A RIOT OF OPPORTUNITY: INTEGRATING REAL-TIME DATA INTO THE INTERNET OF THINGS

Henning Schulzrinne

(+ Jan Janak & other CUCS IRT contributors)

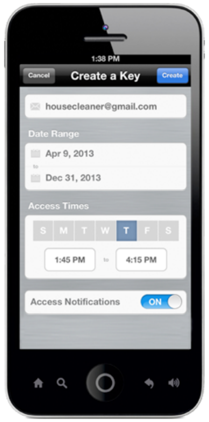
RTC 2016

Natural evolution

Insert face up or slide keycard as illustrated. Turn handle after green light appears.

キーカードは図面のように表側を差し込むか又は上から下へおろしてください。グリーンのライトを確認し、ドアのとってをまわしてください。

OHANA
HOTELS AND RESORTS
OHANAHOTELS.COM
800-462-6262



1:38 PM

Cancel | Create a Key | Create

housecleaner@gmail.com

Date Range

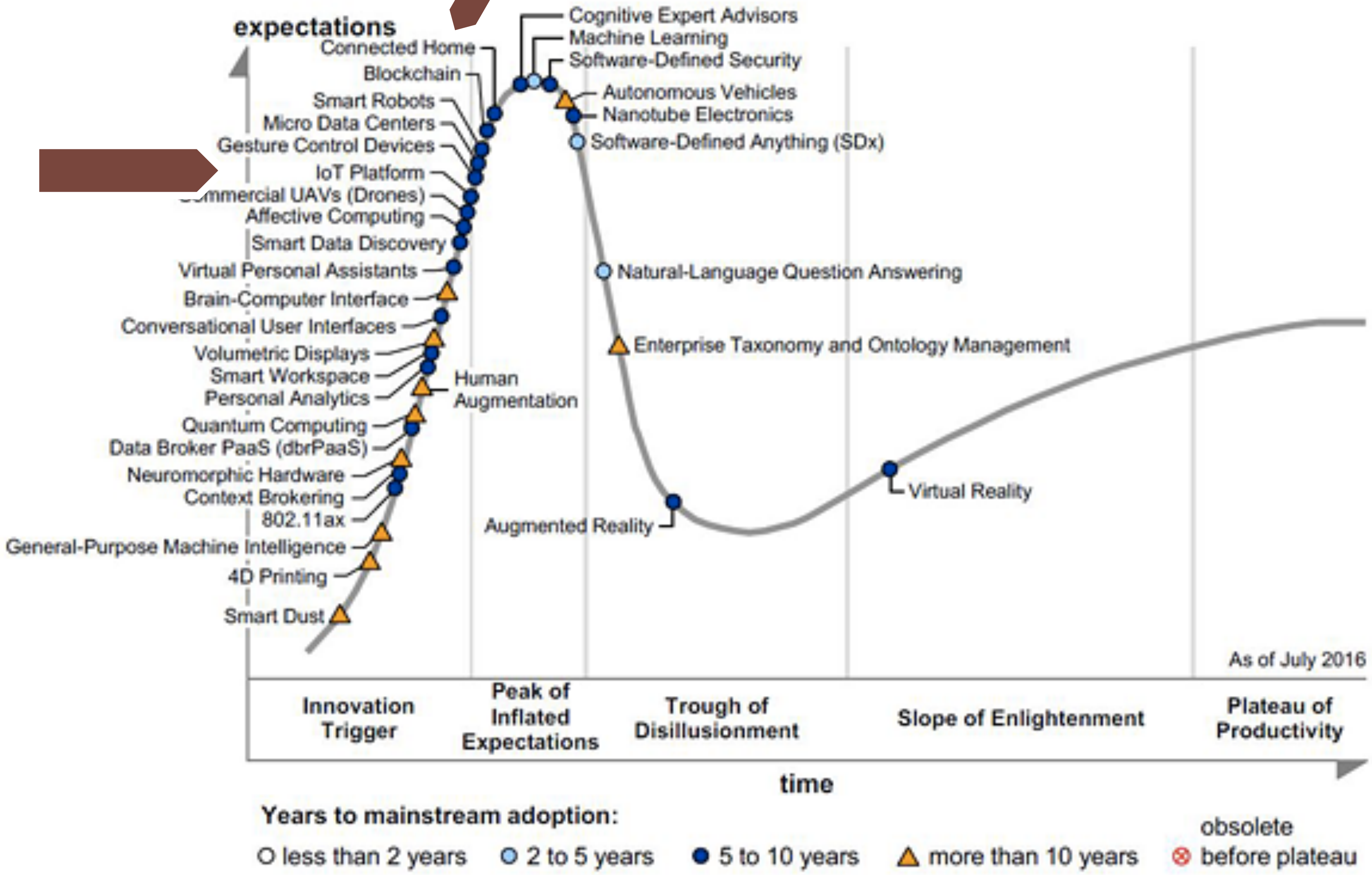
Apr 9, 2013
to
Dec 31, 2013

Access Times

S M T W T F S

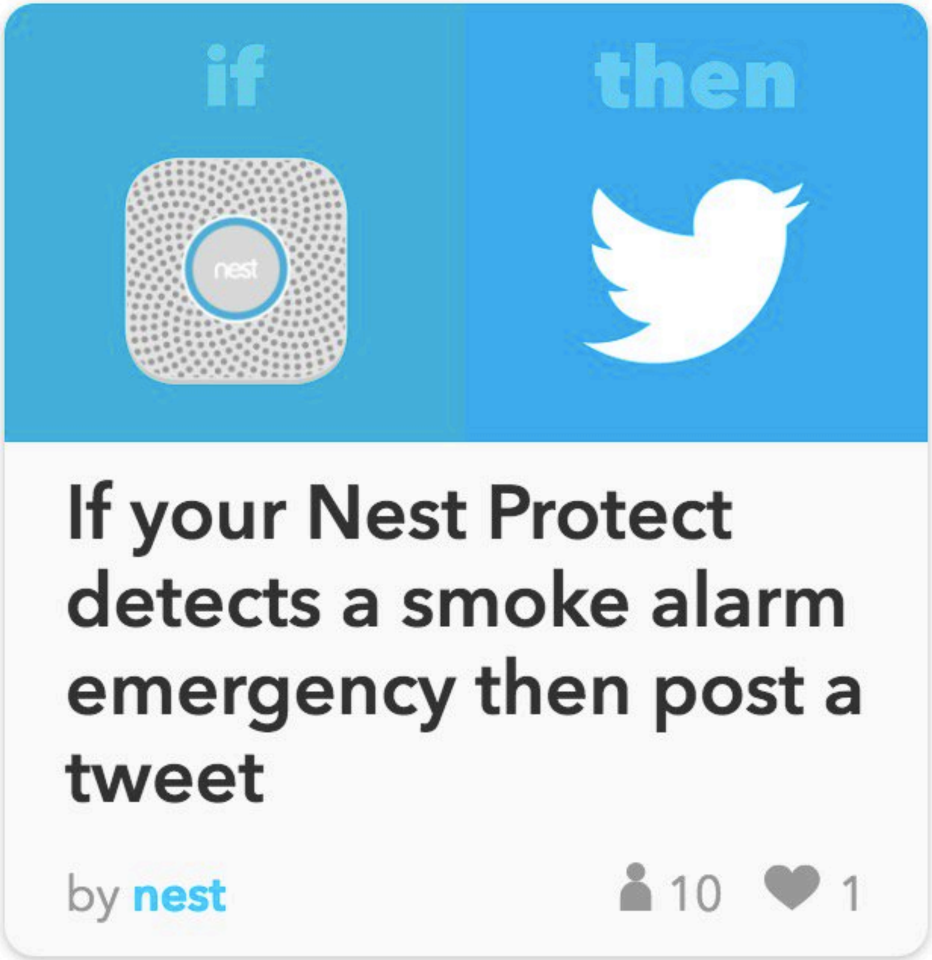
1:45 PM to 4:15 PM

Access Notifications ON



Source: Gartner (July 2016)

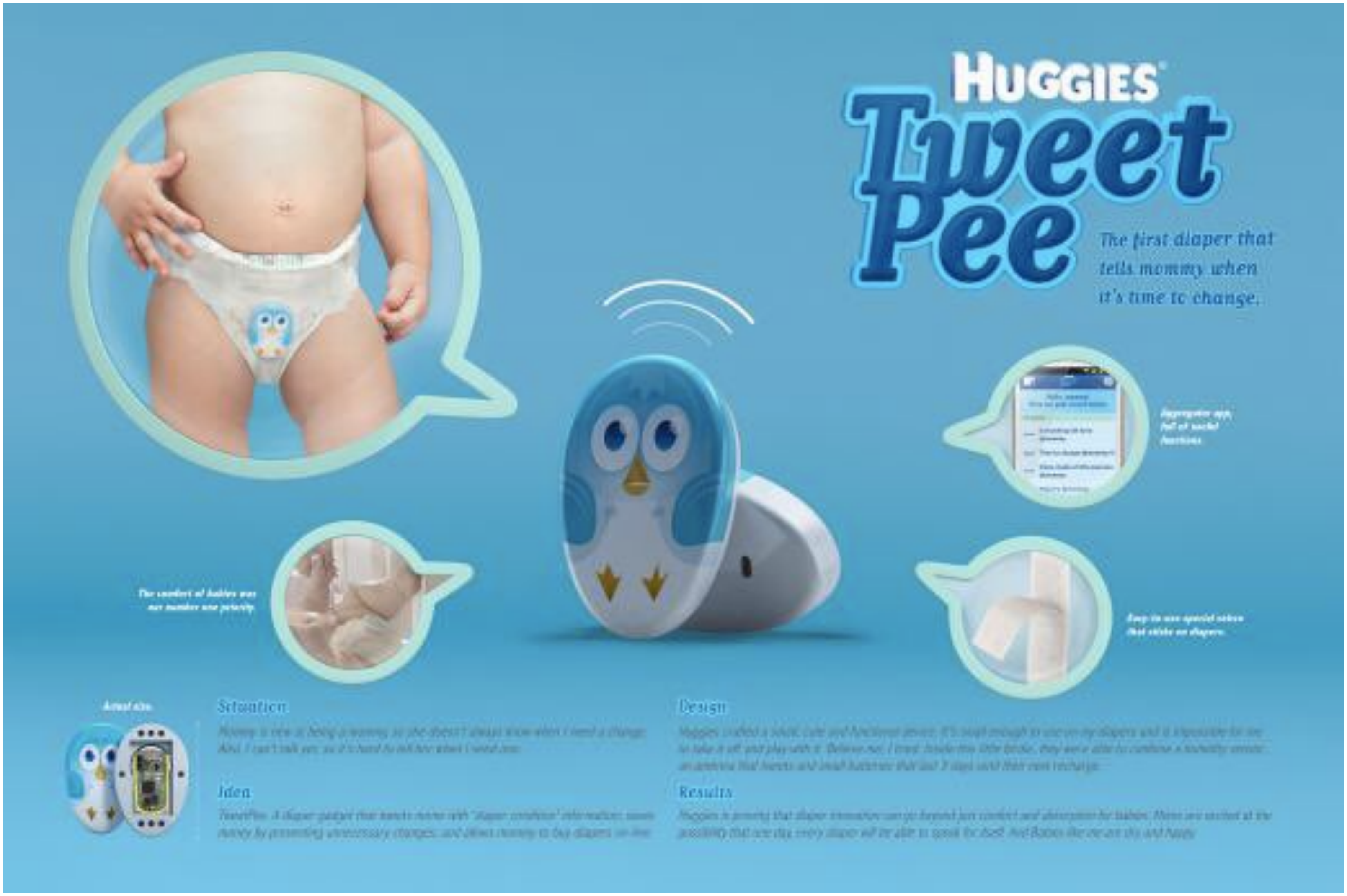
Kids, don't do this at home



If your Nest Protect detects a smoke alarm emergency then post a tweet

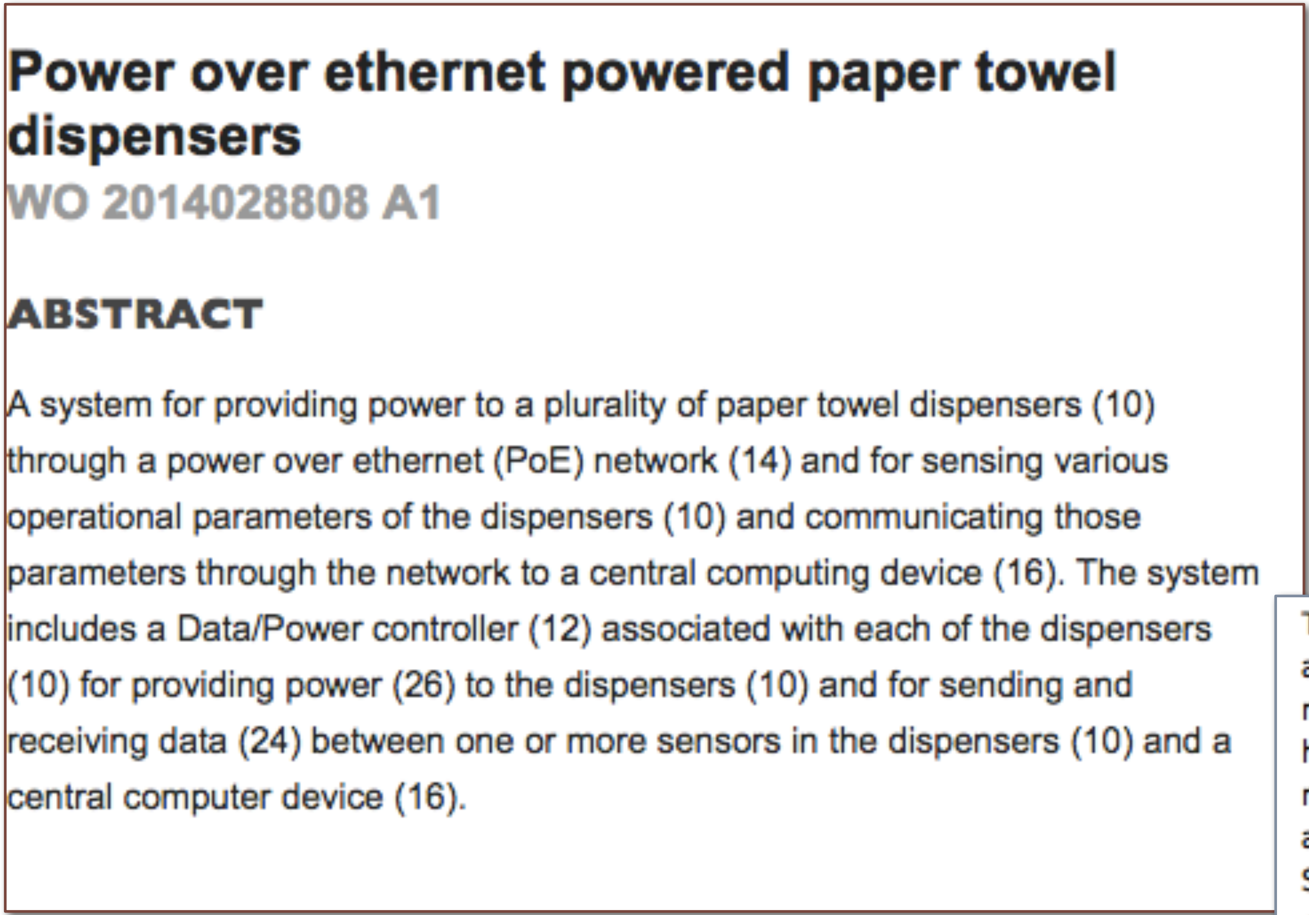
by nest

10 1


HUGGIES
Tweet Pee
The first diaper that tells mommy when it's time to change.
Aggregator app, full of social functions.
The comfort of babies was our number one priority.
Easy-to-use special velcro that sticks on diapers.
Actual size.
Situation
Mommy is new at being a mommy so she doesn't always know when I need a change. And, I can't talk yet, so it's hard to tell her when I need one.
Idea
TweetPee. A diaper gadget that tweets mommy with "diaper condition" information, saves money by preventing unnecessary changes, and allows mommy to buy diapers on-line.
Design
Huggies crafted a small, cute and functional device. It's small enough to use on my diapers and it is impossible for me to take it off and play with it. Believe me, I tried. Inside this little birdie, they were able to combine a humidity sensor, an antenna that tweets and small batteries that last 3 days until their next recharge.
Results
Huggies is proving that diaper innovation can go beyond just comfort and absorption for babies. Moms are excited at the possibility that one day every diaper will be able to speak for itself. And Babies like me are dry and happy.

