Internet of Things

CS @CU

What is the “Internet of Things”?

OED A proposed development of the internet in which many everyday objects are embedded with microchips giving them network connectivity, allowing them to send and receive data.

Merriam-Webster The networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet.

Wikipedia A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Me Non-computer objects that both contain a CPU and can communicate over a wide-area network.

CS@CU

Excluded

- Devices with only a CPU, e.g., my toaster and coffeemaker
- Devices with only local networking, e.g., RF remote controls for ceiling fans
- Special-purpose CPUs embedded in larger, networked objects or computers, e.g., USB flash drives, Apple's Lightning connectors, laptop cameras, keyboards, etc.
- Must distinguish IoT from *embedded systems*

What Are Some IoT Devices?

- Roombas
- Smart thermostats
- Amazon's "Ring" doorbell
- Smart electric meters
- Many newer cars
- Some medical devices

Cars are Mobile Data Centers

- A modern car has (at least) 50–75 CPUs
- These are networked together via a CAN Bus
- Many cars also have cellular links for driver assistance, e.g., GM's OnStar and the like
  - My car will light a dashboard indicator for possible icy roads, which means that a) there's cellular connectivity to the manufacturer, and b) the manufacturer has some notion of my location
  - I declined to pay for their optional connected package, but some of it is there anyway…

Attributes of IoT Devices

- Not a computer, and hence often lacks conventional I/O devices: a screen, a keyboard, a mouse or touchscreen, etc.
- Users generally cannot reprogram them
- Generally cannot run outside software (though that may change)
- By definition, connected to a physical device

Resetting a GE Smart Light

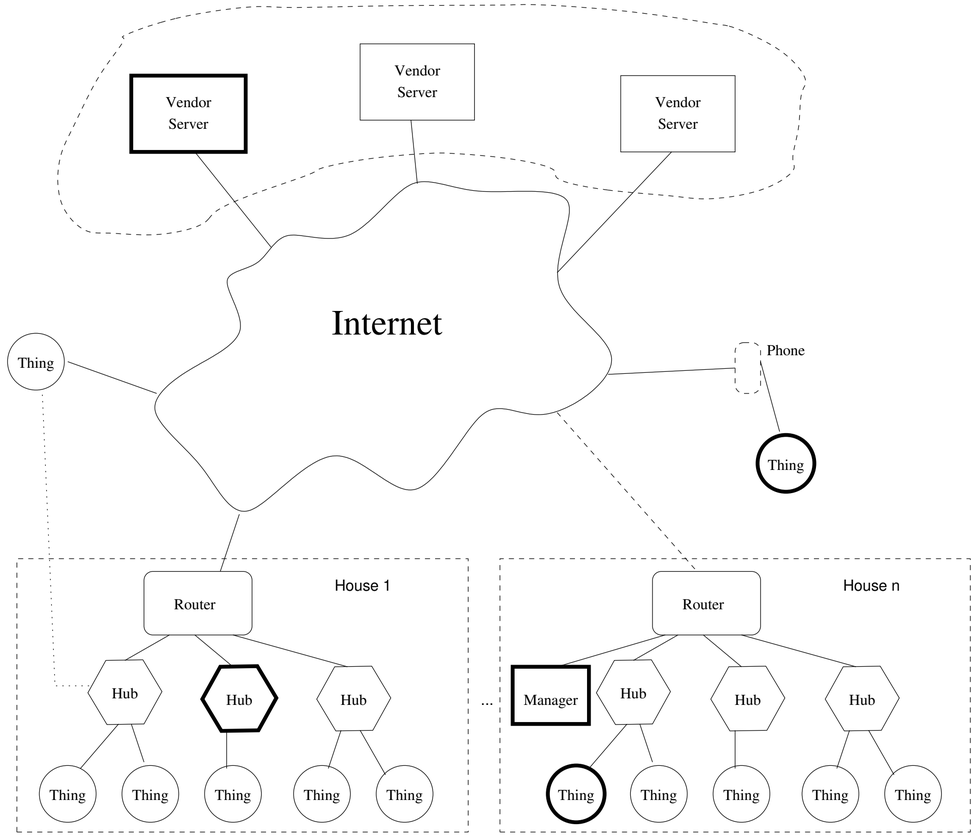
https://www.youtube.com/watch?v=u6NJQ4FeMpA&feature=youtu.be

The Data

- What data is collected?
- Where does it go?
- Who owns it?
- What is done with it?

