Security and the Internet of Things

Prashant Krishnamurthy

Department of Informatics and Networked Systems

School of Computing and Information

University of Pittsburgh

About

- Faculty member in the School of Computing and Information
  - Department of Informatics and **Networked Systems**
  - Part of **LERSAIS** – Pitt's Laboratory for Education and Research in Security Assured Information Systems
  - Part of Prof. Joshi's team for **SAC-PA**
- Teaching
  - Cryptography, Network Security, Wireless Networks, and now **IoT**
- Research
  - Wireless networks, localization, and security

Past Related Research

- Efficiency of cryptographic algorithms/protocols
  - When you perform per packet stateless encryption, the “best” encryption algorithm depends on the length of the packet
- Security in multi-hop sensor and ad hoc networks
  - Part of an ARL multi-university research project
- Jamming and key establishment in sensor networks

Thoughts

- Information security needs to be pervasive and coordinated
- There are many moving parts
- Need to have a 1000 foot understanding for all security professionals as to how the parts fit and how one may impact the other
- IoT is a good example of need to understand the “system” and the moving parts

Thoughts (2)

- IoT is coming, if it has not already arrived
- As consumer/business adoption increases, it gets into the scientific/research community as well
  - The new cyberinfrastructure?
- Data credence and integrity
  - (Trusted and Reproducible Science)
- IoT Track
  - Professional Masters programs at Pitt

Agenda

- Quick overview of IoT
- Security in IoT
- Efforts at LERSAIS
  - Data credence in IoT

