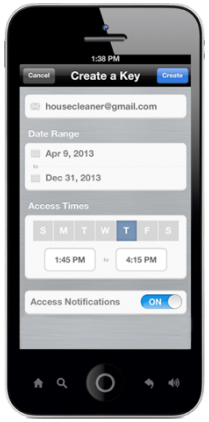
SCALING IOT UP, DOWN AND OUT

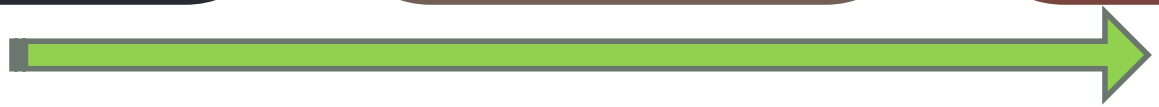
Henning Schulzrinne

(+ Jan Janak & other CUCS IRT contributors)

CNSM 2016

Natural evolution

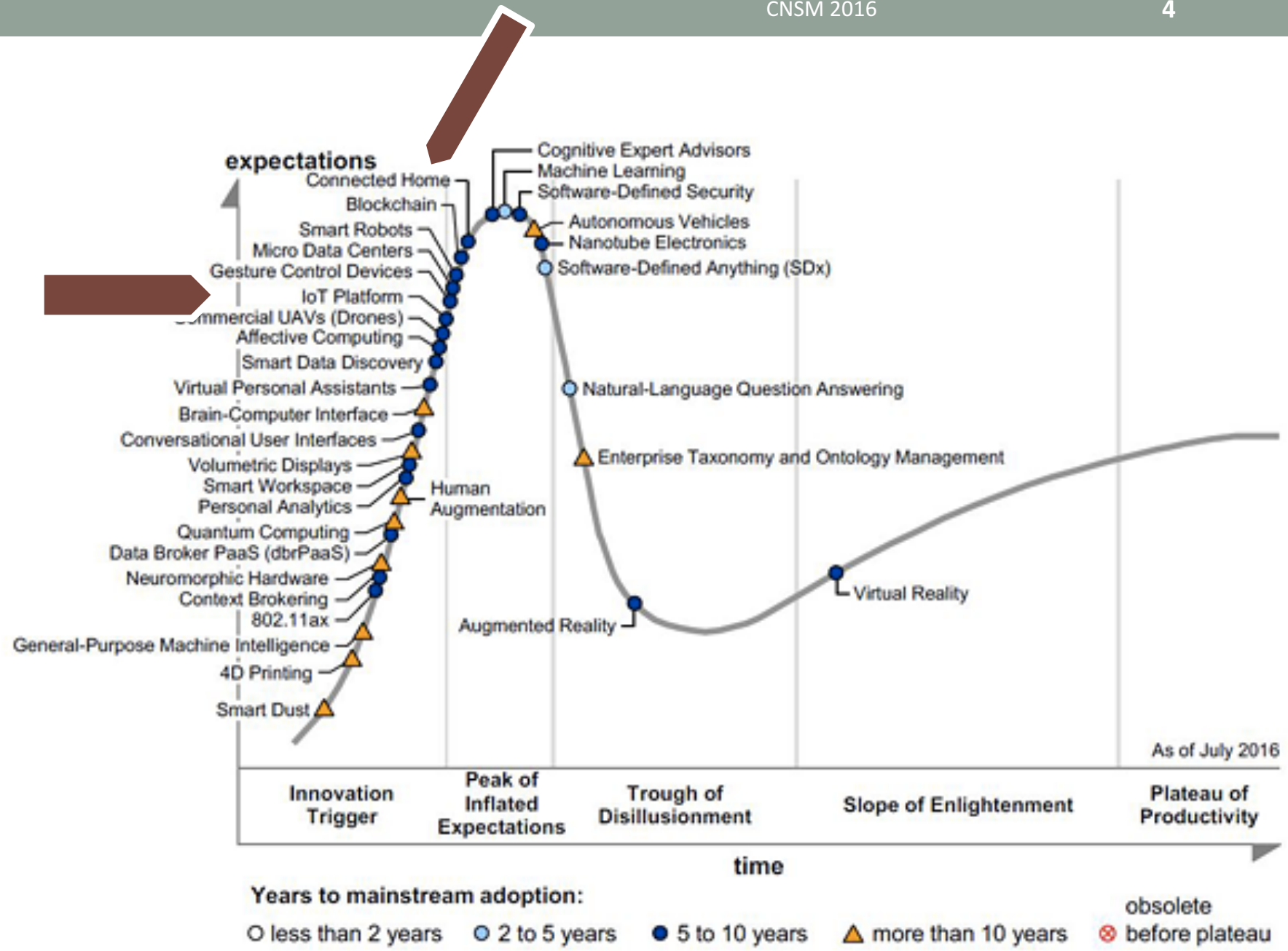




The IoT universe

network devices

sense & control



Source: Gartner (July 2016)