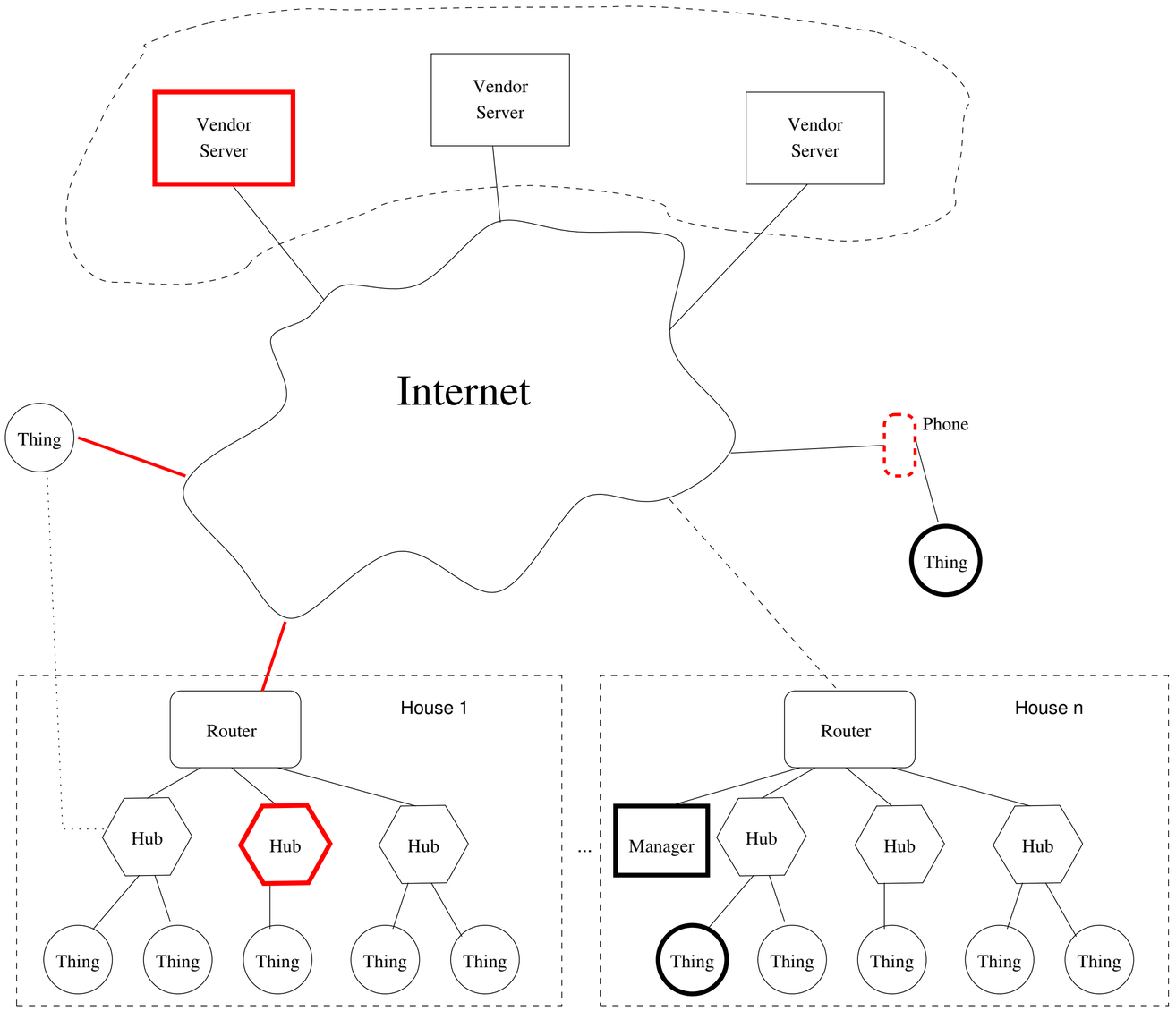
Remember the definition of privacy (RFC 4949): “The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.”

Typical IoT Architecture



Important Elements

- There's generally a vendor-operated Server
  - There often needs to be some sort of authentication to it
- Things that talk to the server directly have an IP address (or phone number)
- Hubs are on the local network
- Phones have vendor-supplied apps



Data

The vendor knows:

- Your login (often an email address or linked to it)
- Everything your Thing does and/or senses
- Your IP address and/or your phone number
- Other devices on your local net
- Whatever your phone lets it learn

(Why a Vendor Server?)

- It's hard to talk directly to consumer devices; they're almost always behind NATs and usually don't have stable IPv6 addresses
- Battery-operated devices can't be online 100% of the time, but they can poll the vendor at reasonable intervals
- Usability is a problem: most consumers would have trouble learning an IP address and setting up a DNS entry for each of their devices
- The usual solution: consumers talk to their devices indirectly, via the vendor

In Other Words…

- The vendor generally *must* be in the loop
- The vendor *could* provide relaying of end-to-end encrypted messages
- But why bother, when it's more profitable to collect data…?

