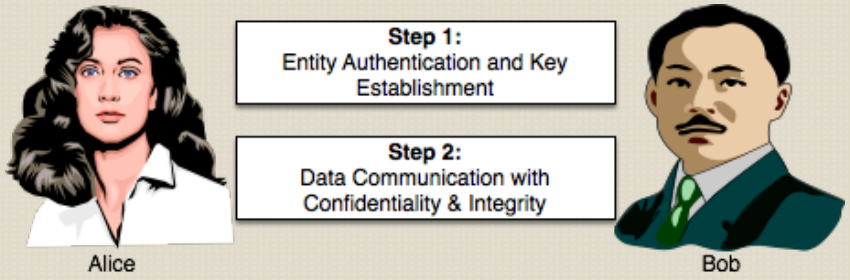
Information Assurance in General

Privacy &
Confidentiality
Integrity
Authentication
Non-repudiation
Availability

Protection/Prevention
Detection
Assessment
Response

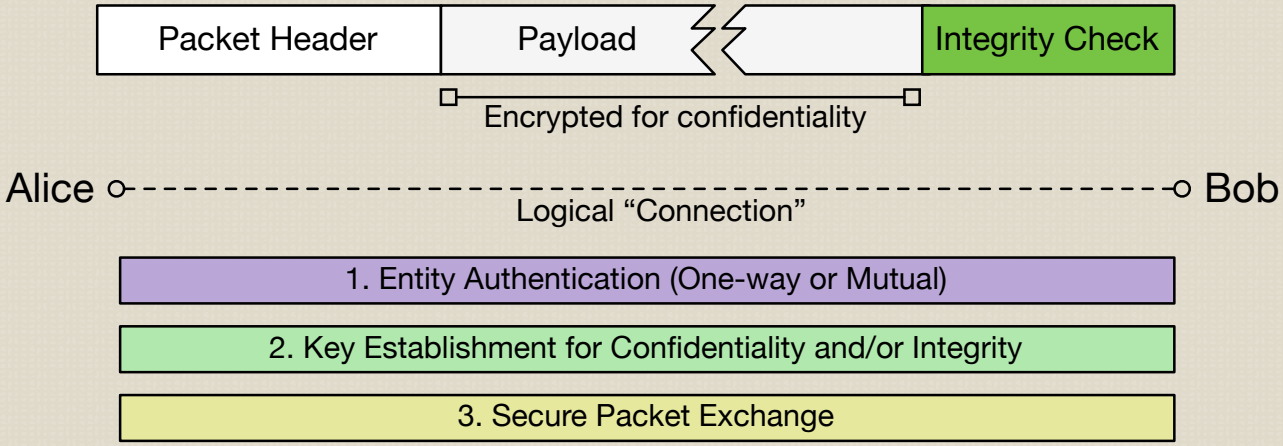


Cryptographic Protocols – General Process



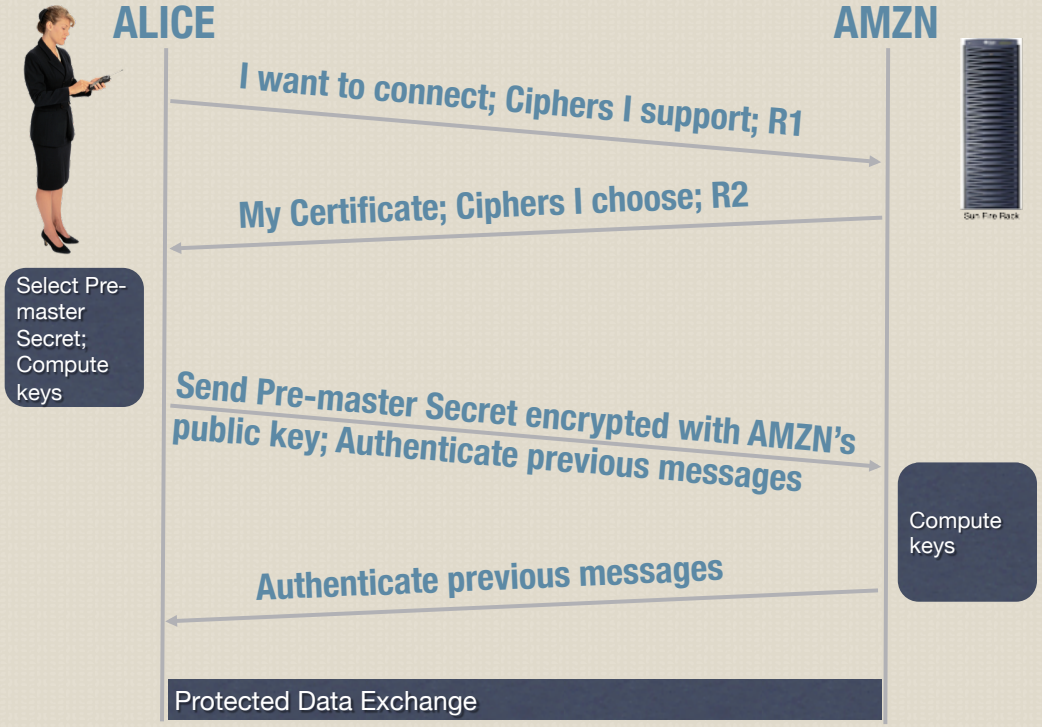
- Usually “two-party” protocols
- Alice and Bob are honest parties
- Oscar is the bad guy – somewhere in the middle