Kids, don’t do this at home

https://twitter.com/internetofshit

Towel dispensers

Power over ethernet powered paper towel dispensers

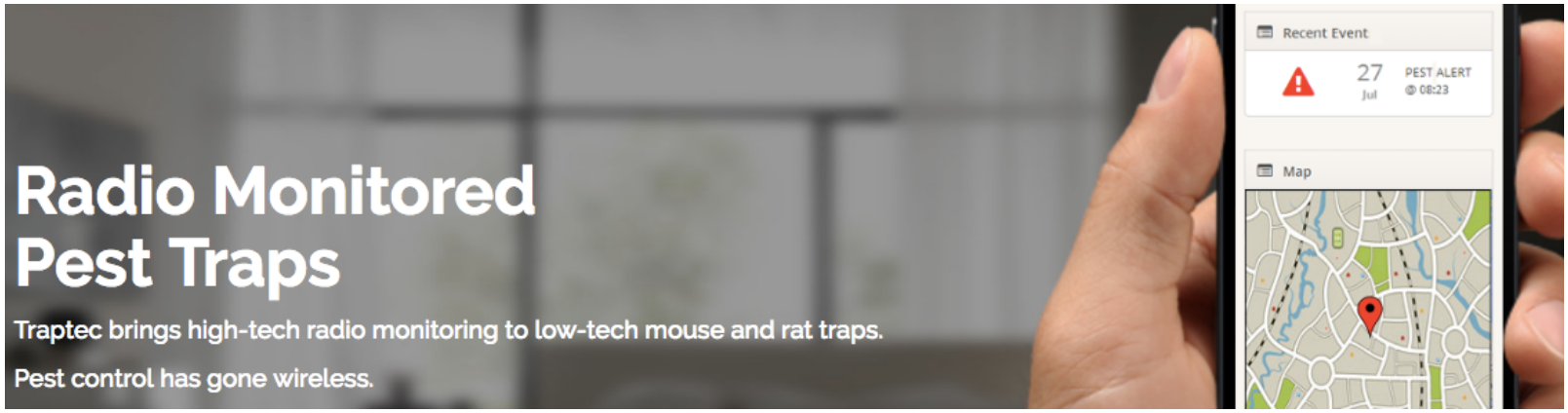
WO 2014028808 A1

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



http://www.traptec.eu/

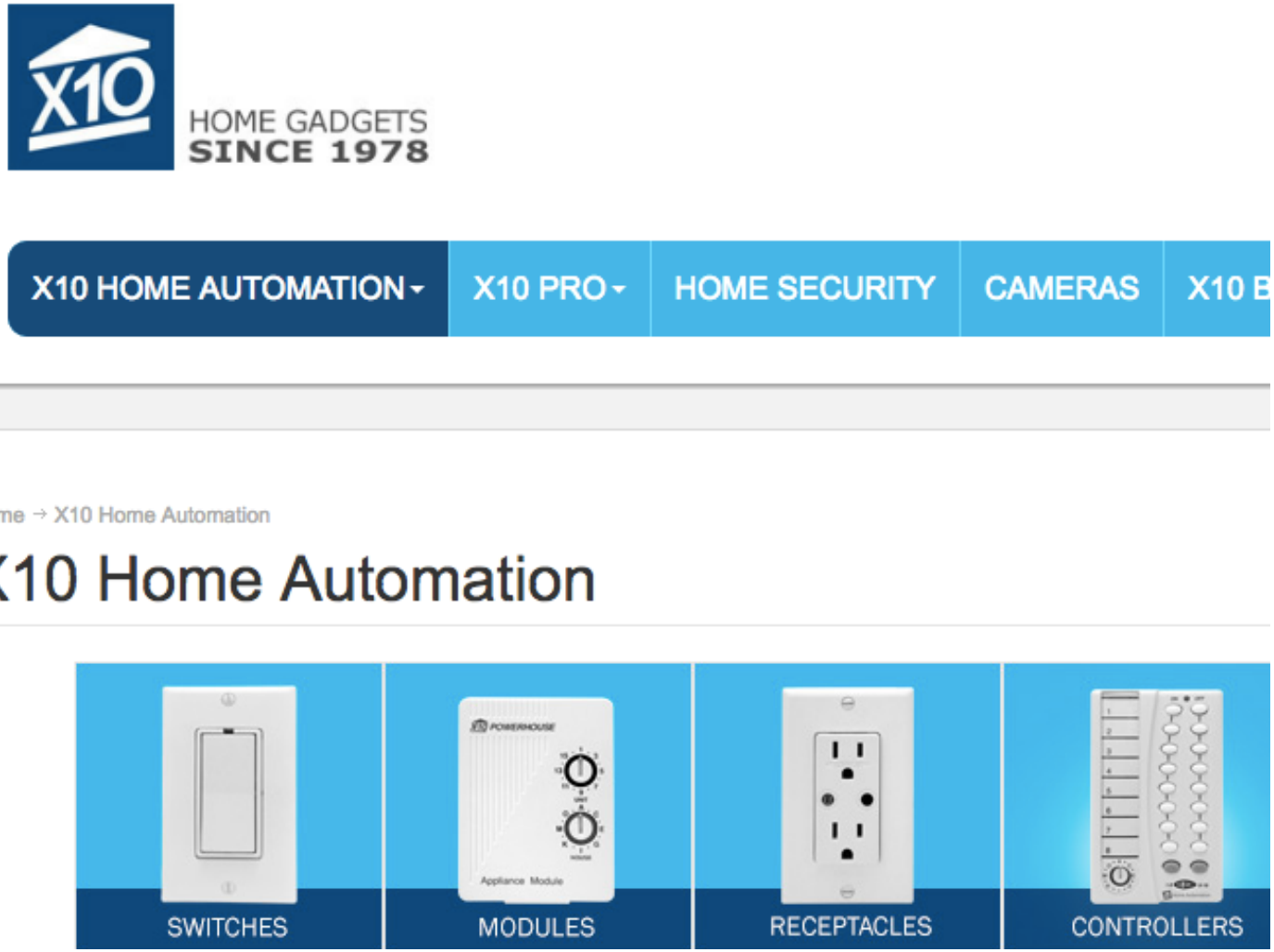