https://twitter.com/internetofshit

Towel dispensers



Power over ethernet powered paper towel dispensers

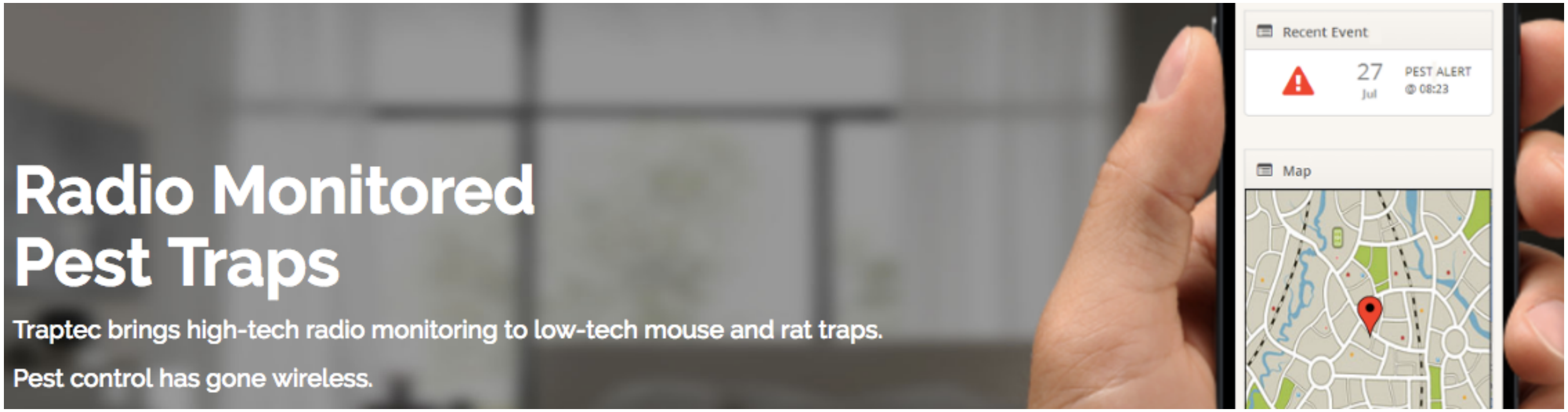
WO 2014028808 A1

ABSTRACT

A system for providing power to a plurality of paper towel dispensers (10) through a power over ethernet (PoE) network (14) and for sensing various operational parameters of the dispensers (10) and communicating those parameters through the network to a central computing device (16). The system includes a Data/Power controller (12) associated with each of the dispensers (10) for providing power (26) to the dispensers (10) and for sending and receiving data (24) between one or more sensors in the dispensers (10) and a central computer device (16).

The IoT has already been used for a range of use cases in facilities management. For example, Coor has worked with a paper towel manufacturer in Sweden to implement automated monitoring of dispensers. Sensors fitted to each dispenser monitor its fill level, and send an alert to the building manager, who can make sure it is refilled before it becomes empty.

The IoT killer app



Radio Monitored Pest Traps

Traptec brings high-tech radio monitoring to low-tech mouse and rat traps.

Pest control has gone wireless.

http://www.traptec.eu/

Drones as part of the IoT

images

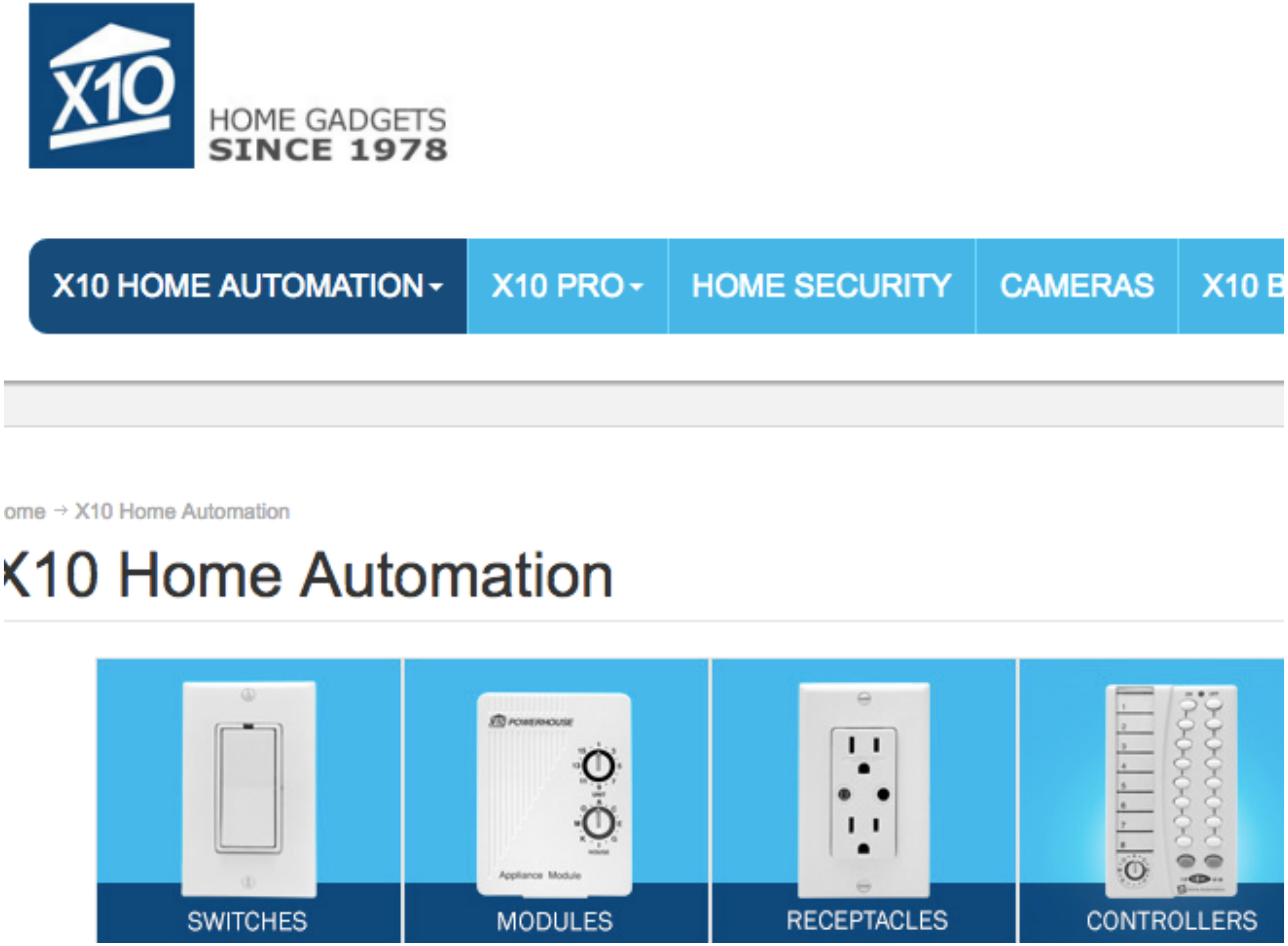
pollution

noise

link.nyc & smart trash cans

GPRS or CDMA
GPS location service

IoT is not exactly new



ome → X10 Home Automation

X10 Home Automation

But controlling light switches is still not the best use

> Want to turn on the bedroom light? Sure, just pick up your smartphone, enter the unlock code, hit your home screen, find the Hue app, and flick the virtual switch. Suddenly, the smart home has turned a one-push task into a five-click endeavor, leaving Philips in the amusing position of launching a new product, Tap, to effectively replicate the wall switches we always had.

https://techcrunch.com/2014/12/04/the-problem-with-the-internet-of-things/

Where does IoT make sense?

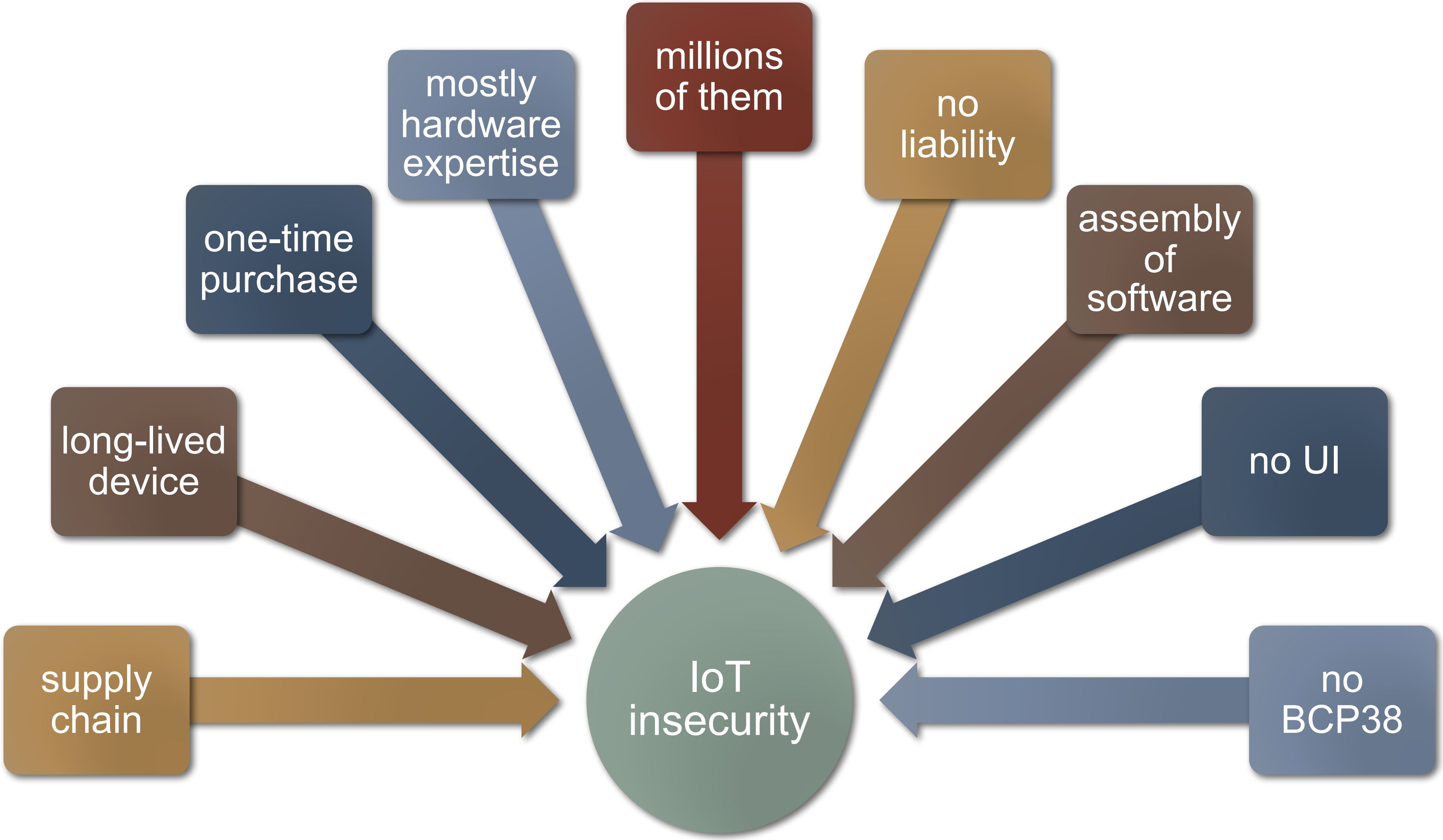
- Probably
  - home security
  - residential & commercial locks
  - home medical (recording)
  - housekeeping (restroom supplies)
  - outdoor lighting
  - parking meters
  - vending machines

- Not so much
  - light switches
  - most household appliances
  - clothing
  - smoke detectors?