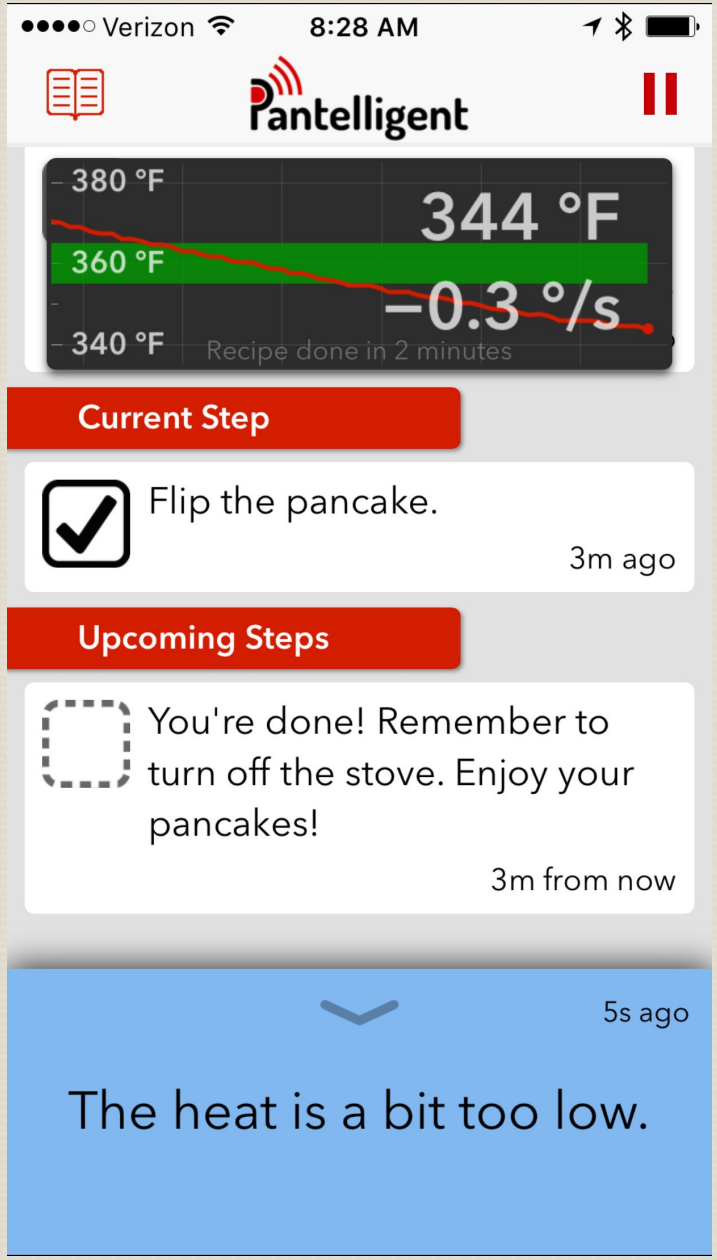
IoT Everywhere

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

All critical infrastructure sectors

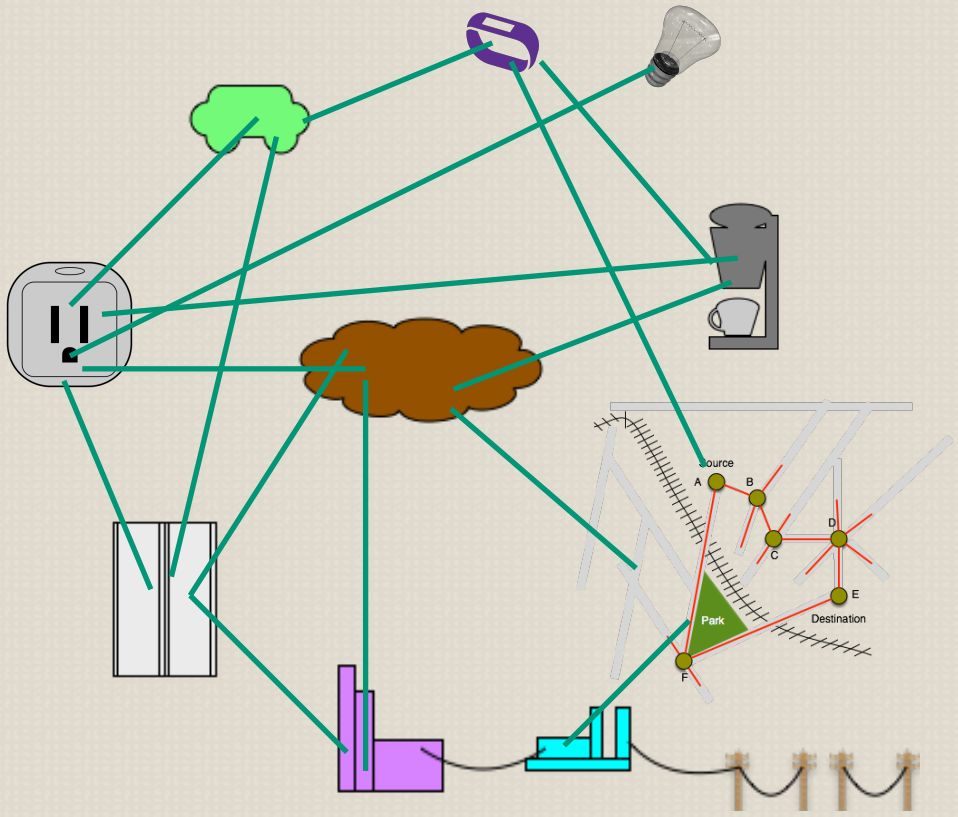
What is a thing?