Drones as part of the IoT

images
pollution
noise

link.nyc & smart trash cans

GPRS or CDMA
GPS location service

IoT is not exactly new



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?

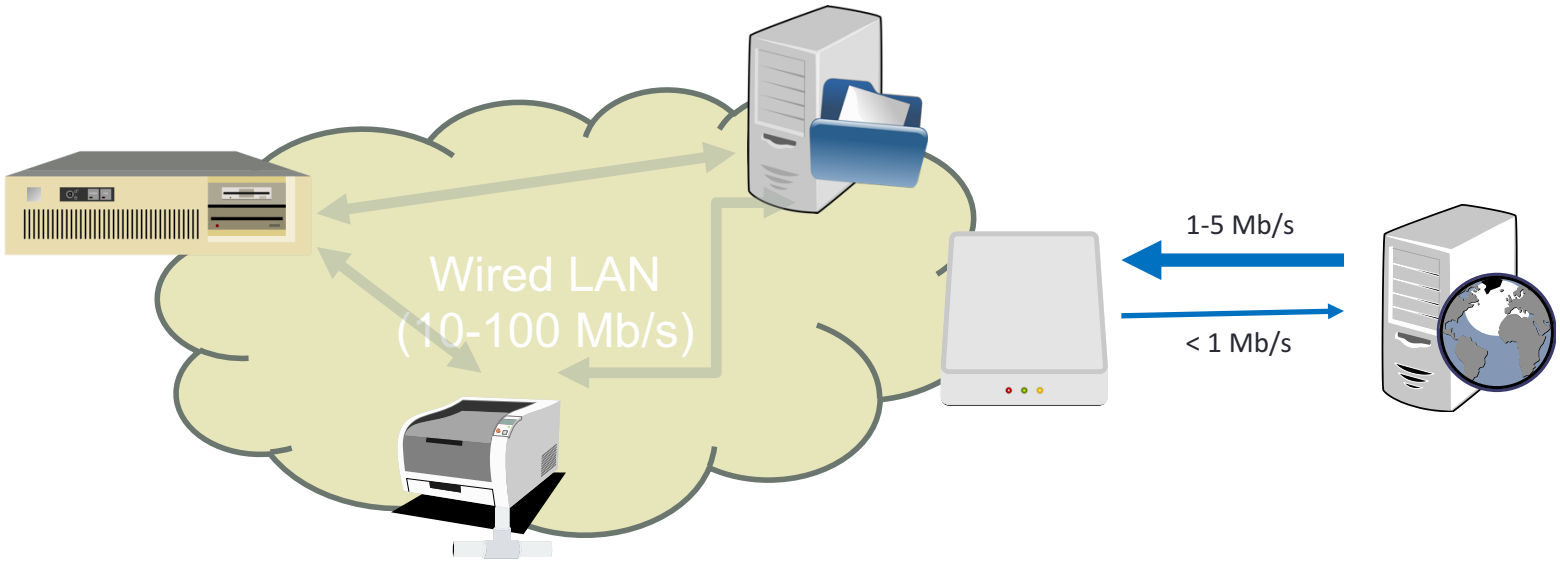
not cost-effective, not just useless

What is still to be solved?