not cost-effective, not just useless

SECURITY

IoT security confluence


supply chain

long-lived device

one-time purchase

mostly hardware expertise

millions of them

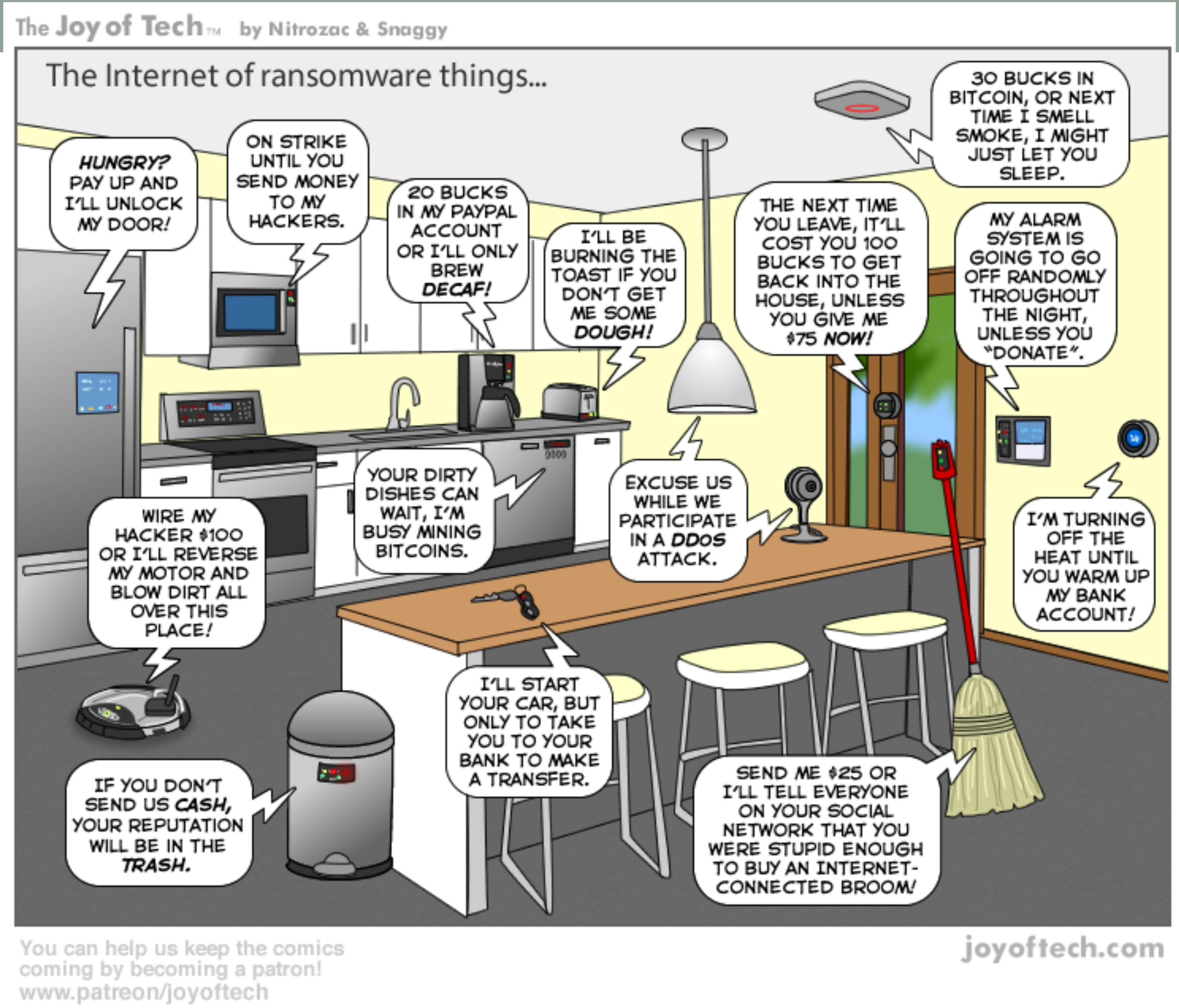
no liability

assembly of software

no UI

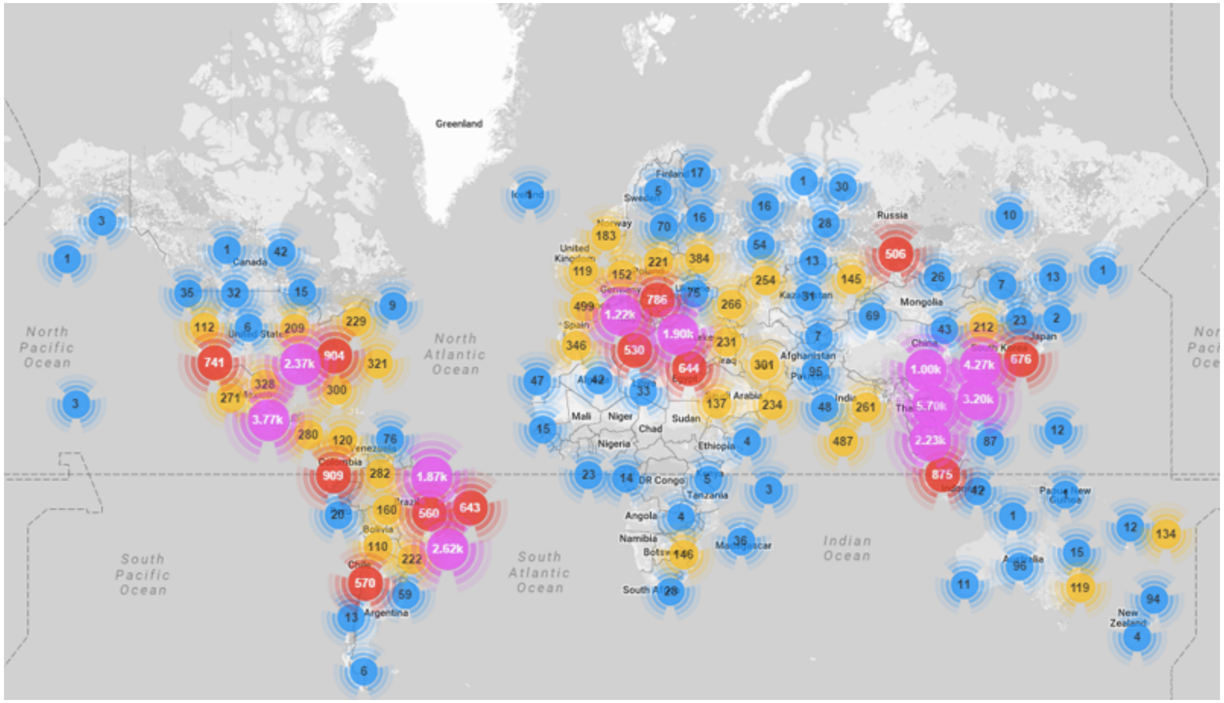
no BCP38

IoT insecurity


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

DDOS via IoT

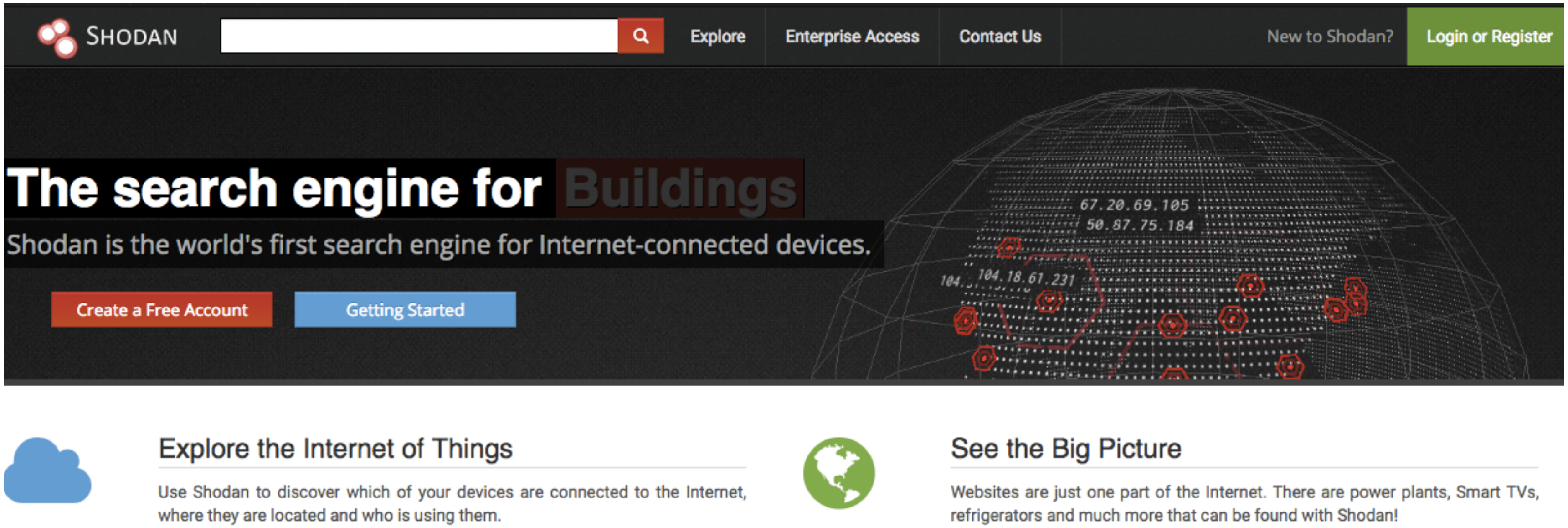
- Krebs DDOS, 9/2016: **620 Gb/s, total of > 1.5 Tb/s**
- GRE, SYN, HTTP GET, POST
- MiraiNet: “380k bots from telnet alone”
- Enabled by UPnP → bypass NATs



xc3511 vizxv
admin 888888
xmhdipc
default
123456 54321
support

Mirai botnet

- Chinese manufacturer, used by lots of OEMs
- BusyBox Linux
- Brute-force ssh and telnet
- Web reset doesn't change ssh or telnet



The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

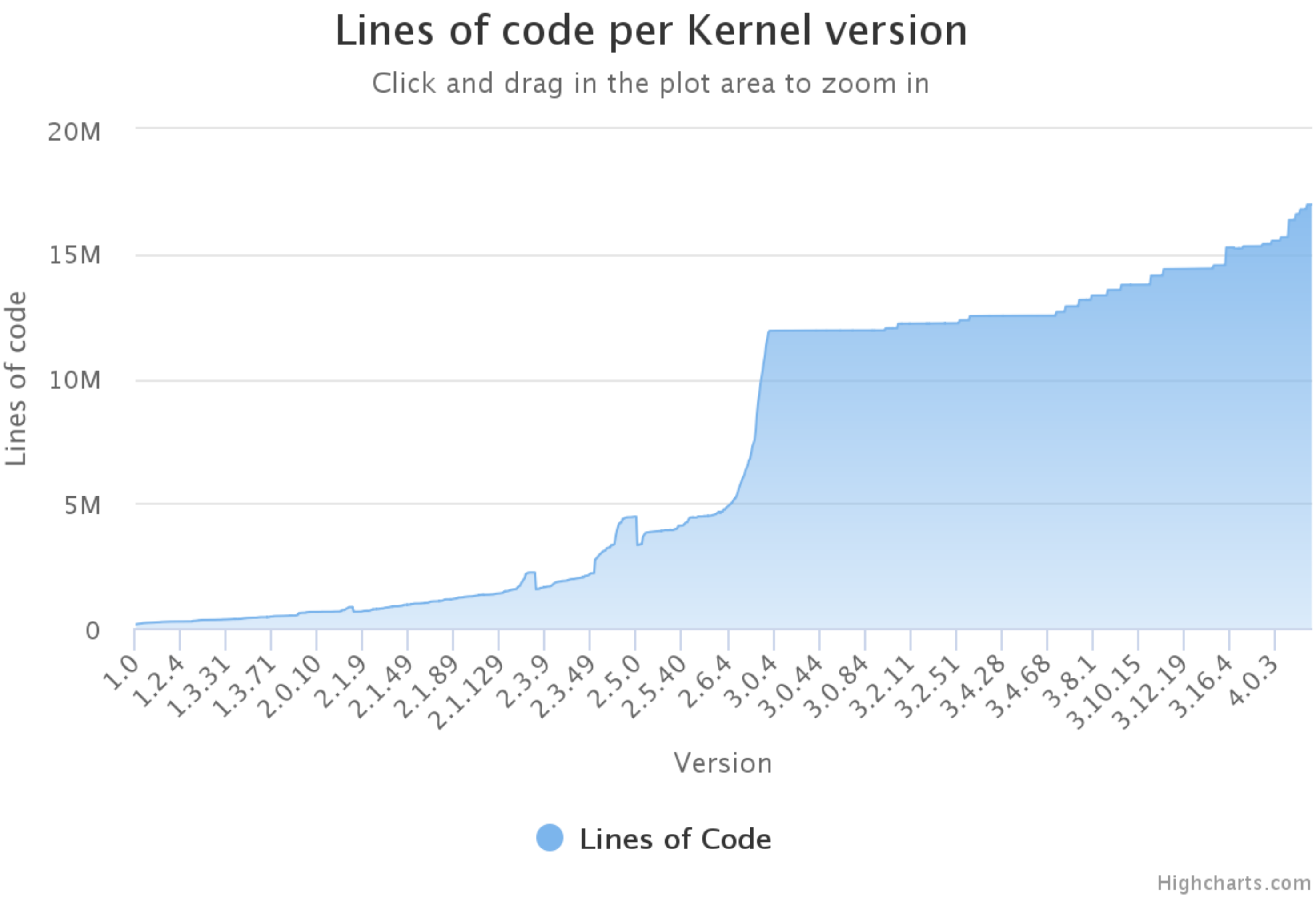
Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Linux kernel lines of code



BusyBox:
177,650 SLOC

You cannot hide

> Hackers worldwide currently probe IoT devices for vulnerabilities after they have been connected to the internet for six minutes. Each hour these devices are tested for vulnerabilities - at least 800 times per hour - with an average of 400 login attempts occurring daily. On average, hackers try to access one IoT device every five minutes and a total of 66 per cent of their attempts end up being successful.

http://www.itproportal.com/news/the-average-iot-device-is-compromised-after-being-online-for-6-minutes/

IoT DDOS economics

Schneier
Oct. 2016
Cohan
Apr. 2013

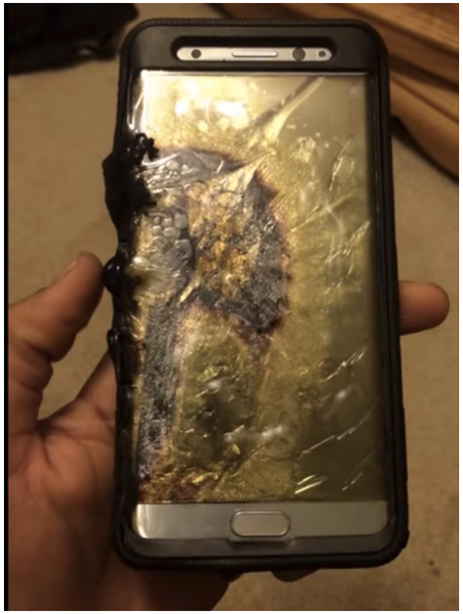
- DDOS as externality
  - device owners don’t care:
    - barely slows down their Internet service
    - device still functions normally
    - don’t know victims, generally
  - vendors don’t care (enough)
    - not liable for damage (right now) – public nuisance?
    - only marginally affects their business reputation
  - ISP don’t care (much)
    - individually, not much load – in lightly-loaded direction (outbound)
    - hard to combat
    - haven’t adopted BCP38 (egress address filtering)

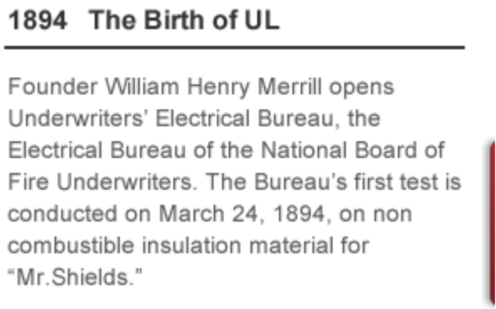
IoT lemons

- *"The Market for Lemons: Quality Uncertainty and the Market Mechanism*" (Akerlof, 1970)
- Information asymmetry
  - purchaser cannot judge invisible qualities
  - pays only average price
  - → above-average-quality goods not marketed
- "defect four or more times and the problem is still occurring, the car may be deemed to be a lemon" → get purchase price back
  - more than four patches?