Cryptographic Protocols (2)

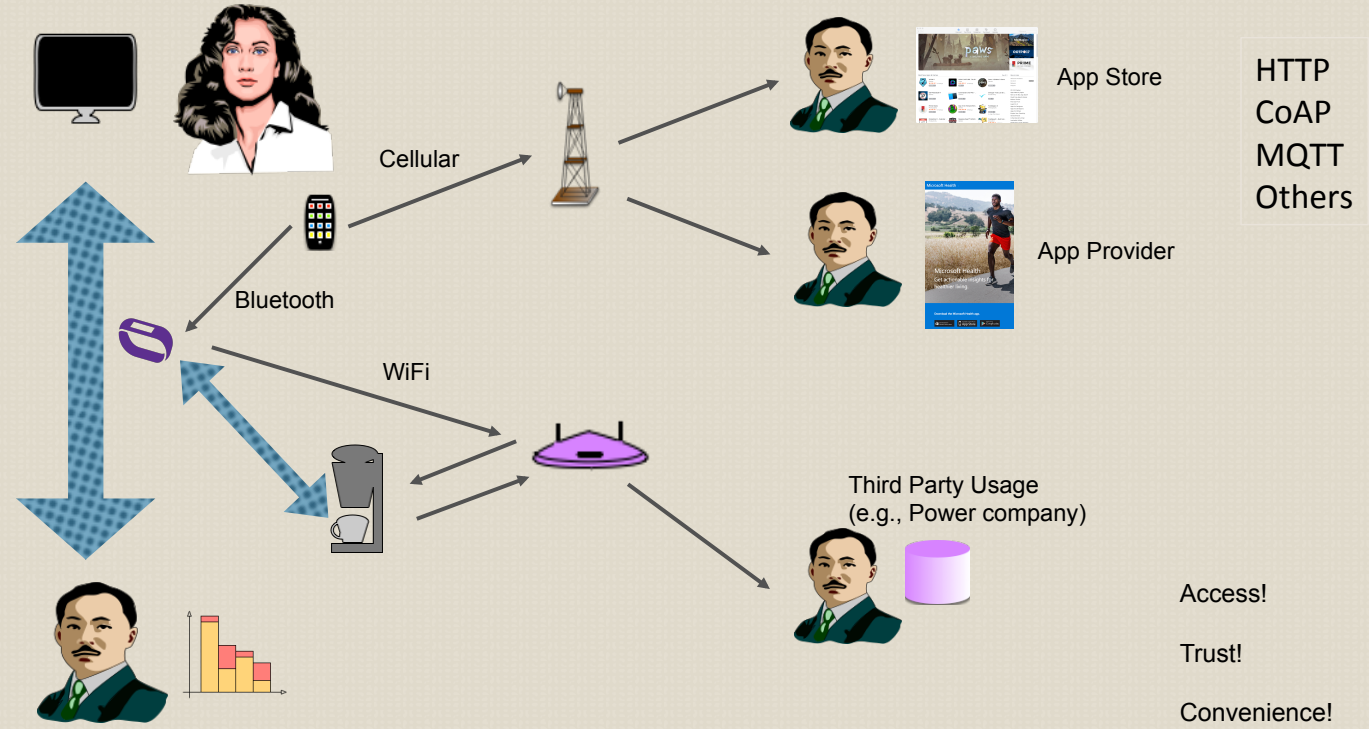


- At various levels of the protocol stack
- Protecting link, network, and application data

General Process – SSL/TLS



General Process and… IoT??