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

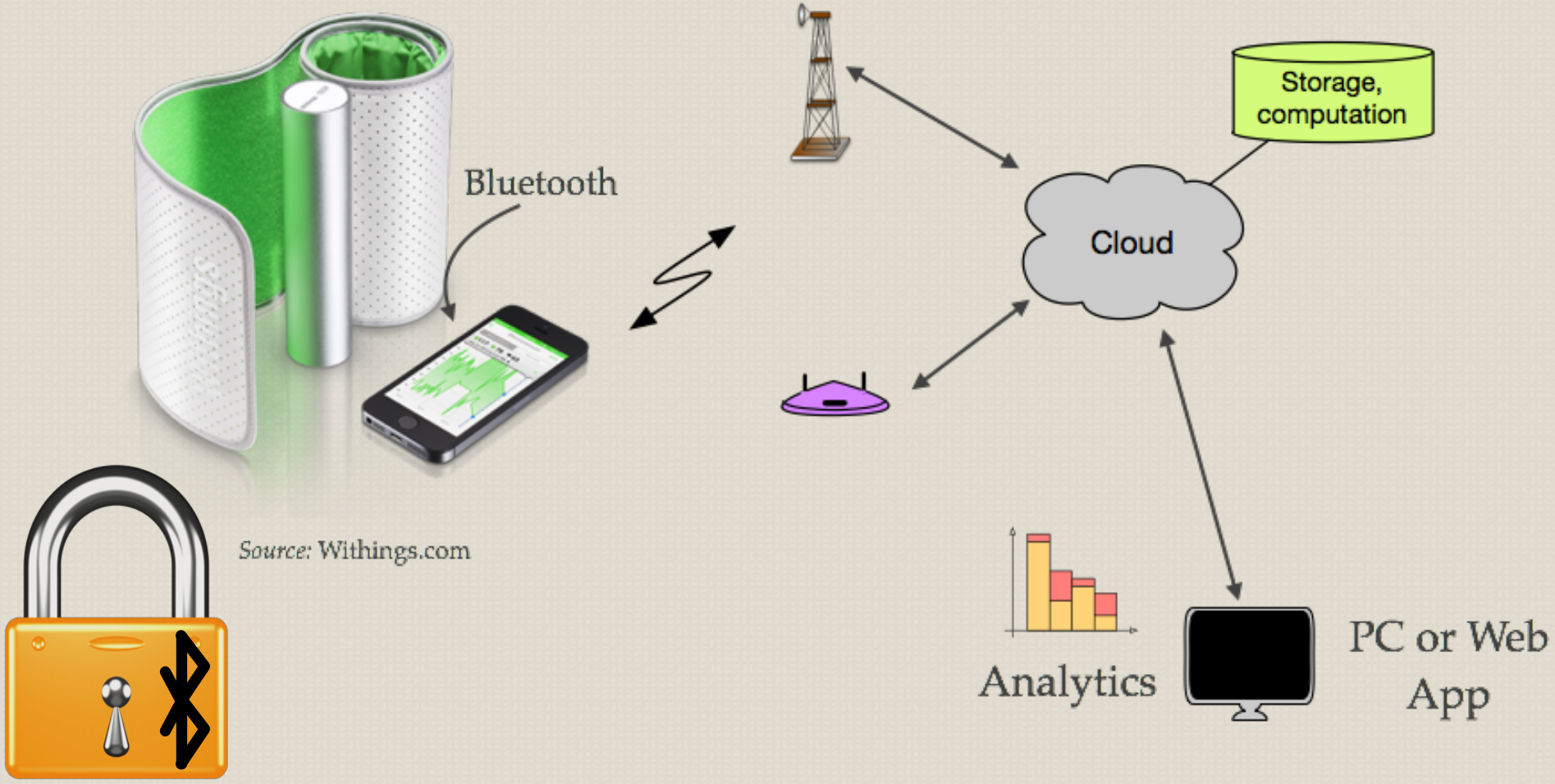


What is the “Internet of Things?”

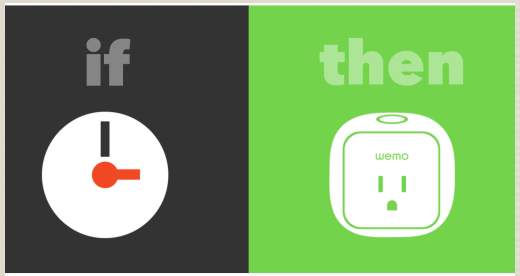
- Every “thing" has an IP address
  - Maybe or maybe not?
- IoT =? Smart Environment
  - Smart cities
  - Smart grid
  - Smart health
  - Connected life



Example (1)


Bluetooth
Storage, computation
Cloud
Analytics
PC or Web App
Source: Withings.com

Example (2)