Fixes for externalities and lemons

- Liability
  - slow, one-by-one, uncertain standards of care
  - what is “negligent”?
- Certification
  - voluntary or mandatory
- Insurance liability
  - homeowner’s insurance
- Regulation
  - adherence to minimum perfo standards





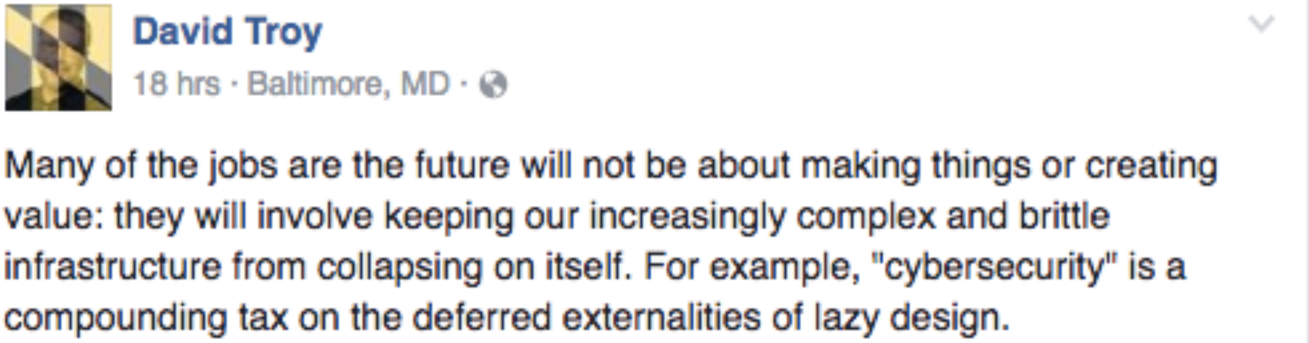
1894 The Birth of UL

Founder William Henry Merrill opens Underwriters’ Electrical Bureau, the Electrical Bureau of the National Board of Fire Underwriters. The Bureau’s first test is conducted on March 24, 1894, on non combustible insulation material for “Mr.Shields.”

This is not **that** hard!

- No factory-default passwords
  - long-term, no human-setable passwords at all → client certs
- No telnet, ssh, SNMP (typically)
- Only configure from local subset
- Automated, signed updates
- Web interfaces use non-root accounts
- Automated testing for XSS and SQL injection

PCI DSS COMPLIANT



David Troy

18 hrs · Baltimore, MD ·

Many of the jobs are the future will not be about making things or creating value: they will involve keeping our increasingly complex and brittle infrastructure from collapsing on itself. For example, "cybersecurity" is a compounding tax on the deferred externalities of lazy design.

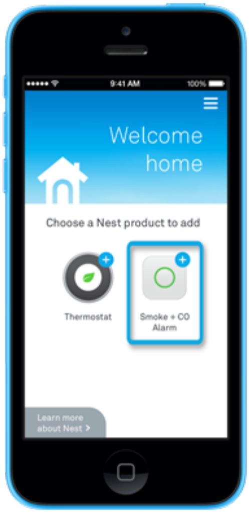
IoT good-citizen rules

FCC TAC recommendations +

- Implement current best practices
  - no plain-text data or commands
    - low-power CPUs are no excuse – long-payback or infrequent crypto operations
  - no default passwords
- Do not assume that your (cellular) network is around in > 8 years
  - short-range unlicensed bands more likely a safe harbor
- Update yourself securely
- Don’t trust random APs → PassPoint, 802.1x?
  - matters mainly for DNS and denial-of-service
- Go into fail-safe mode if no updates
- Be nice to cellular network (signaling, white spaces, …)
  - and maybe “kill switch” if misbehaving (or stolen!)
- Don’t ask for special spectrum
  - except maybe if you’re a health-and-safety device (but share nicely)
  - or maybe low-bandwidth narrowband spectrum

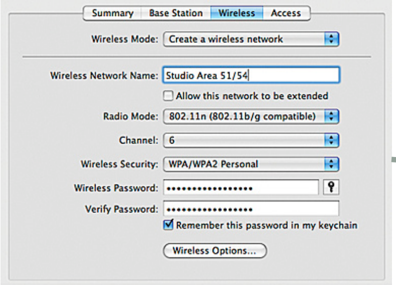
Challenge: enrollment

- Commercial buildings → enroll 1,000s of devices at once
- Home → enroll one device at a time
  - current model: one app per device (class)
  - re-do if Wi-Fi password changes
  - common options:
    - QR code
    - P2P Wi-Fi (Wi-Fi Direct)
  - possibilities
    - “hi, I’m a Philips light bulb – add me!” (PKI)



How should we secure things?

Old model



Summary | Base Station | Wireless | Access

Wireless Mode: Create a wireless network

Wireless Network Name: Studio Area 51/54

☐ Allow this network to be extended

Radio Mode: 802.11n (802.11b/g compatible)

Channel: 6

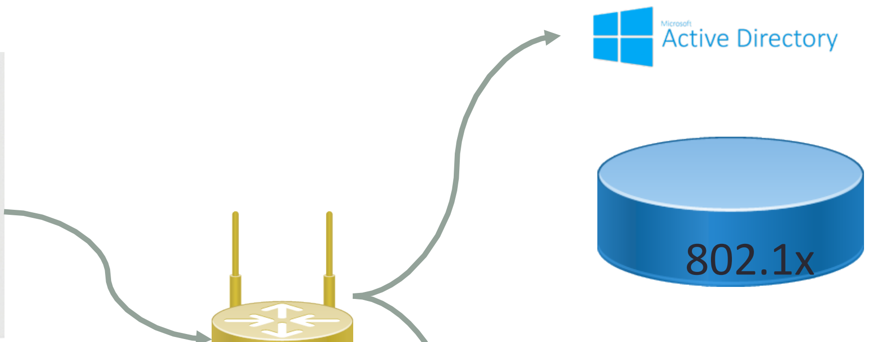
Wireless Security: WPA/WPA2 Personal

Wireless Password: •••••••••••••••••

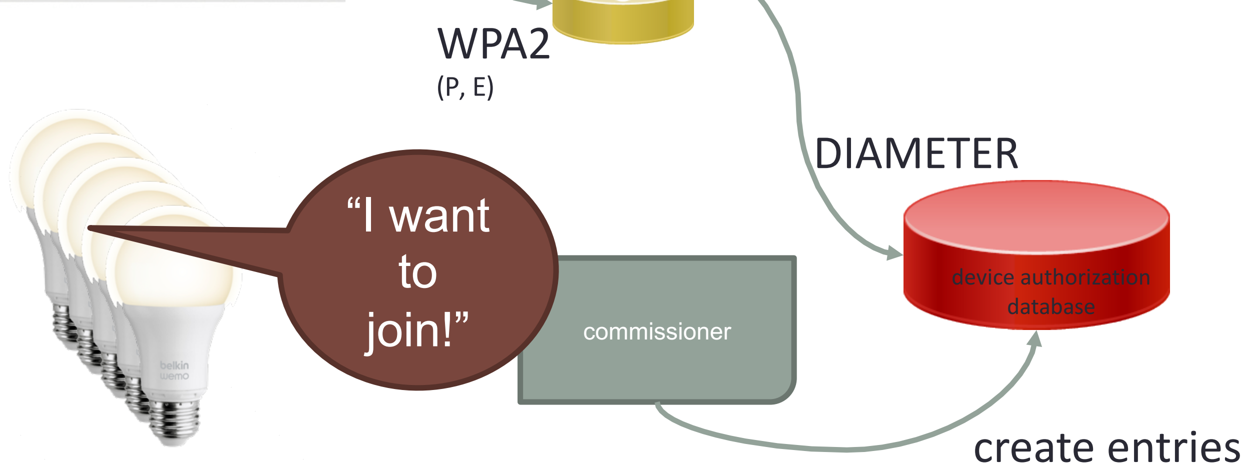
Verify Password: •••••••••••••••••

☑ Remember this password in my keychain

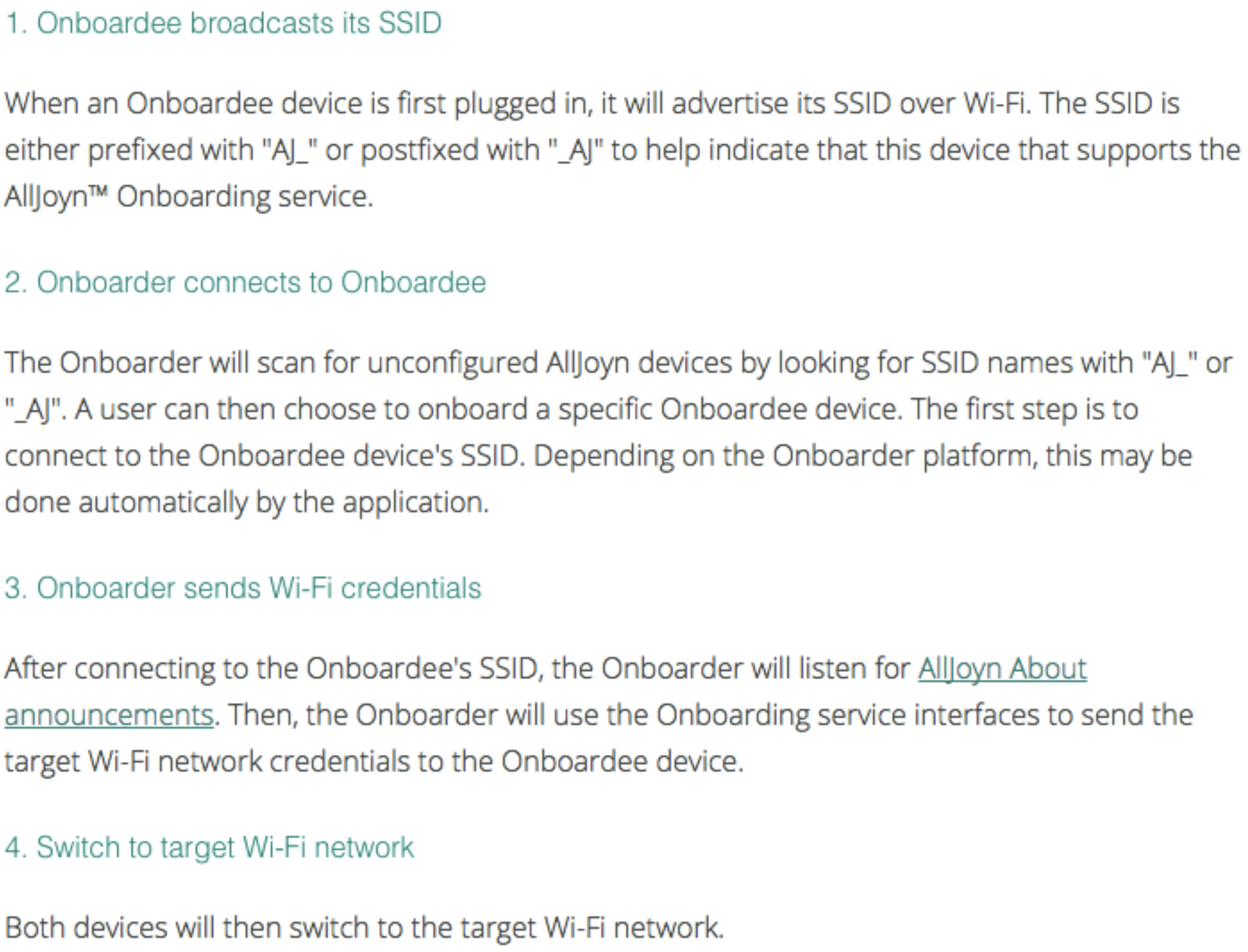
Wireless Options...



New model



AllJoyn is doing something similar



1. Onboardee broadcasts its SSID

When an Onboardee device is first plugged in, it will advertise its SSID over Wi-Fi. The SSID is either prefixed with "AJ_" or postfixed with "_AJ" to help indicate that this device that supports the AllJoyn™ Onboarding service.

2. Onboarder connects to Onboardee

The Onboarder will scan for unconfigured AllJoyn devices by looking for SSID names with "AJ_" or "_AJ". A user can then choose to onboard a specific Onboardee device. The first step is to connect to the Onboardee device's SSID. Depending on the Onboarder platform, this may be done automatically by the application.

3. Onboarder sends Wi-Fi credentials

After connecting to the Onboardee's SSID, the Onboarder will listen for AllJoyn About announcements. Then, the Onboarder will use the Onboarding service interfaces to send the target Wi-Fi network credentials to the Onboardee device.