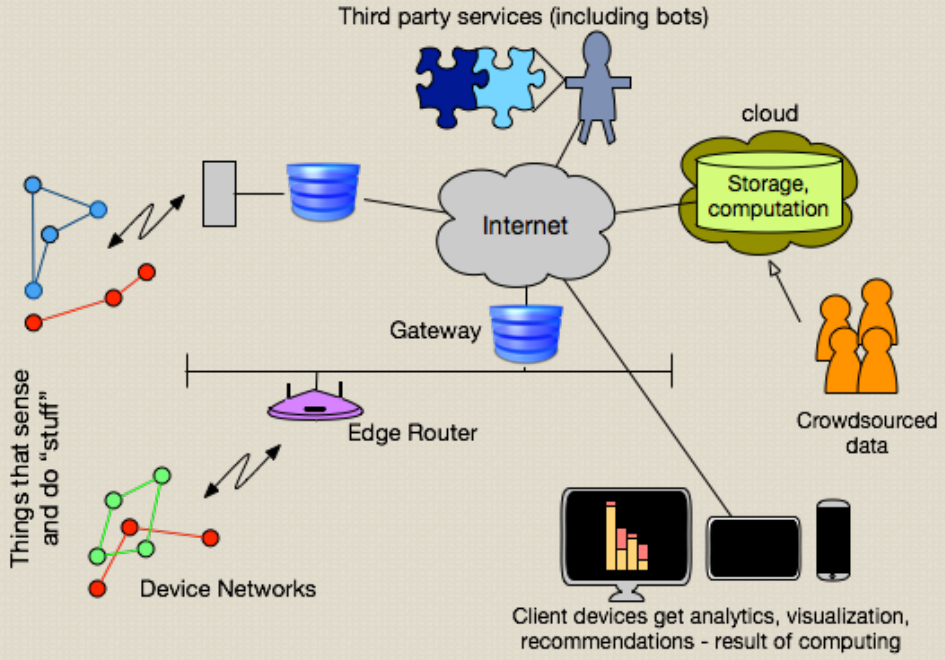
HTTP
CoAP
MQTT
Others

Access!

Trust!

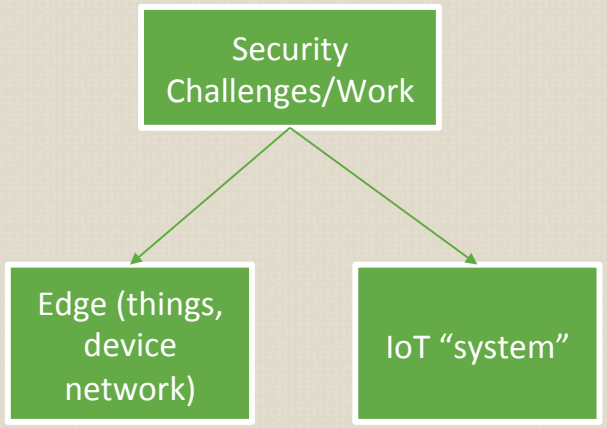
Convenience!

Security Threats at a High Level



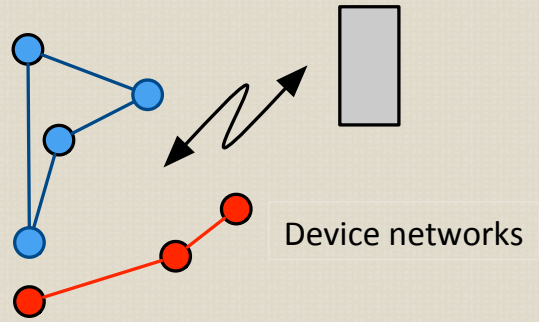
So…

- Many security challenges
- Subdivision into smaller problems
  - Heterogeneity of devices and platforms
    - Capabilities vary widely
  - Usable security of IoT “systems”
    - IoT devices and systems are complex and (human) users do not comprehend the intricacies