Data Collected

- Logs when, where, how long you use your TV
- Facial recognition camera (on iPhones, the data stays local)
- Voice command: “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party”
- Hackers can retrieve all of that data from the TV
- Vizio explicitly sells TV viewing habits

Samsung's Privacy Policy

(From https://www.samsung.com/us/account/privacy-policy/, 1/30/2021)

- "your device, including MAC address, IP address, log information, device model, hardware model, IMEI number, serial number, subscription information, device settings, connections to other devices, mobile network operator, web browser characteristics, app usage information, sales code, access code, current software version, MNC, subscription information and randomized, non-persistent and resettable device identifiers, such as Personalized Service ID (or PSID), and advertising IDs, including Google Ad ID"
- "your use of third-party websites, apps and features that are connected to certain Services"
- "recordings of your voice when you use voice commands to control a Service"
- "We may obtain certain information about you from publicly or commercially-available sources"
- "information you store on your device, such as photos, contacts, text logs, touch interactions, settings and calendar information"

Information Sharing

- “We may share your personal information with our subsidiaries and affiliates and with service providers who perform services for us. We do not authorize our service providers to use or disclose the information except as necessary to perform services on our behalf or to comply with legal requirements. In addition, we may share your personal information with our business partners, such as wireless carriers, as well as third parties who operate apps and services that connect with certain of the Services.
- “… We also may disclose information about you in other circumstances, including:
  - “to law enforcement authorities, government or public agencies or officials, regulators, and/or any other person or entity with appropriate legal authority or justification for receipt of such information, **if required or permitted to do so by law or legal process**;
  - “when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss, or **in connection with an investigation of suspected or actual fraudulent or illegal activity**; or
  - “in the event we may or do sell or transfer all or a portion of our business or assets (including **in the event of a merger, acquisition, joint venture, reorganization, divestiture, dissolution or liquidation**).

Voice-Controlled Devices

- Many devices—Amazon Echo (“Alexa”), Apple HomePod, Google Home, devices with Apple’s Siri or Microsoft’s Cortana—listen for “wake-up” words
- Are they listening at other times?
  - Amazon Guard Plus: “If Alexa detects sounds that could be an intruder while you're away from home… she can send you a Smart Alert mobile notification
  - “From a Smart Alert, you can play back what Alexa heard”
- Can law enforcement (with a warrant) convert that into a bug? (They’ve tried in analogous situations.) What about Siri, Cortana, etc.?

The Company v. the United States

349 F.3d 1132 (CA9, 2003)

- A car used by a suspect had a cellular-connected “Help” feature
- The government wanted the manufacturer to surreptitiously turn on the microphone, to eavesdrop on conversations in the car
- The 9th Circuit said “No”—but only because that would have disabled the help function, and the wiretap law requires "a minimum of interference with the *services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted*.” (Emphasis added by the court)

Car Data

- All recent cars have “black boxes” that record all sorts of driving data
- Data that must be recorded, per Federal regulations, includes “pre-crash speed, engine throttle, brake use, measured changes in forward velocity (Delta-V), driver safety belt use, airbag warning lamp status and airbag deployment times.”
- Who owns it?
  - “Any data retained by an event data recorder… is the property of the owner”
  - “Data recorded or transmitted by an event data recorder… may not be accessed… unless
  - “(1) a court or other judicial or administrative authority having jurisdiction—
  - “(A) authorizes the retrieval of the data
  - (Driver Privacy Act of 2015, 49 U.S.C. §30101)
- But—Fourth Amendment issues not entirely clear

Fitness Trackers

- Fitness trackers record things like heart rate; some record location
- Sites like Strava encourage you to upload such data
- This can be used to track people—and even to locate secret military bases
- Fitness tracker data has been used for both inculpatory and exculpatory evidence
- What legal process is needed to access this? Is it a third party doctrine issue?

More Things

Roombas collect “information about the spaces where you use your Robot, such as floorplans, types of objects (detected using the camera on your Robot)… the location and confidence factor of Wi-Fi devices connected to your local network, and Wi-Fi heat maps. (Note that Amazon is trying to buy Roomba)

Gunshot Detectors can sometimes pick up **street conversations**

Autonomous cars constantly “see” their environment

Medical devices record lots of sensitive information

Connected Sex toys — need I say more?

Broader Privacy Issues

- There's no one answer to the privacy issues—it all depends on what data is being recorded
- Legal issues may vary for government data collection versus private company collection
- Fourth Amendment issues may turn on what is revealed about what is happening inside the house or other privacy-protected area

Daily Bird

Cooper's Hawk, Morningside Park, January 30, 2021

CS@CU