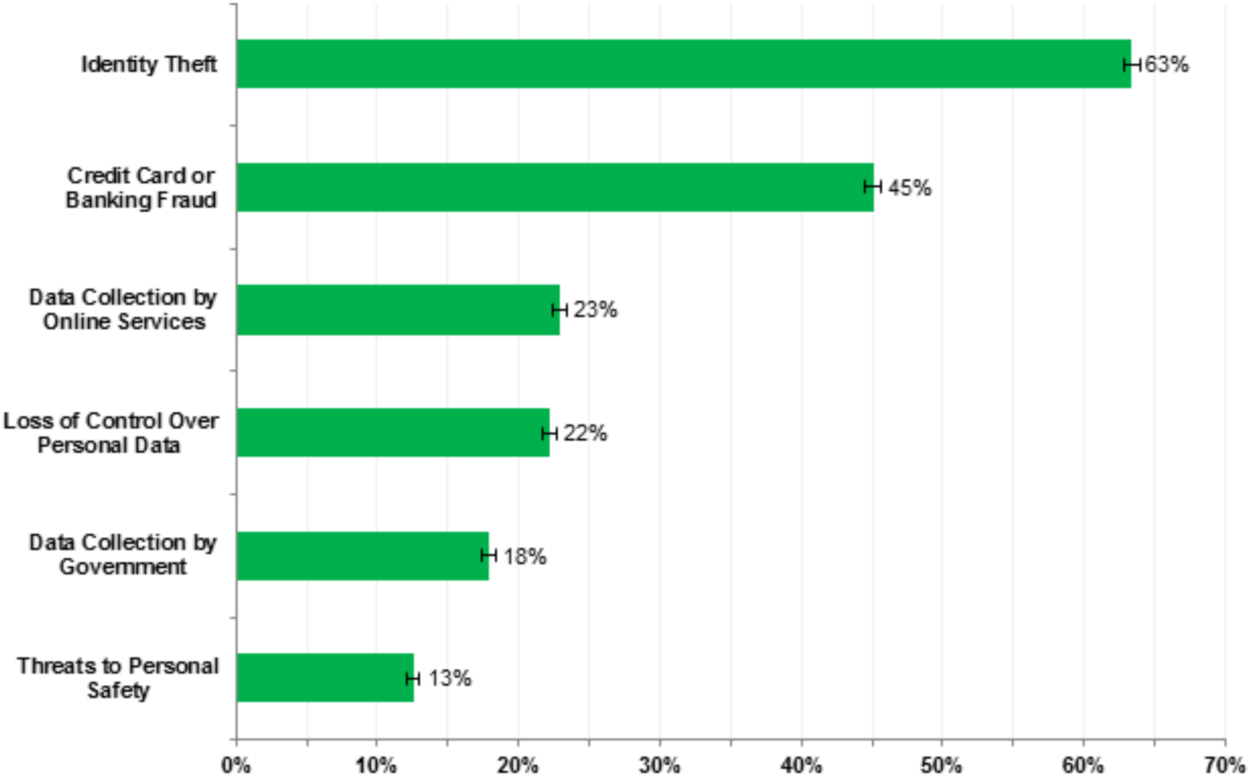
4. Switch to target Wi-Fi network

Both devices will then switch to the target Wi-Fi network.

PRIVACY

“Remember when, on the Internet, nobody knew who you were?”

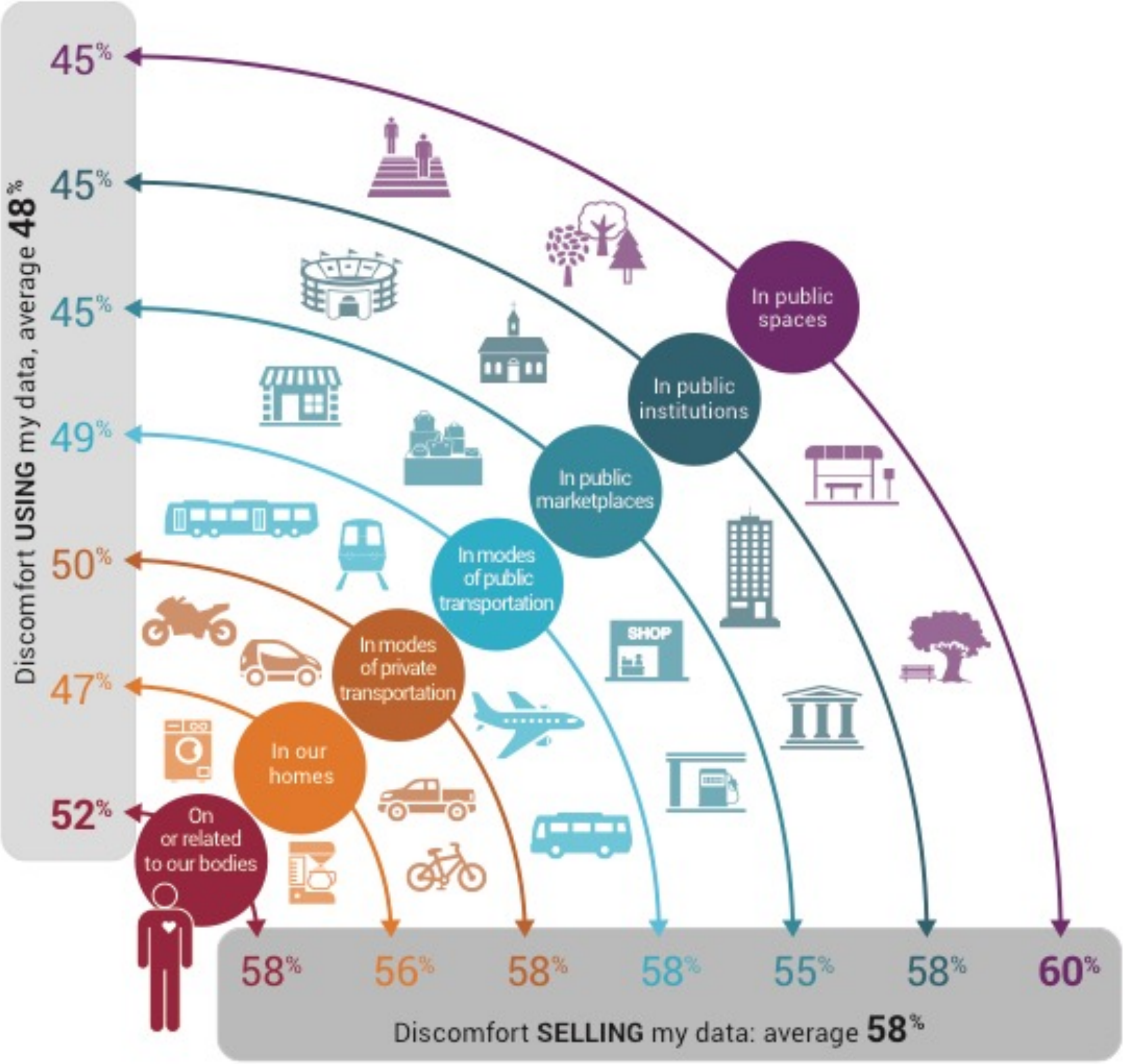
Privacy fears deter usage



NTIA
May 2016

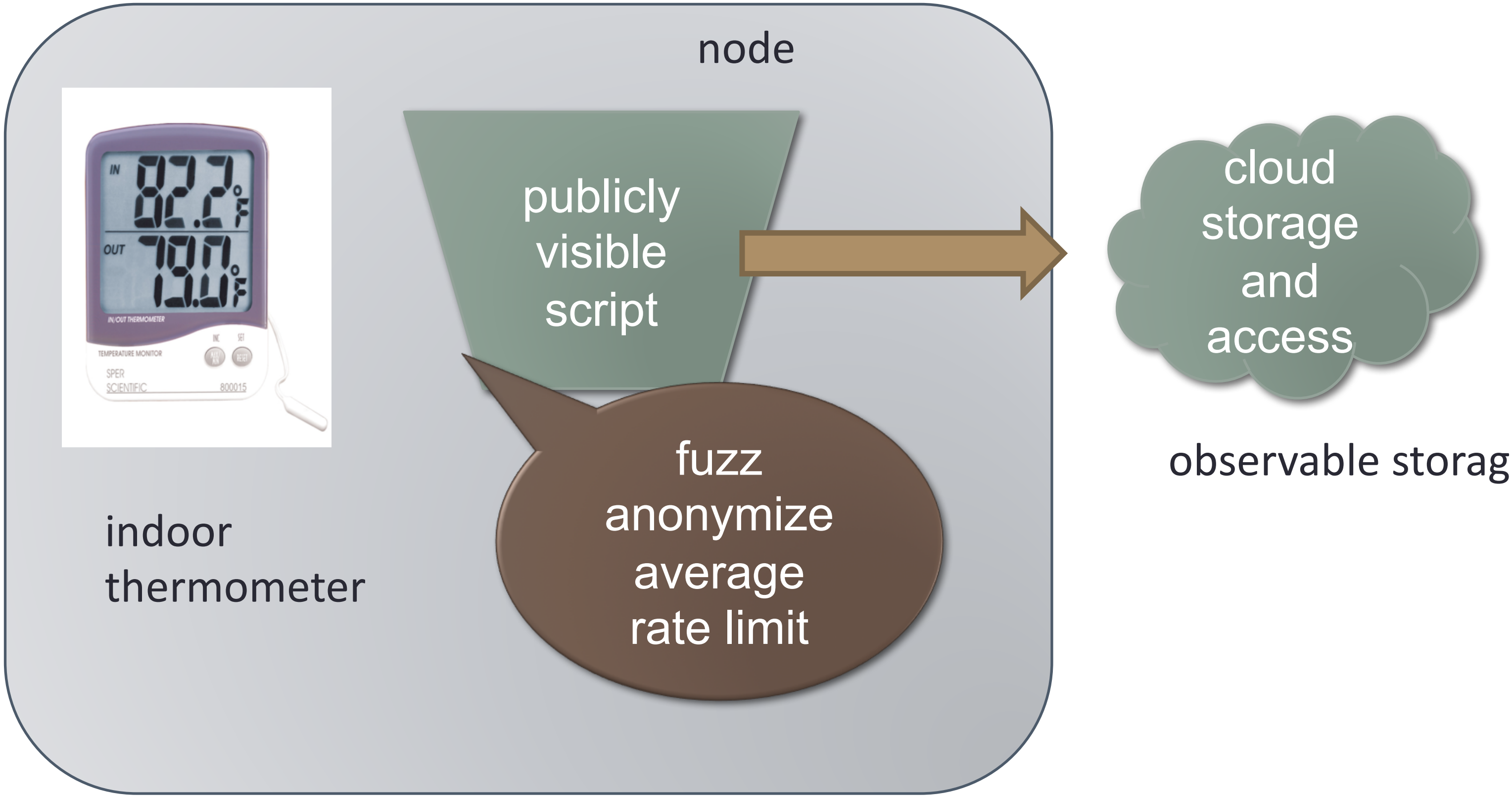
Major Concerns Related to Online Privacy and Security Risks, Percent of Households with Internet Users, 2015

Roughly half of consumers uncomfortable



Altimeter Group
June 2015

Local processing for ~~efficiency~~ privacy



node

indoor
thermometer

publicly
visible
script

fuzz
anonymize
average
rate limit

cloud
storage
and
access

observable storage

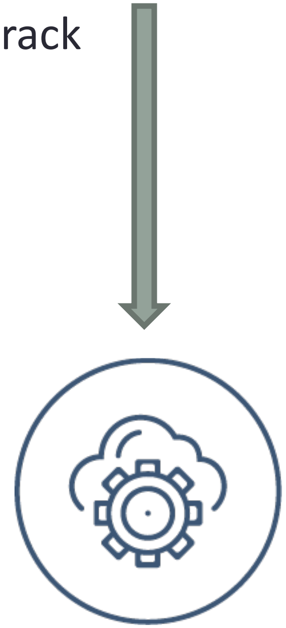
fog computing model

BUILDING LARGE IOT SYSTEMS

IoT = Internet at scale

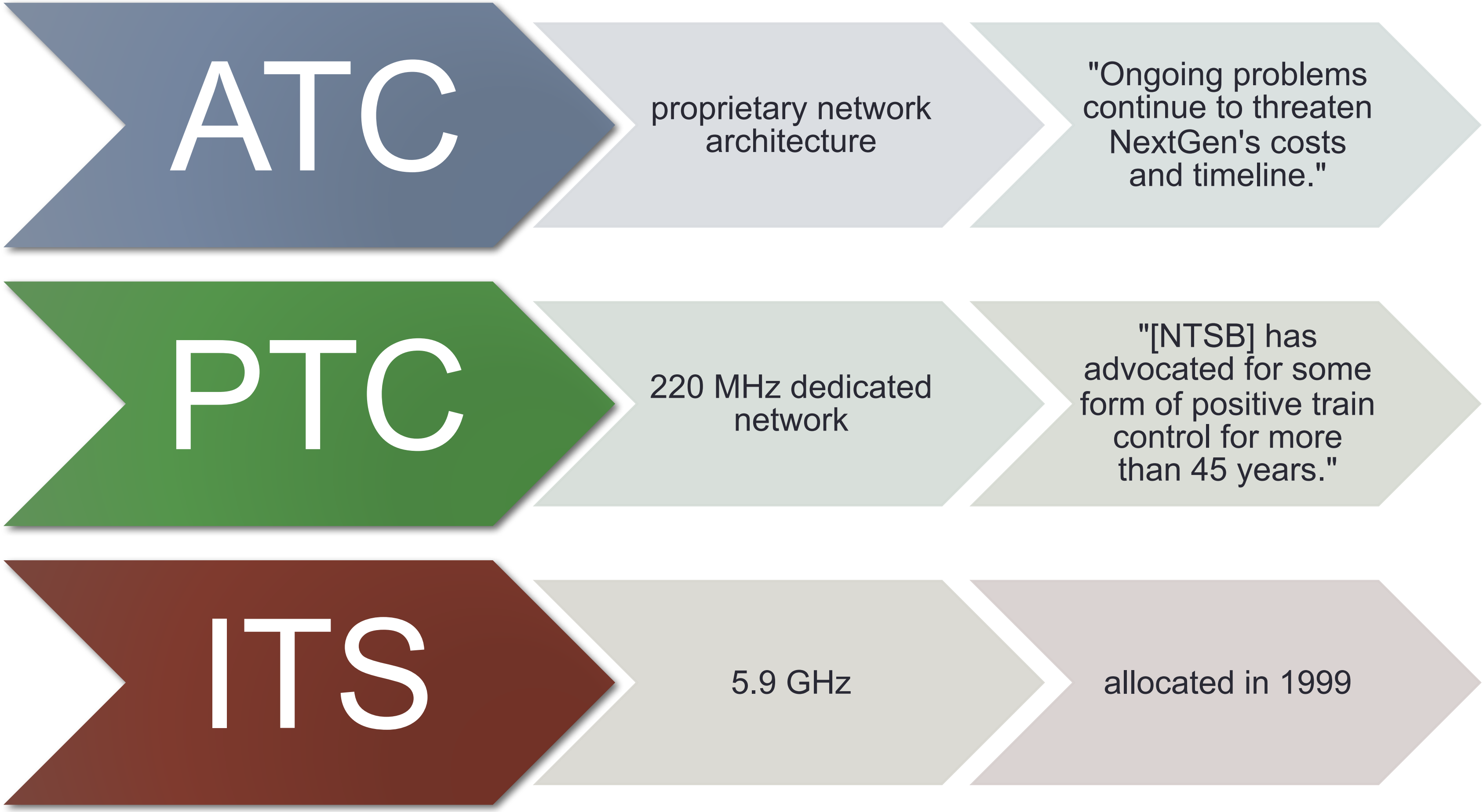
- *Security* at scale
  - still largely “add password to configuration file”
  - identify by IP address
- *Management* at scale
  - device-focused
  - SNMP, at best
  - CLI, at worst
  - no performance diagnostics capabilities (“why is this so slow?”
- *Naming* at scale
  - identify by node name
- *Programming* at scale

system & rack



data center

Lessons from early IoT (and cousins)



ATC

proprietary network architecture

"Ongoing problems continue to threaten NextGen's costs and timeline."