Predominant focus on edge

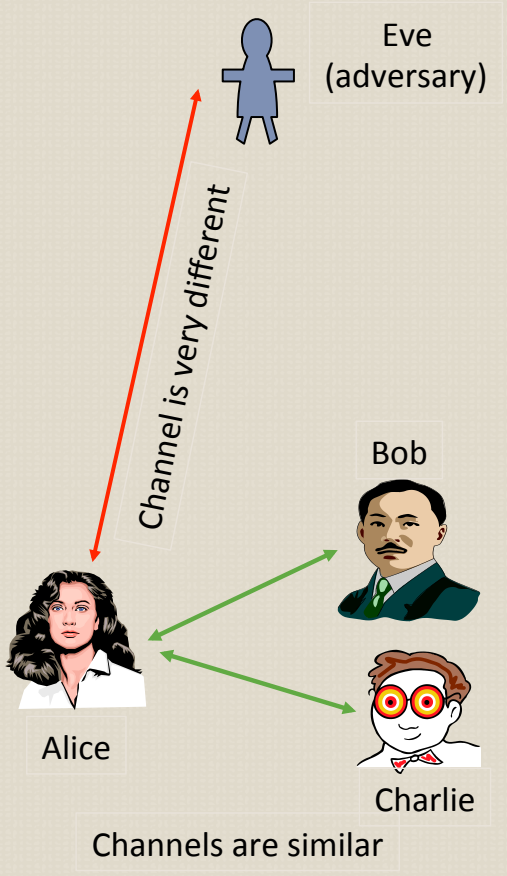
- Scale (number of devices)
- Resource constraints of devices
- Long device life
- Device cannot be updated
- **Key establishment and content delivery to devices**
  - Post manufacturing
- Device exploitation
  - Boot process, software bugs
  - Hardware, chip, side-channels
  - Network access



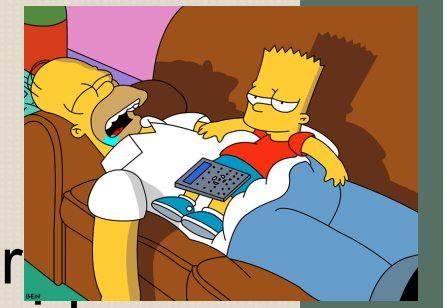
- Use device function to generate high-entropy keys
  - Inter-heart beat times

Physical Layer Security

- Idea
  - Channel between honest communicating parties can be used to establish keys
    - There is “entropy” in the channel to get a set of matching random bits
  - Eavesdropper will see a substantially different channel unless close to one of the honest parties
- Needs authentication to protect against active attacks
  - Can use a trusted third party that is physically close enough



Smart Lock or Am I Simply Lazy?



- D. Strobel, B. Driesser, T. Kasper, G. Leander, O. Oswald, F. Schellenberg, C. Paar, "Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System," Available at https://eprint.iacr.org/2013/598.pdf
- G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, D. Wagner, "Smart Locks: Lessons for Securing Commodity IoT Devices," *Asia CCS*, June 2016.
- D. Coldewey, "'Smart' locks yield to simple hacker tricks," TechCrunch, August 8, 2016.

Image Source: http://images.fanpop.com/images/image_uploads/Lazy-being-lazy-137901_800_600.gif

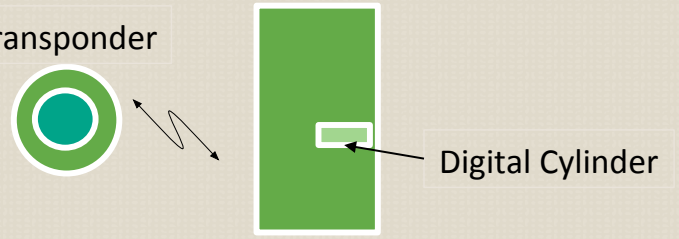
History

- Remote keyless entry
  - Used in cars (Keeloq), has many vulnerabilities
- Why smart locks?
  - Convenience
  - Fine grained controlled access!
  - Data!