- How can we secure IoT?
- How can we protect user privacy?
- How can we design it at scale?
- How can we make sure it works reliably?
- How can we make it work for non-experts?

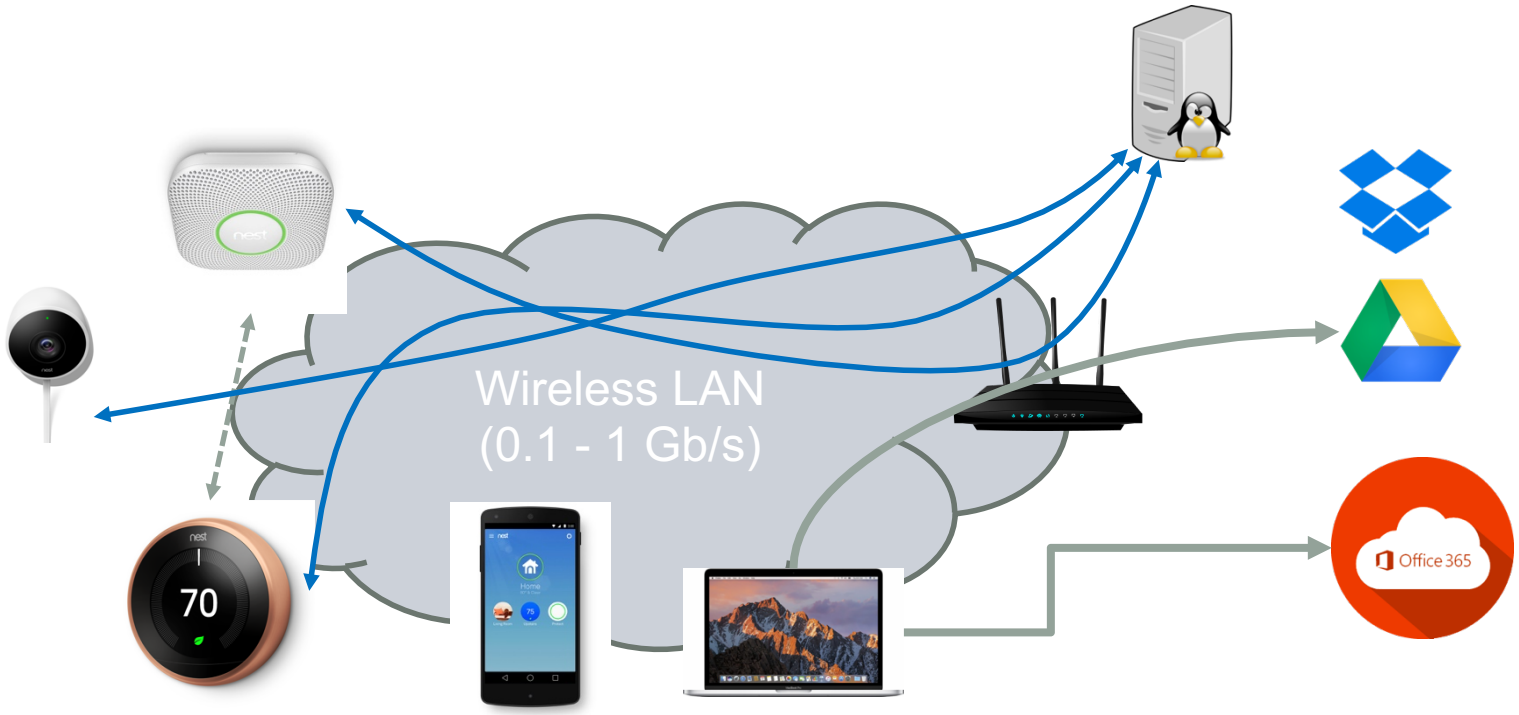
SECURITY

Old home & office architecture



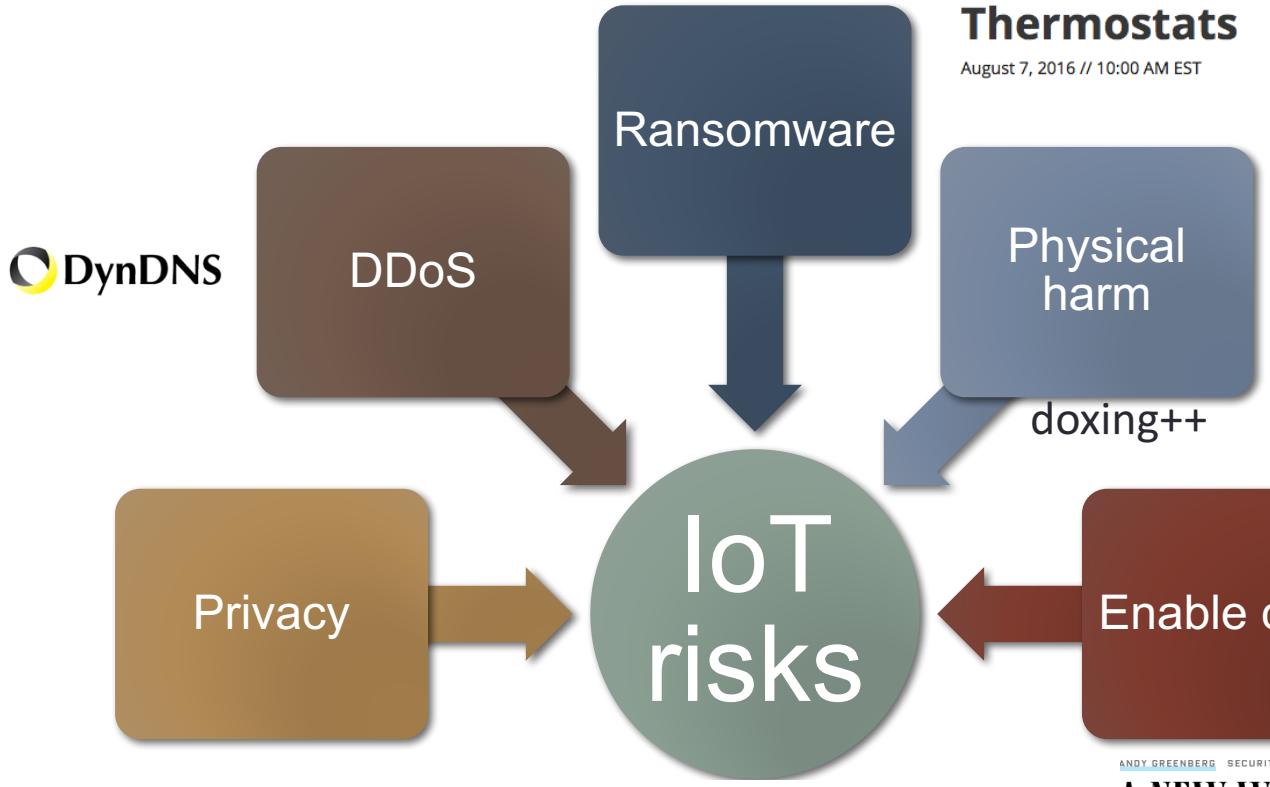
1995 – 2010: most communications was local, with web browsing as main Internet activity

IoT and home architecture



- relatively little intra-LAN
- mostly LAN-to-cloud
- upload-download ratio may change