Enjoy a freshly brewed pot of coffee when you wake up

Amazon Echo

Source: Amazon.com

Storage, computation

Cloud

WiFi Router

Belkin WeMo

Source: belkin.com

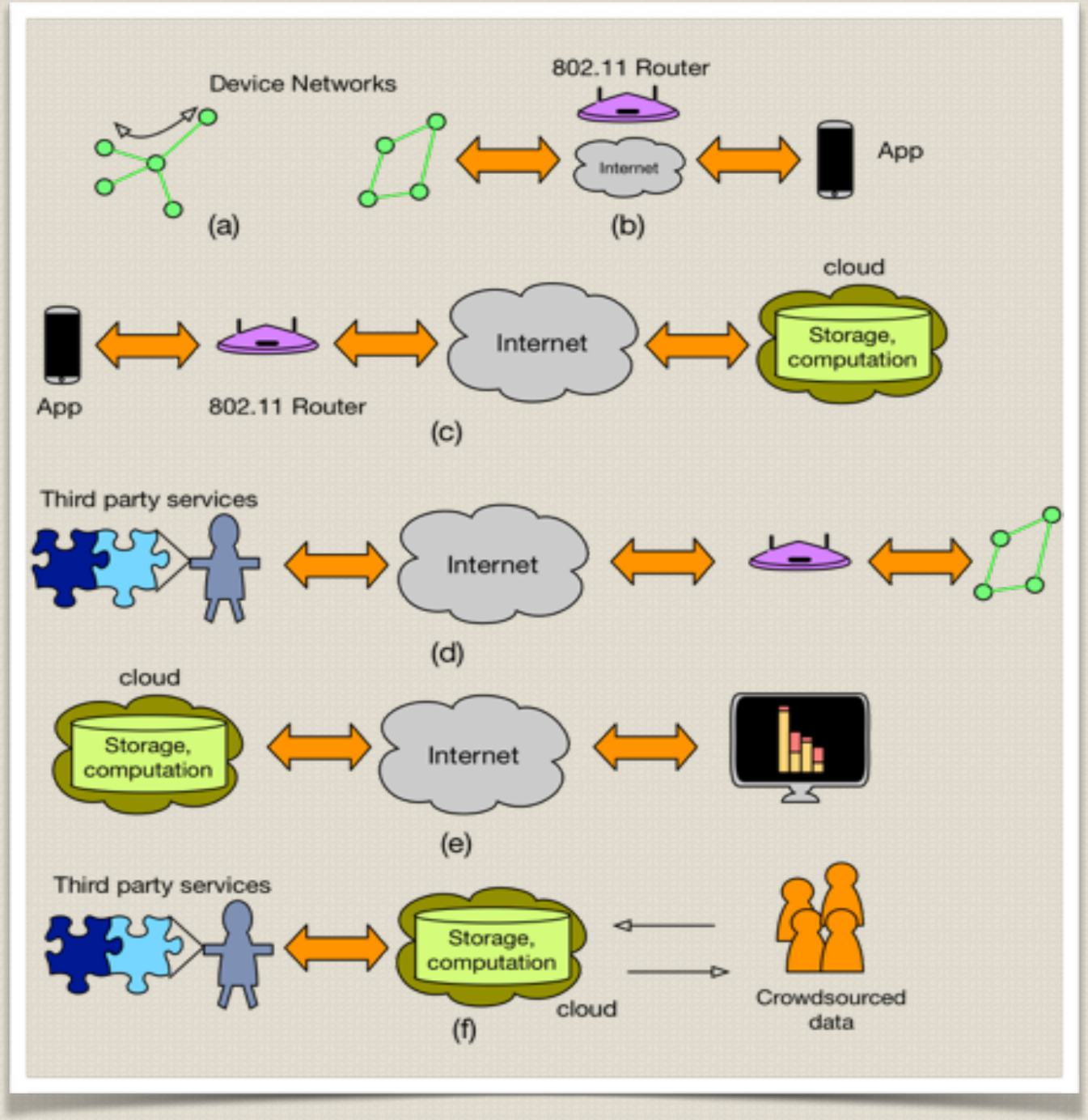
Analytics

Smartphone App