The Story of Smart Locks

- Many types
  - Some connect only through Bluetooth to App
  - Others connect via WiFi
- Easy ones
  - Quicklock, iBluLock, and Plantraco transmit passwords in plaintext over Bluetooth
  - Others fall for replays (Ceomate, Elecycle)
- Security through “obscurity”
- Most advertised themselves as “locks” when discovered through wardriving

SimonVoss System (1)



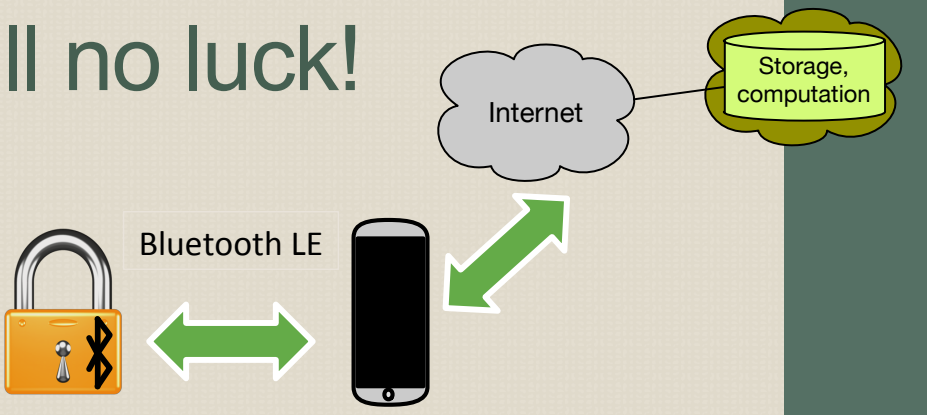
- Uses a “digital key”
  - Press key to hear two beeps
  - Then manually opening the lock is allowed for a few seconds
- Security through obscurity – crypto protocol is proprietary
- Many modes, but connects to a server using 868 MHz wireless links
  - Locks can be configured at the server
- Opening of locks is logged

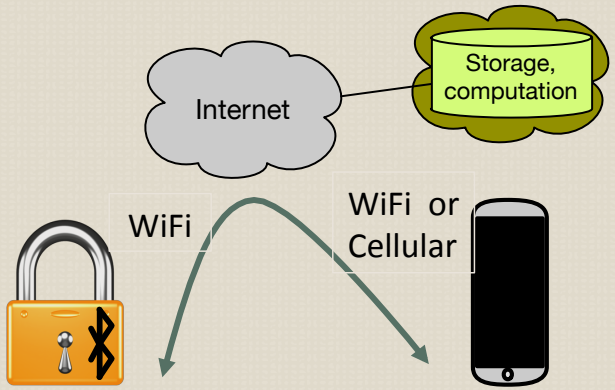
SimonVoss Flaws (now perhaps fixed)

- Chip was reverse engineered to discover proprietary security mechanisms
  - Uses modification of DES
- Each lock stores four *identical* 128-bit keys that allows discovery of any transponder's key
  - Hardcoded keys are easy to clone if discovered
- Uses challenge-response protocol (IDs are in plaintext)
  - Up to 88 challenge bits remain unchanged in each exchange!
- Key can be discovered in a few seconds using a PC

Five Smart Locks – Still no luck!

- Two models
  - Most follow BLE approach
    - Can interact with lock even if Internet connection is blocked
  - Lockitron follows WiFi-Internet model





Examples of problems

- After getting access, if a phone is switched to airplane mode, it retains access for ever!
  - State consistency attack
- Unintentional unlocking
  - If in BLE range, automatically the lock opens
  - Physical attackers may enter using this feature
    - Geofencing does not always work
- Relay attacks are possible

IoT “System” - Sources

- (1) **Video Camera Security and the recent Mirai attack**
- (2) **Transparency** - S. Beran, E. Pignotti, and P. Edwards, “Interrogating Capabilities of IoT Devices,” 5th International Provenance and Annotation Workshop, Cologne, Germany 2014
- (3) **Cloud/Authorization** – S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, “IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," IEEE Sensors, Vol. 15, No. 2, Feb 2015.
- (4) **Cloud Commissioning** – T. Hardjono and N. Smith, “Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains,” IOTPTS, 2016.
- (5) **Privacy/Integrity** - N. Davies and others, "Privacy Mediators: Helping IoT Cross the Chasm," ACM HotMobile, 2016

The Mirai Attack

- Sources:
  - (1) Laura Hautala, “Why it was so easy to hack the cameras that took down the web,” CBS News, October 25, 2016
  - (2) Mikey Campbell, “Mirai-based DDoS attack highlights benefits of Apple's secure HomeKit platform,” Appleinsider.Com, October 21, 2016
  - (3) **HoneyPots** – Y. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, “IoTPOT: Analyzing the Rise of IoT Compromises,” WOOT 2015
  - (4) J. Obermaier and M. Hutle, “Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems,” IOTPTS, 2016
  - Other news sites

What happened to Dyn

- Dyn provides DNS services to 6% of Fortune 500 companies
- At least three waves of DDoS attacks on Dyn
  - Morning, noon, and later afternoon
- Twitter, Netflix, Spotify, Visa, AirBnB were among the affected sites
- The attacks came from “things” infected by the Mirai malware

What “things” were infected?