IoT combines risks



Hackers Make the First-Ever Ransomware for Smart Thermostats

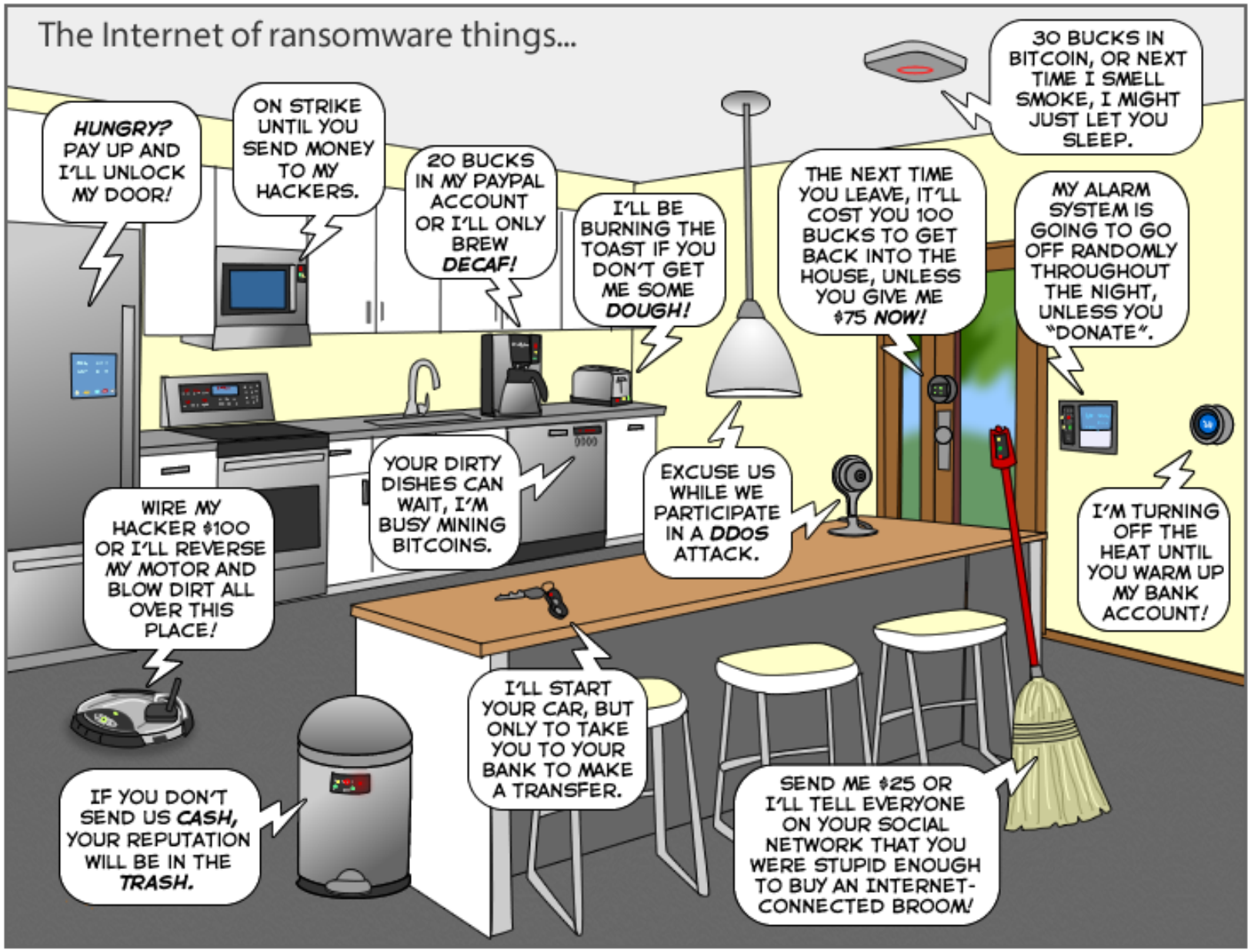
August 7, 2016 // 10:00 AM EST

Stranger hacks family's baby monitor and talks to child at night

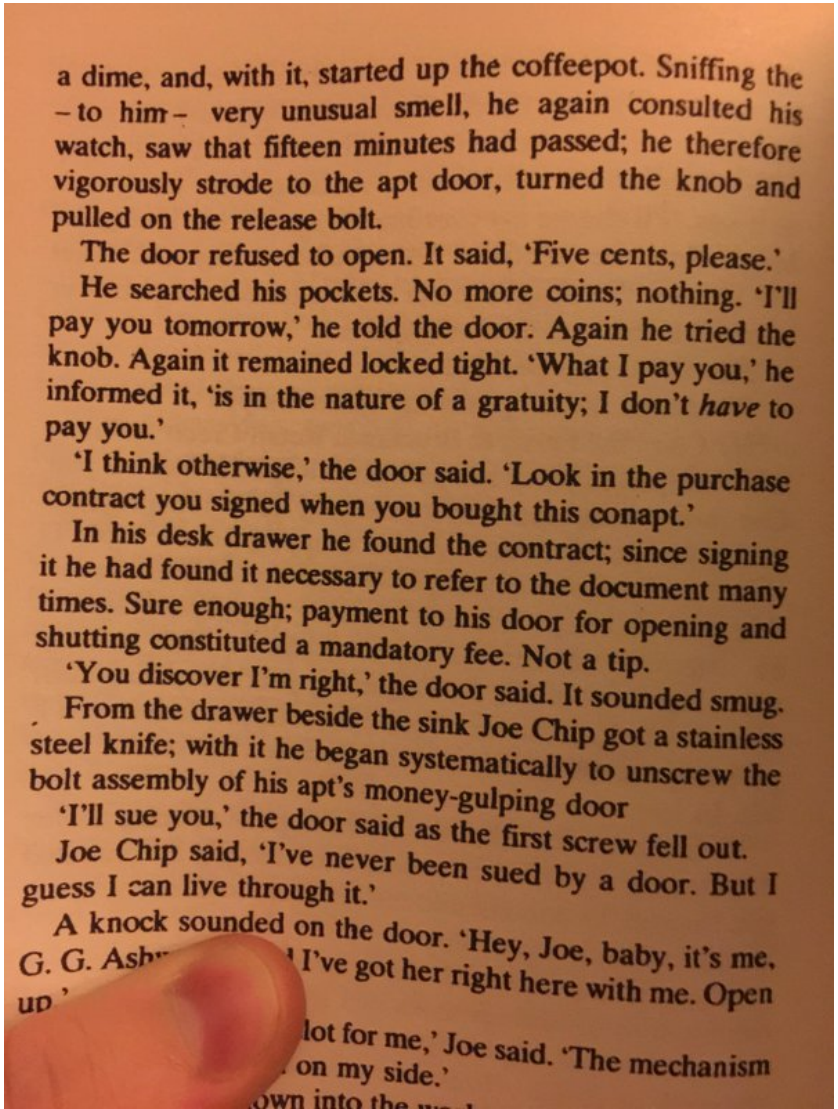
By CHANTE OWENS August 4, 2016

ANDY GREENBERG SECURITY 08.10.16 4:29 PM

A NEW WIRELESS HACK CAN UNLOCK 100 MILLION VOLKSWAGENS



Philip K Ubik (1969)



a dime, and, with it, started up the coffeepot. Sniffing the –to him– very unusual smell, he again consulted his watch, saw that fifteen minutes had