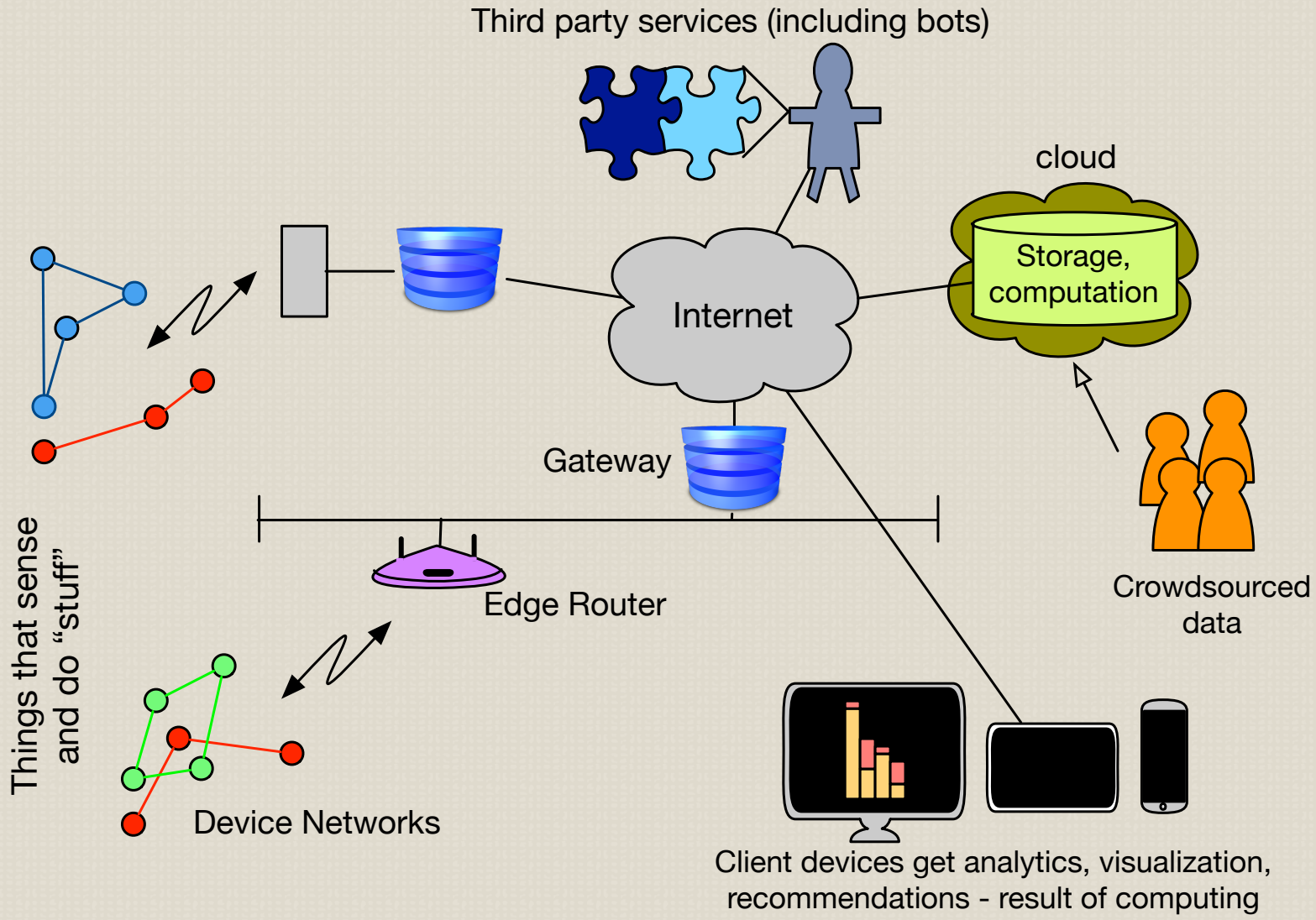
PC or Web App

Six Pathways

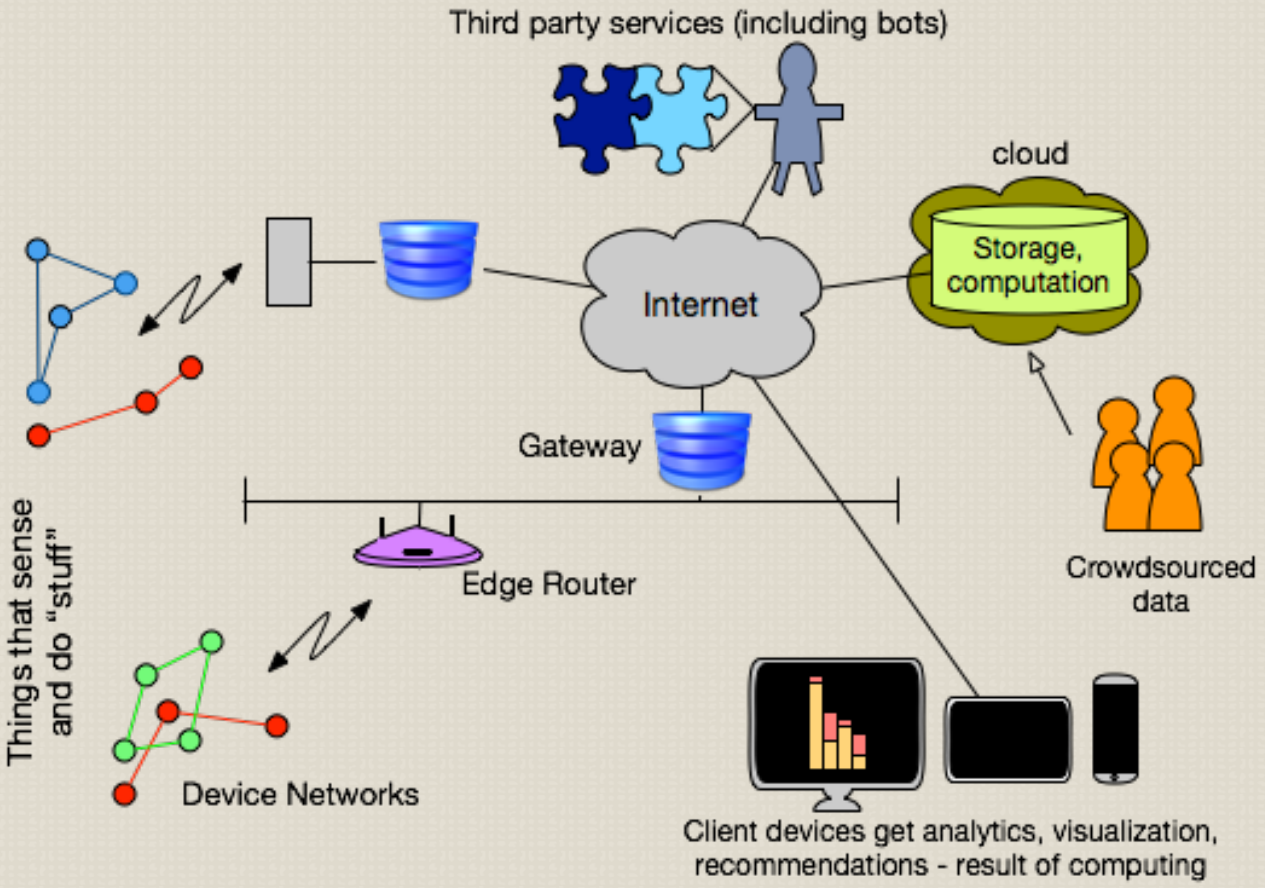
- Device Network
- App & Things (Devices)
- App & Cloud
- Device and Third-Party Services
- Analytics and Presentation
- Third-Party Services