PTC

220 MHz dedicated network

"[NTSB] has advocated for some form of positive train control for more than 45 years."

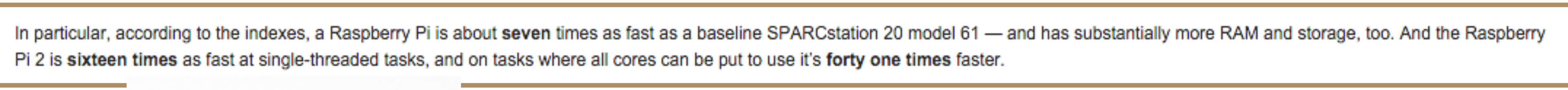
ITS

5.9 GHz

allocated in 1999

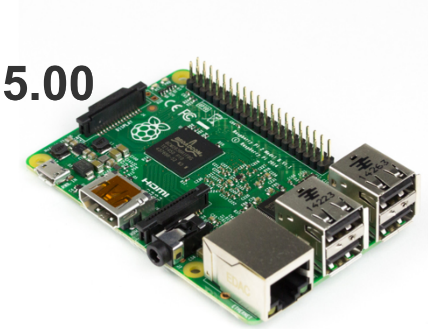
Lesson: sensor networks may be (tiny) niche

- Most IoT systems will be near power since they'll interact with energy-based systems (li
- Most IoT systems will not be running TinyOS (or similar)
- Protocol processing overhead is unlikely to matter
- Low message volume → cryptography overhead is unlikely to matter

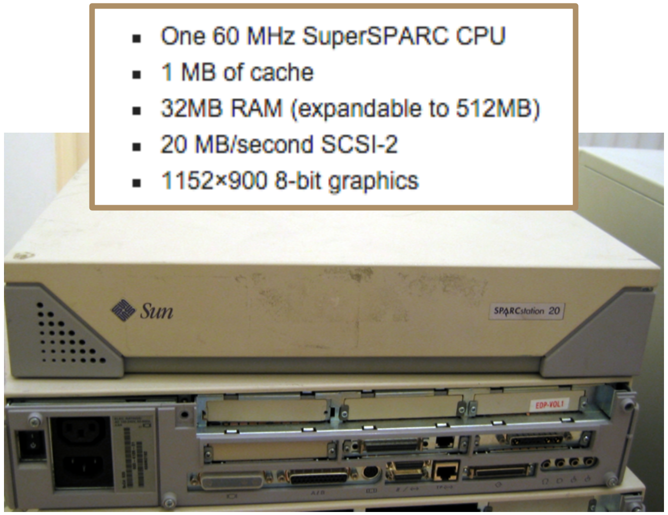


In particular, according to the indexes, a Raspberry Pi is about **seven** times as fast as a baseline SPARCstation 20 model 61 — and has substantially more RAM and storage, too. And the Raspberry Pi 2 is **sixteen times** as fast at single-threaded tasks, and on tasks where all cores can be put to use it's **forty one times** faster.

$35.00



- A 900MHz quad-core ARM Cortex-A7
- 1 GB RAM



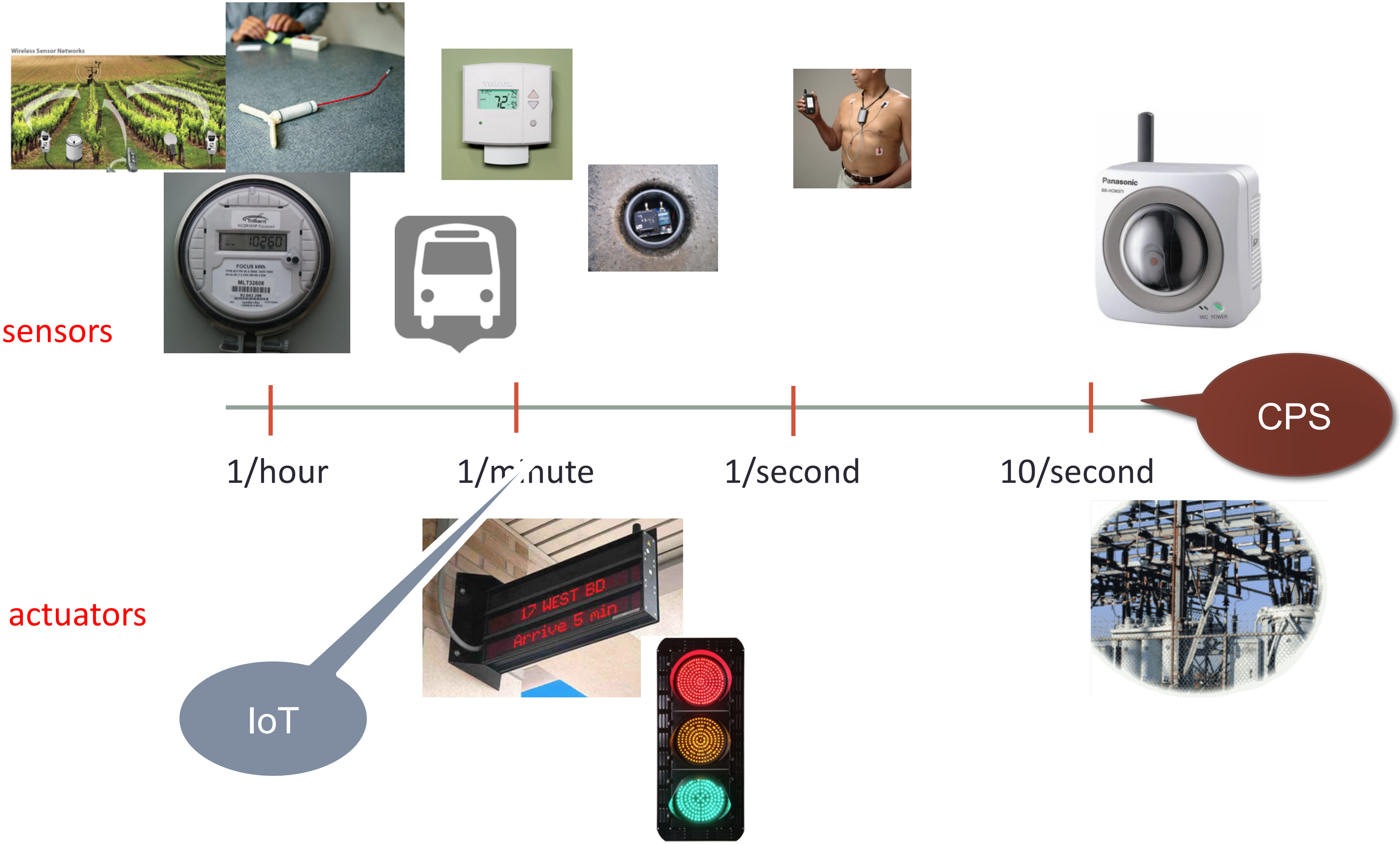
- One 60 MHz SuperSPARC CPU
- 1 MB of cache
- 32MB RAM (expandable to 512MB)
- 20 MB/second SCSI-2
- 1152×900 8-bit graphics

http://eschatologist.net/blog/?p=266

The age of application-specific {sensors, spectrum, OS, protocol …} is over

- *Computing system*: dedicated function → OS
  - → abstract into generic components
  - e.g., USB human interface device (HID)
- What are the equivalent sensor and actuator classes?
- *Networks*: generic app protocols
  - request/response → HTTP
  - event notification → SMTP, SIP, XMPP
- *Spectrum*: from new application = new spectrum to generic data transport

IoT varies in communication needs



sensors

1/hour

1/minute

1/second

10/second

CPS

actuators

IoT

5G is not the only option

indoor
unmanaged

ZigBee®

Bluetooth®

Wi Fi™

indoor
ext. managed

Lte

outdoor
urban

LoRa™

outdoor
rural

Lte

SIGFOX

outdoor
remote

Niche networks

short range

ZigBee®

low energy; mesh

Bluetooth®

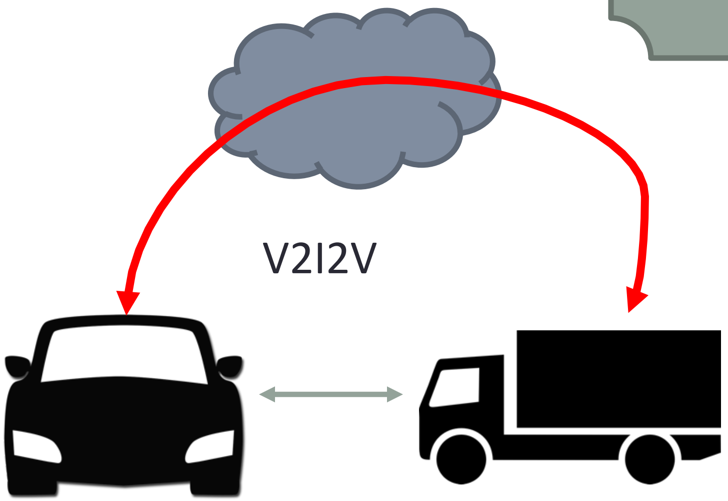
ubiquity; low cost

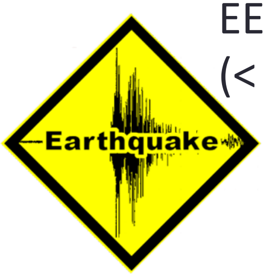
Wi Fi™

speed; public APs

5G = low latency + mmW + …

one-to-many!



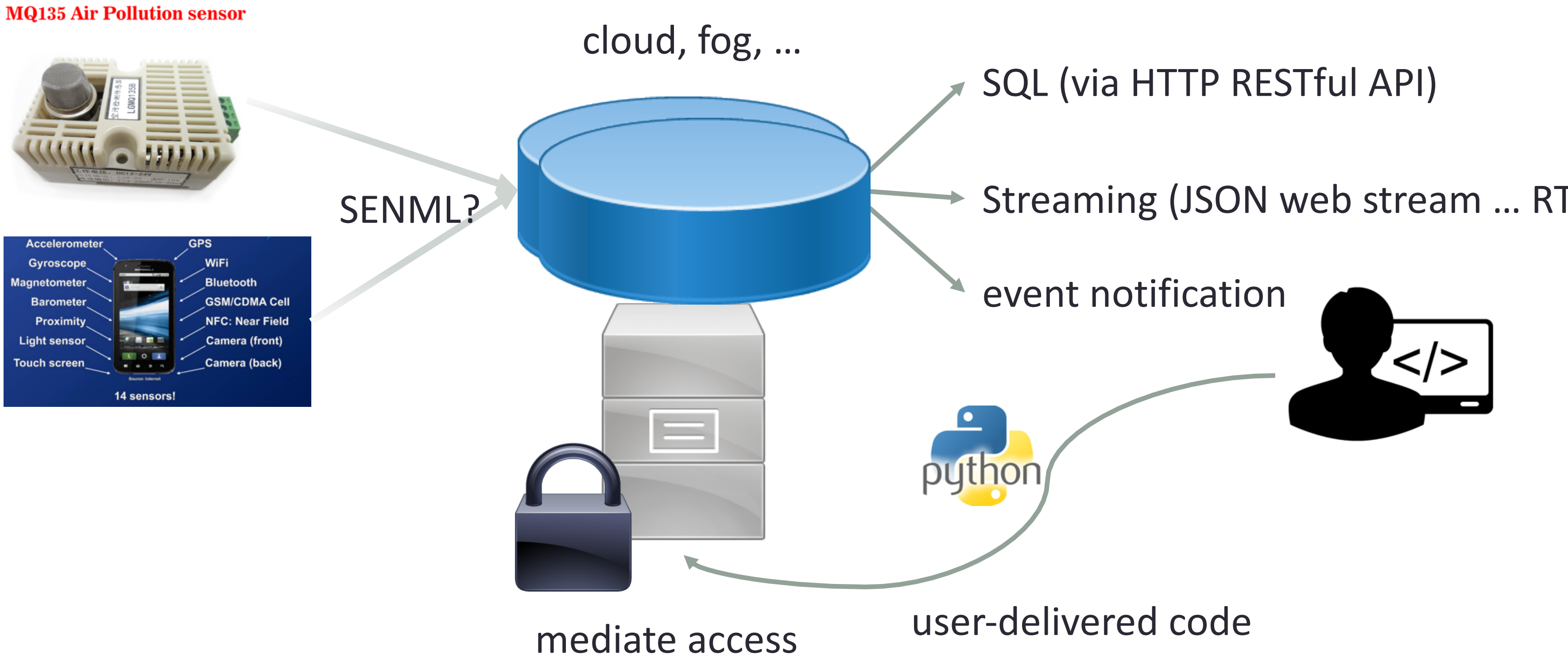


EEW
(< 5 s)

Protocols matter, but programmability matters more

- Nobody wants to program raw protocols
- Most significant network application creation advances:
  - 1983: socket API → abstract data stream or datagram
  - 1998: Java network API → mostly names, HTTP, threads
  - 1998: PHP → network input as script variables
  - 2005: Ruby on Rails → simplify common patterns
- Many fine protocols and frameworks failed the programmer hate test
  - e.g., JAIN for VoIP, SOAP for RPC
- Most IoT programmers will not be computer scientists

What is the best generic (simple) architecture?



MQ135 Air Pollution sensor

cloud, fog, …

SENML?