passed; he therefore vigorously strode to the apt door, turned the knob and pulled on the release bolt.

The door refused to open. It said, 'Five cents, please.'

He searched his pockets. No more coins; nothing. 'I'll pay you tomorrow,' he told the door. Again he tried the knob. Again it remained locked tight. 'What I pay you,' he informed it, 'is in the nature of a gratuity; I don't *have* to pay you.'

'I think otherwise,' the door said. 'Look in the purchase contract you signed when you bought this conapt.'

In his desk drawer he found the contract; since signing it he had found it necessary to refer to the document many times. Sure enough; payment to his door for opening and shutting constituted a mandatory fee. Not a tip.

'You discover I'm right,' the door said. It sounded smug.

From the drawer beside the sink Joe Chip got a stainless steel knife; with it he began systematically to unscrew the bolt assembly of his apt's money-gulping door

'I'll sue you,' the door said as the first screw fell out.

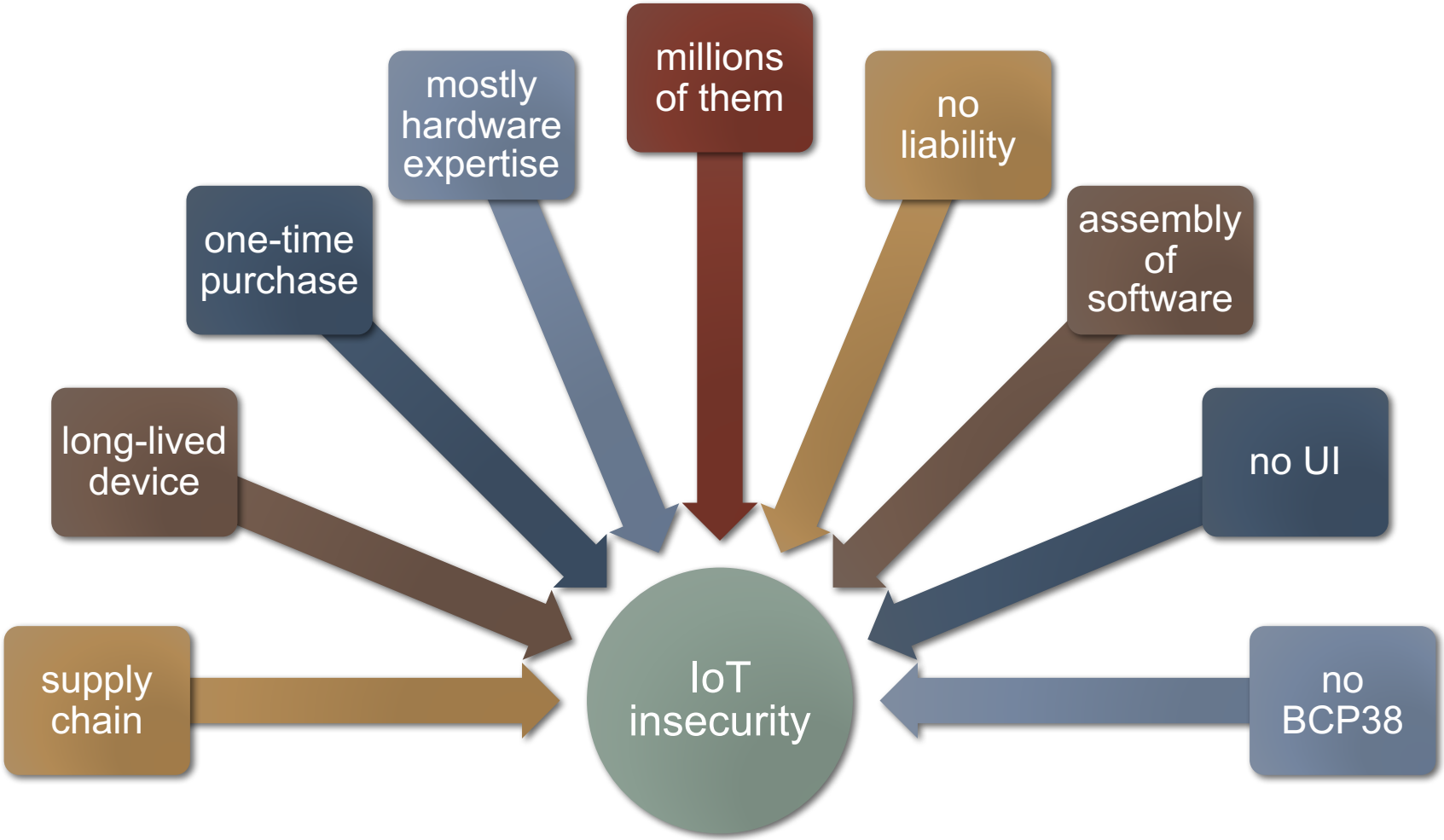
Joe Chip said, 'I've never been sued by a door. But I guess I can live through it.'