Summary: High-Level Architecture

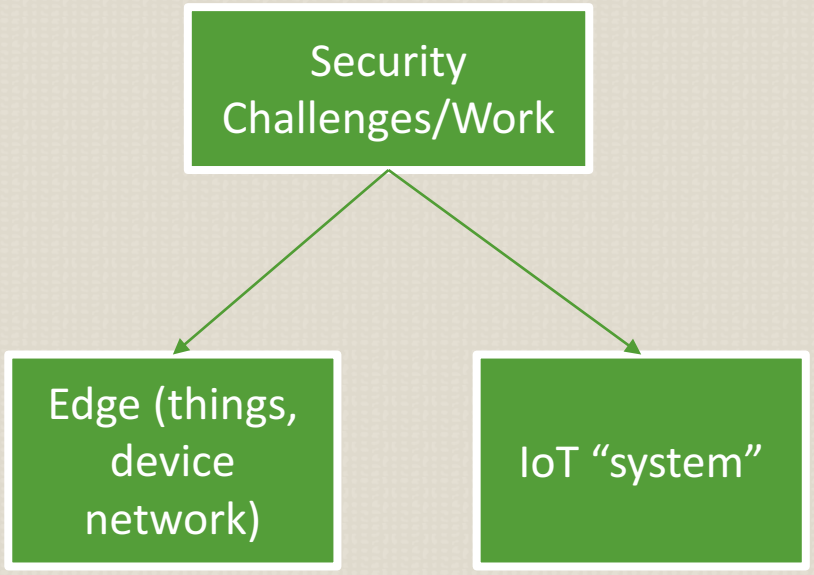


Security Threats at a High Level



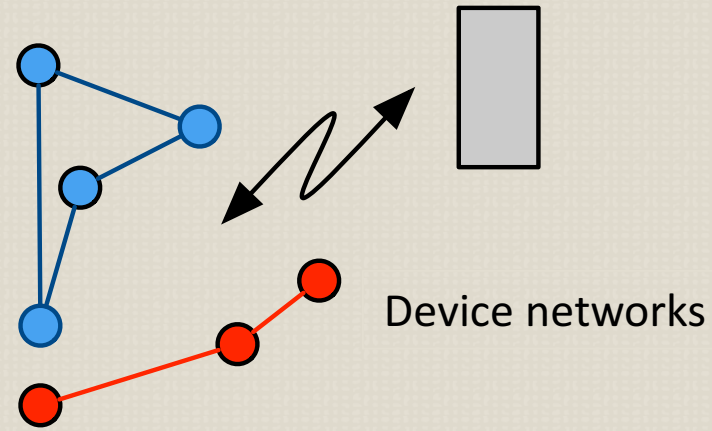
So…

- 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



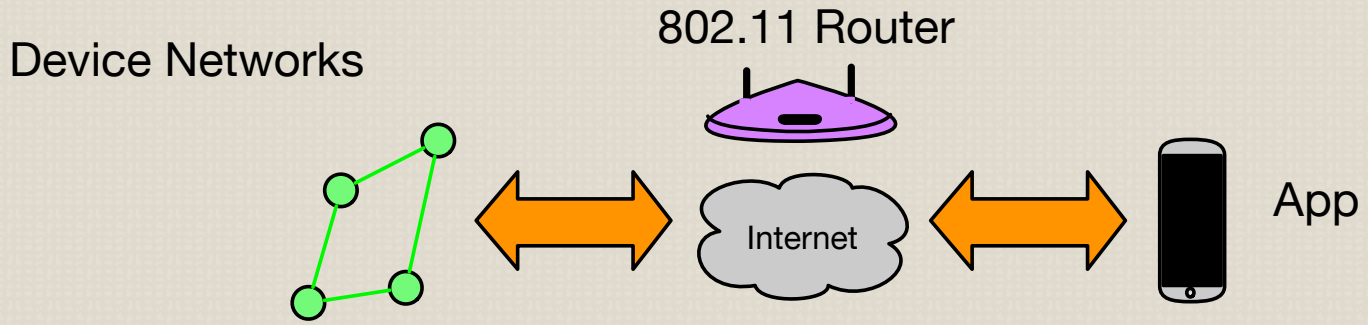
Predominant focus on edge

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



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

HomeKit

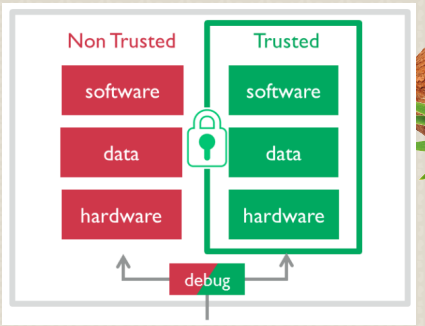


- Restrictive
  - Device has to generate new keys if factory reset
  - Uses Apple Coprocessor
  - Needs Bluetooth or WiFi connectivity between iOS device and Homekit accessory (thing)
- Device has a public key/private key pair, as also the iOS device
  - User has to enter an 8-digit code by device vendor
  - Use SHA-512 with something like HMAC to generate keys
- Communications use the ChaCha stream cipher (more efficient than AES) with authentication/integrity

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?