SQL (via HTTP RESTful API)

Streaming (JSON web stream … RT

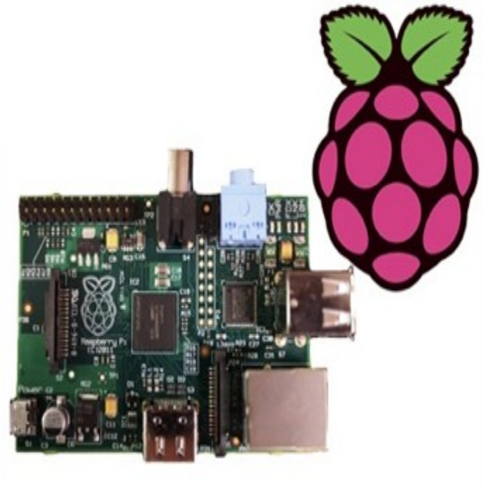
event notification

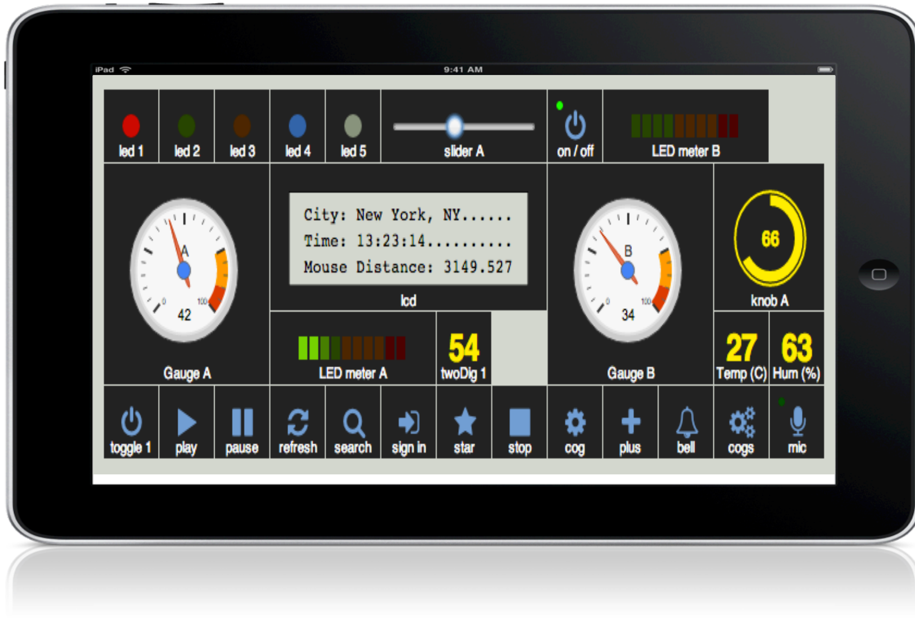
mediate access

user-delivered code

Challenge: integrate embedded, mobile & virtual

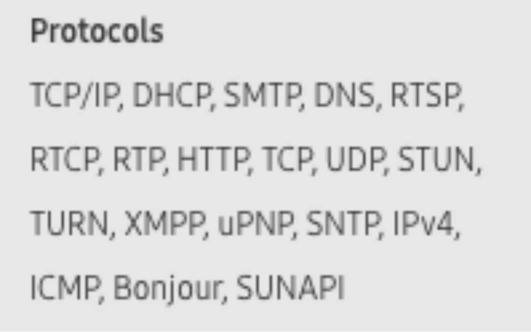
magnetometer
accelerometer
location
gyroscope





City: New York, NY......
Time: 13:23:14.........
Mouse Distance: 3149.527

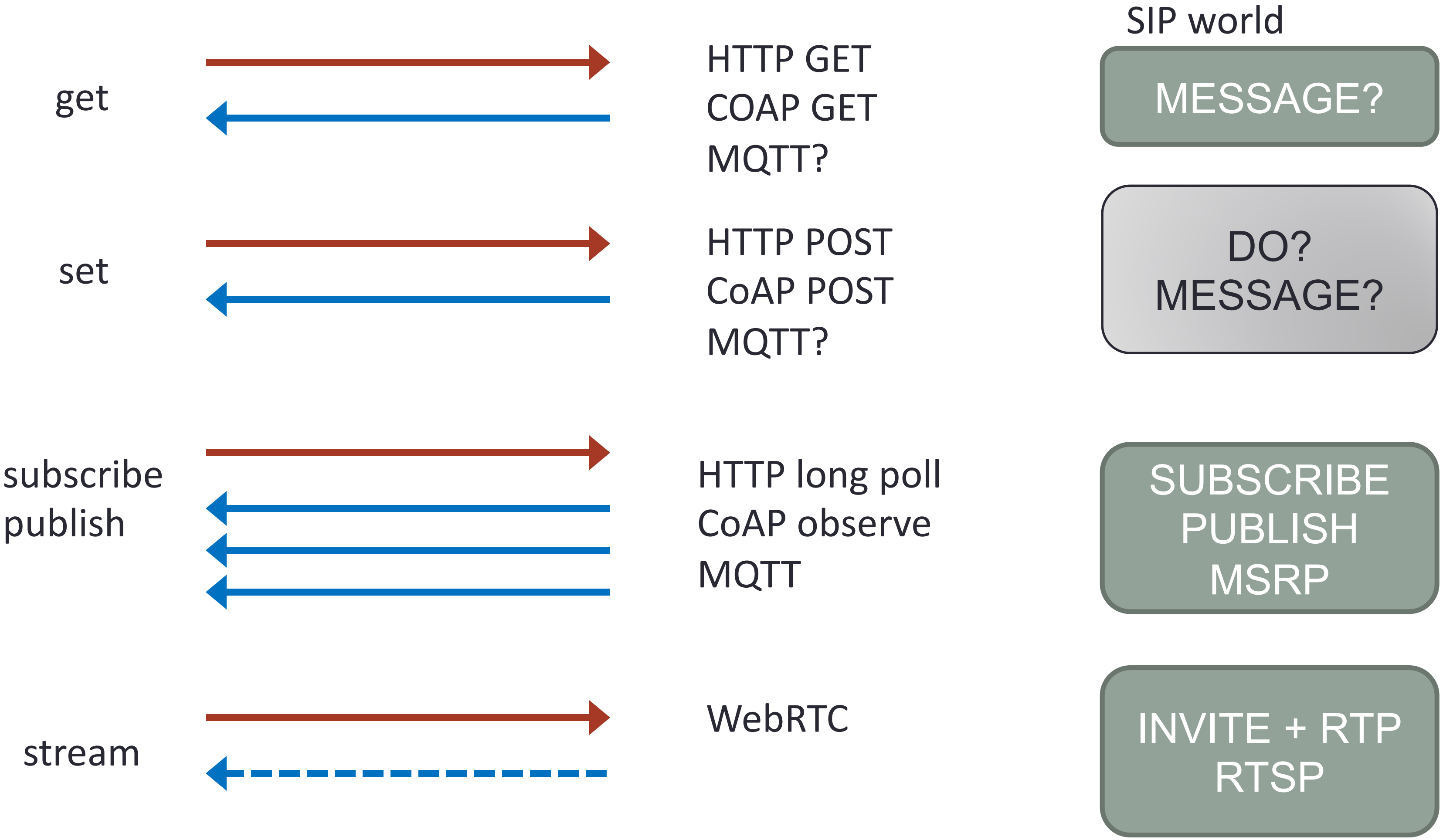
Some of IoT is streaming


Protocols

TCP/IP, DHCP, SMTP, DNS, RTSP, RTCP, RTP, HTTP, TCP, UDP, STUN, TURN, XMPP, uPNP, SNTP, IPv4, ICMP, Bonjour, SUNAPI

update rate of 10 to 250 Hz

IoT communication modalities



SIP world

get

HTTP GET
COAP GET
MQTT?

MESSAGE?

set

HTTP POST
CoAP POST
MQTT?

DO?
MESSAGE?

subscribe
publish

HTTP long poll
CoAP observe
MQTT

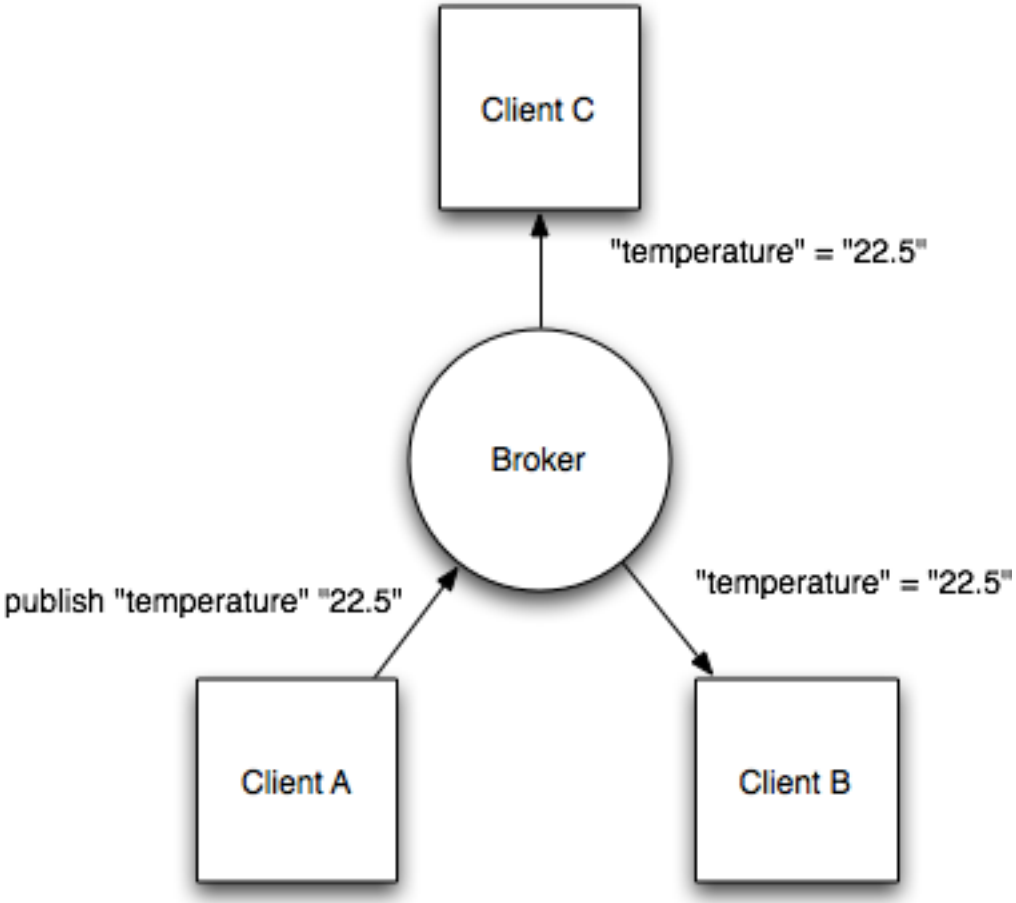
SUBSCRIBE
PUBLISH
MSRP

stream

WebRTC

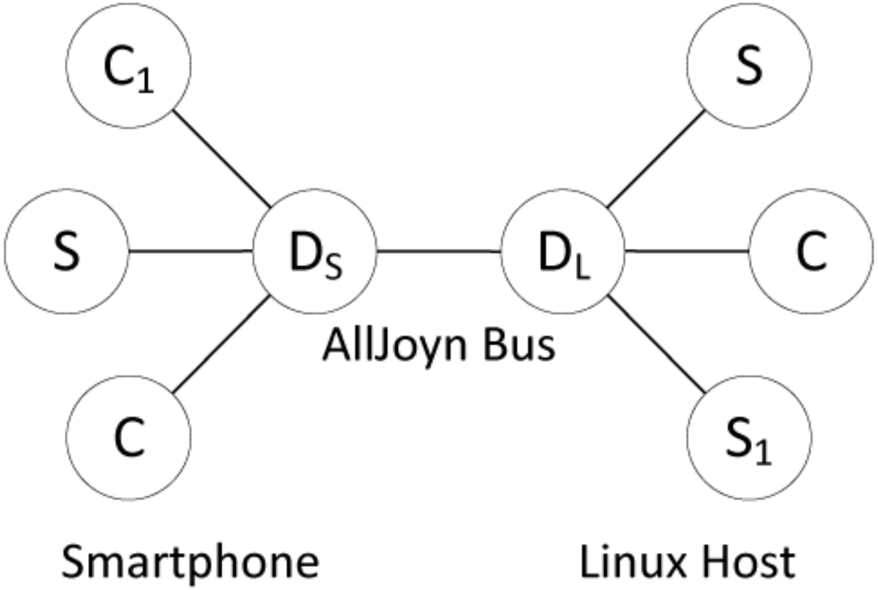
INVITE + RTP
RTSP

MQTT model



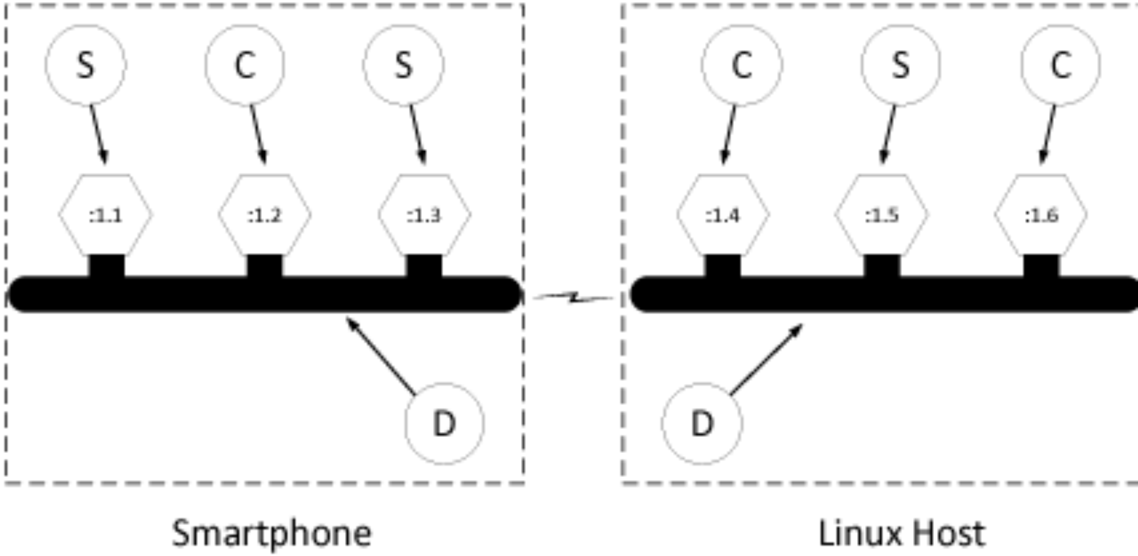
```
kitchen/+/temperature matches
kitchen/foo/temperature but not
kitchen/foo/bar/temperature
```

Example: AllJoyn bus



publish-subscribe model (implicit)

Wi-Fi
UDP multicast
BT SDP



Device control

2001

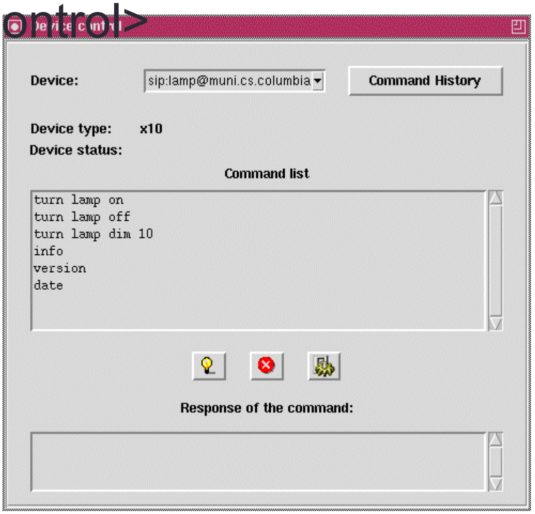
Do sip:lamp@cs.columbia.edu SIP/2.0

…..