- Mostly DVRs and IP cameras made by Xiongmai
  - Directly connected to the Internet with an IP address and with access to large bandwidth
  - Registries may list the IP addresses
- How were they attacked?
  - Telnet/SSH backdoor with “hardcoded” password
- Mirai created botnets of up to 100,000 “things”
  - Later used to attack Dyn

Security Problems with Cloud Based Video Surveillance Systems (1)

- Cameras that allow access to video through the Internet using a cloud server or gateway
  - Local Attacker
    - Guest in a hotel or an employee with local *network* access but not physical access
  - Remote Attacker
    - Can reach cloud servers, but not the camera through the Internet
- Cameras use TLS or SSL, sometimes proprietary protocols to talk with cloud server
  - One camera with proprietary protocol used common pre-shared keys in all cameras!
  - Those using TLS simply used an ID based on MAC address to get access to server!

Security Problems with Cloud Based Video Surveillance Systems (2)

- All cameras could be reached through the local network using HTTP for their configuration
- Weak login credentials
  - Example: If MAC address is 01:23:45:67:89:AB, the password is BA9876543210 in base 64 encoding with a known padding
  - Attacker can view and record video streams once password is revealed
- If camera is impersonated to cloud, user may be alarmed or service may be denied

Honeypots for IoT

- Japanese group implemented a Honeypot for IoT devices that emulates Telnet services of various IoT devices
  - Goal was to analyze Telnet based scans (think Mirai - mostly DVRs and IP cameras were attacked)
  - Emulated different CPU architectures (ARM, PPC)
  - Discovered that common behavior is to do DoS attacks
- Increased scans and attacks from January 2014-January 2015
  - 4 malware families, reconnaissance and malware infection were done by *different* hosts in coordination

Transparency

- Who “owns” the devices?
  - Manufacturer, OS Vendor, App Developer, Service Provider, Me?
- What are the devices doing?
  - What information are they gathering?
  - What data are they manipulating?
  - Who gets access to the data? What is shared?

Transparency (2)

- **Trusted Tiny Things project**
- Developed an ontology using OWL (Web Ontology Language)
- Allows discovery of
  - who is behind the activity of an IoT device
  - what activity(ies) an IoT device is (capable of) performing
- Hope
  - Now find out if the devices are doing the things they should be doing
- Cons
  - No verification of whether the reports are fabricated or modified

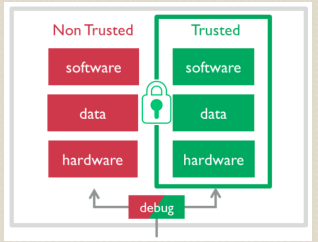
Privacy

- Many problems with privacy in IoT
- General agreement – users own their data
  - But do they really?
- Among various ideas
  - Set up a “local” intelligence (maybe a laptop)
    - This is called a “privacy mediator”
  - The local intelligence can add noise to the data, blur pictures, etc. as needed
    - Avoid sending “raw” sensor data to the cloud
    - User has control over the fidelity of data

Other Sources

- Enabling Things to Talk and the IoT Architecture Project: available at http://www.iot-a.eu
- S. Ray, A. Raychowdhury, Y. Jin, “The Changing Computing Paradigm with Internet of Things: A Tutorial Introduction,” *IEEE Design and Test*, March/April 2016
- J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” *Elsevier Future Generation Computer Systems*, Vol. 29, pp. 1645-1660, 2013
- J. Bughin, M. Chui, J. Manyika, “An Executive's Guide to the Internet of Things,” *McKinsey Quarterly*, August 2015

http://www.arm.com/products/security-on-arm/trustzone



Recent trends

- Forrester 2017 prediction
  - “Hackers will continue to use IoT devices to promulgate DDoS attacks”
- ARM puts security into its chips through its TrustZone technology
  - Secure and not software/data are hardware separated
- Akamai state of the internet report has started highlighting IoT related attacks
  - Example of Spike DDoS toolkit targeting Linux on ARM chips
- Calls for standardizing IoT security