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



Recent trends

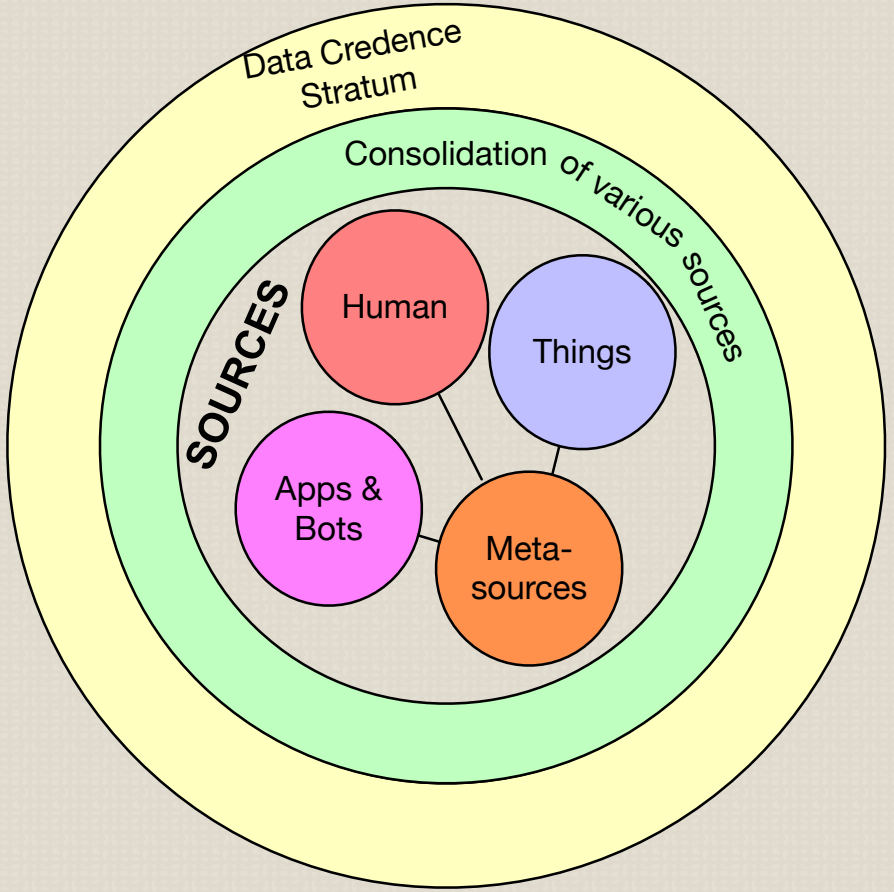
- Forrester 2017 prediction
  - “Hackers will continue to use IoT devices to promulgate DDoS attacks”
- ARM puts security into its chips through its TrustZone technology
  - Secure and not software/data are hardware separated
- Akamai state of the internet report has started highlighting IoT related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

Efforts at LERSAIS

- Fall 2018
  - Special topics class in IoT
  - Two weeks dedicated to security issues
- Research directions
  - How can we exploit multiple-link layer technologies in “things” for enhancing security?
  - How can we best use energy harvesting in “things” to improve the tradeoffs between security and performance?