<Control>

<Action>turn lamp on</Action>

</Control>



Device: sip:lamp@muni.cs.columbia

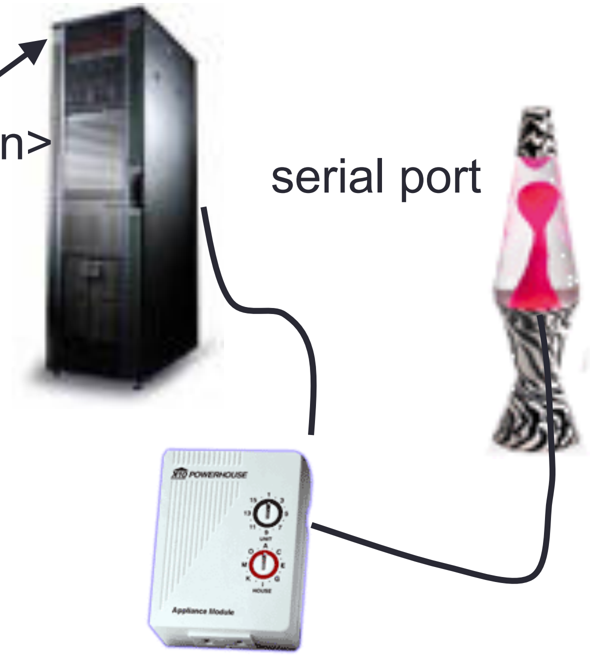
Device type: x10

Device status:

Command list

```
turn lamp on
turn lamp off
turn lamp dim 10
info
version
date
```

Response of the command:



We could do better

- Somewhat unsatisfactory
  - AllJoyn model only for LAN operations
  - CoAP & HTTP better for get/set operations
  - MQTT simpler for publish/subscribe
  - SIP (or RTSP) better for media streaming
- Lots of proprietary network protocols
  - BAC for building automation
- Same device or source, multiple identifiers
  - HTTP URL or SIP URL or MQTT IP address/domain name
  - none are particularly useful or semantically meaningful
    - e.g., likely change if device is replaced

LIFECYCLE

Windows XP, Corolla & Revolv

13 years

available 12/2001

end of sales 6/2008

end support 4/2009

end install 10/2010

end ext. support 4/2014

1996 Corolla
- still can get parts

$2,359

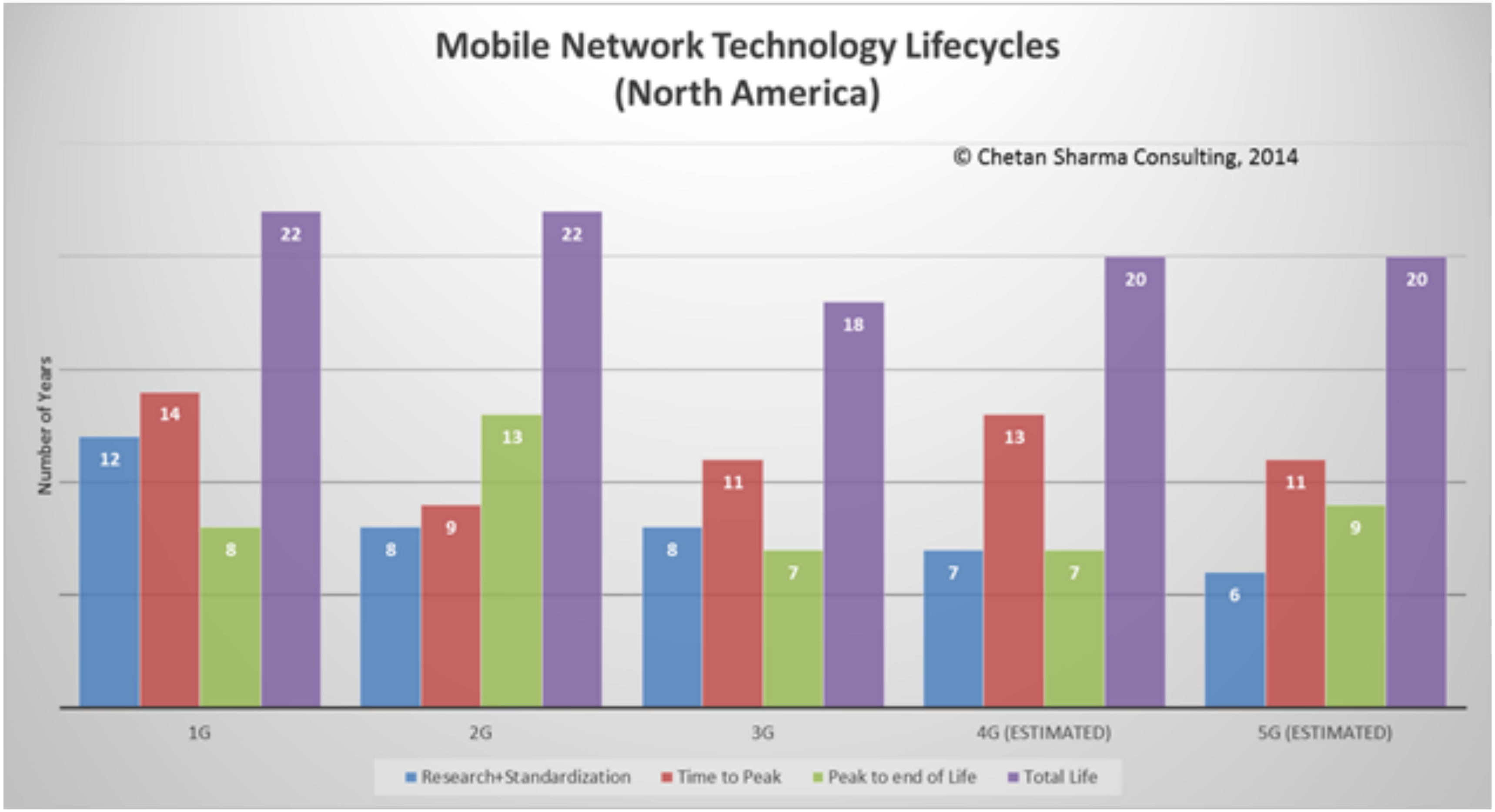
NEST'S HUB SHUTDOWN PROVES YOU'RE CRAZY TO BUY INTO THE INTERNET OF THINGS

VOLV

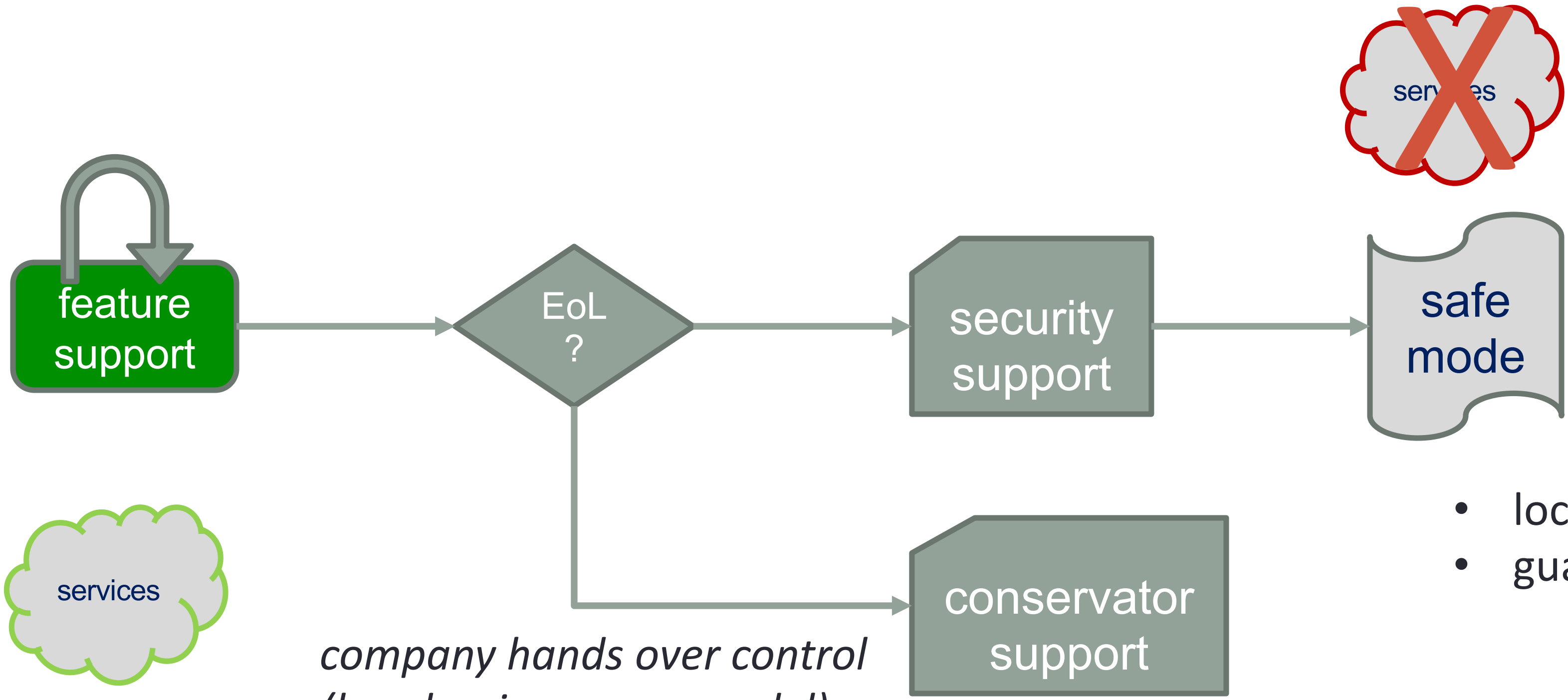
founded 2012
acquired by Nest 2014
shut down May 2016

IF YOU WERE one of the people who shelled out $300 for Revolv's smart home hub, you've probably already heard the bad news: the web service that powers the little gadget is shutting down next month, which will render the thing effectively useless.

Design for 20 years



IoT needs a life cycle model



services

feature support

services

EoL ?

security support

safe mode

conservator support

company hands over control (bond or insurance model)

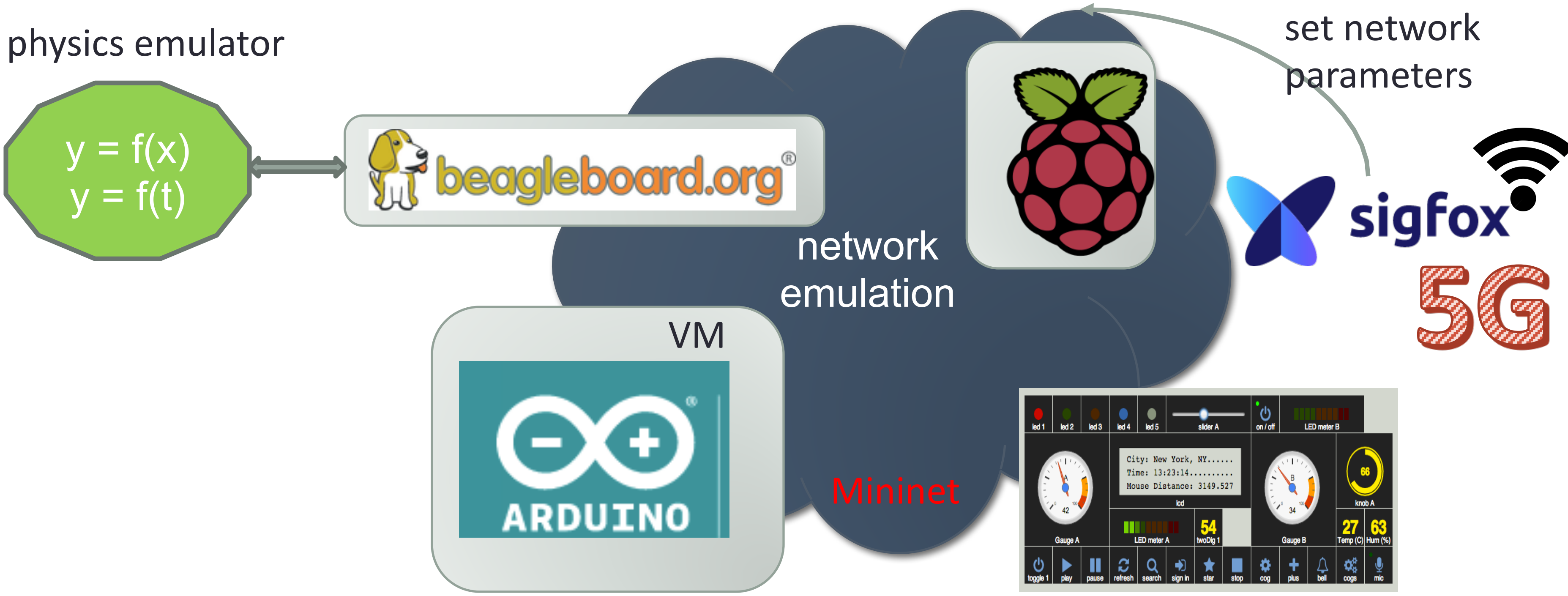
- local only
- guardian

IoT needs an economic model

- Do you own or rent a device?
    - and do you know what rights you have (transfer, sale, …)?
    - and for how long?
- What is expected lifetime?
    - in what mode?
    - with what enhancements?
- Who pays for computation and storage?
    - printer & ink? stove & electricity?
    - subscription model → doesn't scale except with aggregator
    - advertising model → creepiness-factor, no direct interaction
    - third party model: health or fire insurance, research ("your data for science"), electric utility

Development lifecycle

- Currently, hard to design large-scale reliable systems
  - failure modes, server load, control algorithms, …
- See Jan Janak’s talk at 1.30 today



http://mininet.org/

Conclusion

- IoT is finding lots of boring niches
- But IoT security is exposing almost all the security deficiencies of the Internet eco system
  - “thoughts and prayers” approach
  - continuing to do the same thing for the next 5 years and hoping for better results is not a strategy
- Start thinking beyond stove pipes of applications
- → engineering large scale systems