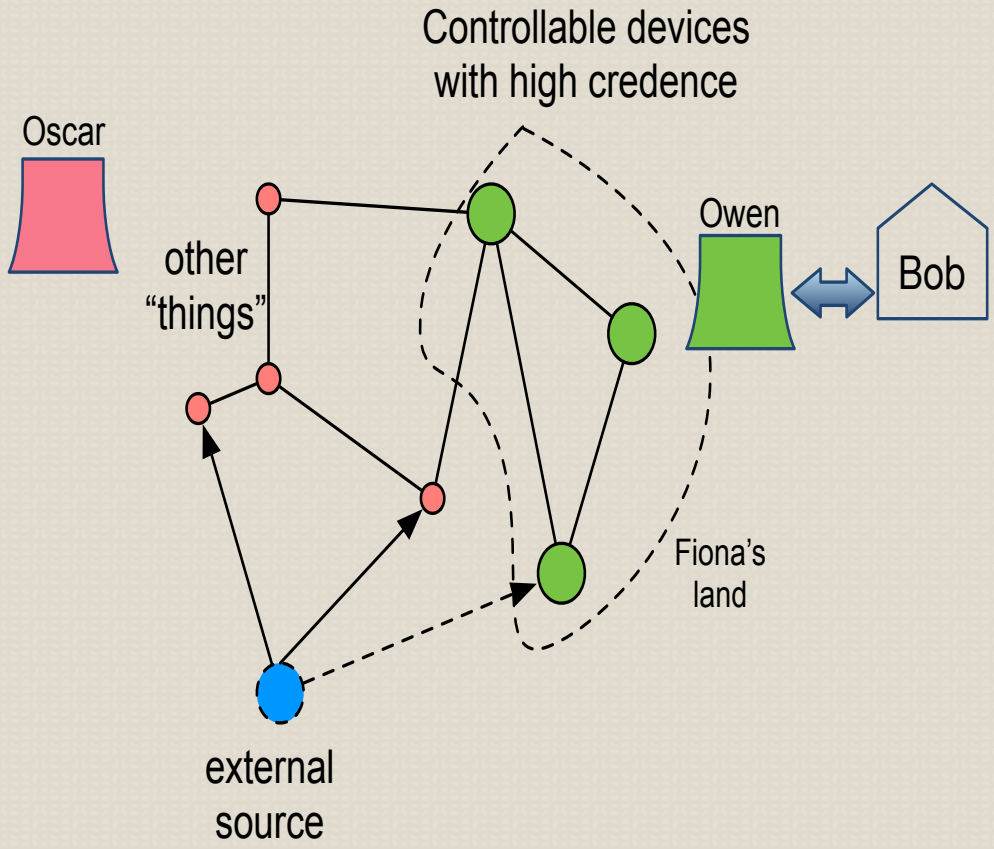
Data Credence and IoT

- Work with Dr. Vladimir Zadorozhny
- Typical IoT scenarios
  - Variety of heterogeneous data sources
  - Trusted or not, granularity/gaps in space/time, semantics, scope, etc.
- Probabilistic “confidence” in data



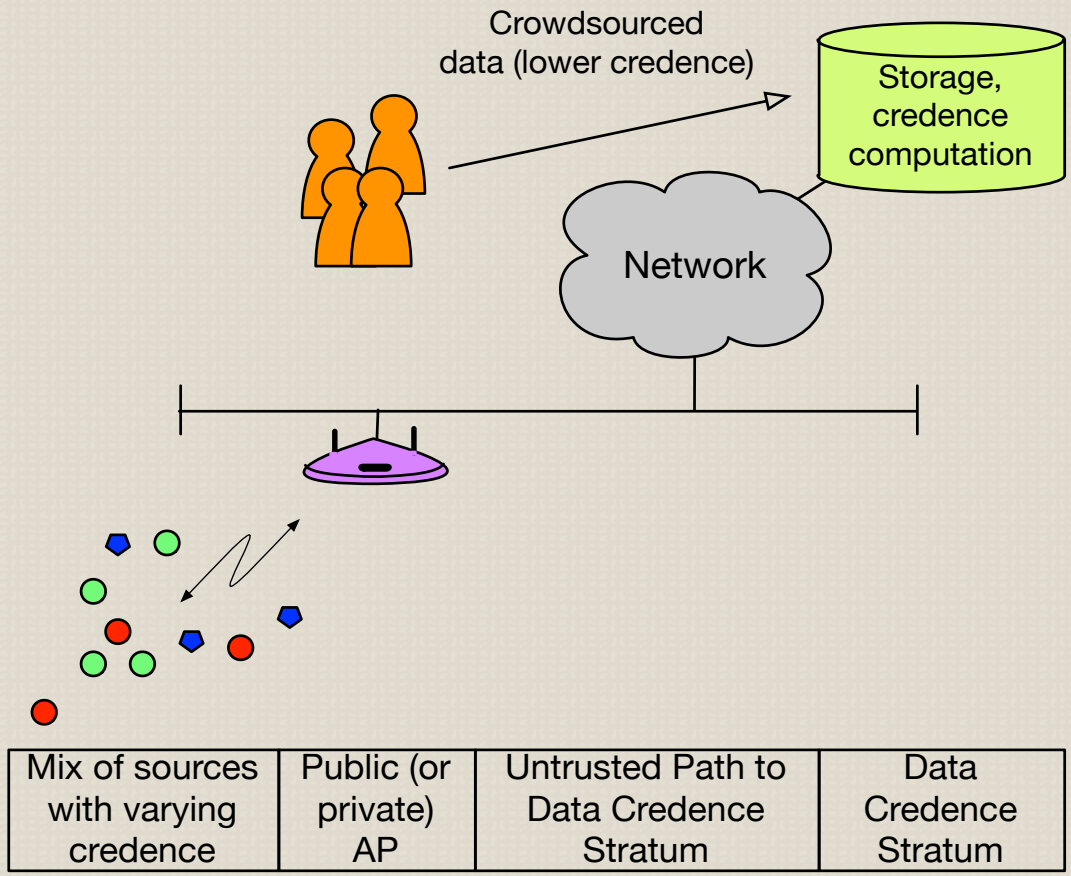
Working Example

- Banking
  - Farmer Fiona takes a loan
  - Collateral – crops
- Sensors to monitor land, moisture, crop growth
  - Should we approve second round or foreclose on land?
- Many data sources
  - Green = trusted
  - Red = untrusted
  - Blue = external “macro”



How can we develop a model for the "credence" of data?

- One approach
  - Subjective logic + graphs (like page rank)
  - Tuple with "opinions" that iteratively improve
- Role of crypto
  - Tuning credence
  - Tradeoffs with efficiency



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

"Your next car will need a firewall."

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

“The bank at the middle of an attempted $950m cyber heist didn’t even have a firewall”

– Title of article by Ben Woods, The Next Web, April 21, 2016

Thank You!

If you have time and interest, please see:
goo.gl/Crifhd