A knock sounded on the door. 'Hey, Joe, baby, it's me, G. G. Ash[illegible] I've got her right here with me. Open up.'

[illegible]lot for me,' Joe said. 'The mechanism [illegible] on my side.'

[illegible]own into the

IoT security confluence



Long supply chain

Manufacturing process

RomPager 4.07

- Dated to 2002
- Appears in many new firmwares

- 2,249,187 devices on port 80
- 11,328,029 devices on port 7547

Port 7547 Analysis

- TR-069 - ~45m
  - 100% IoT

L. Oppenheim & S. Tal
CCC Congress 2014

Port 80: more than *.com

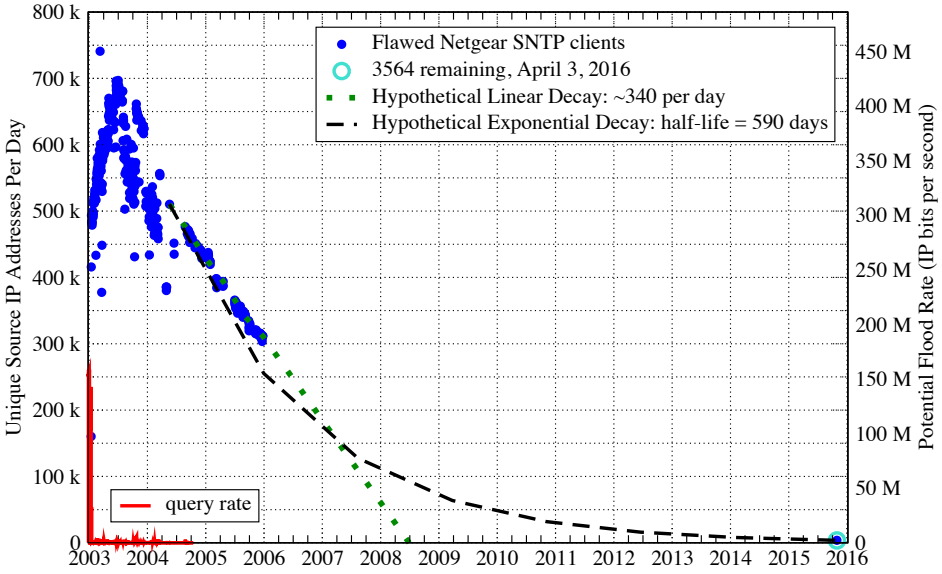
Port 80 Analysis

- Port 80 - ~70m
  - 50% Web Servers
  - 50% IoT things
    - Routers
    - Webcams
    - VoIP Phones
    - Toasters

- usually updated
- usually managed
- in a smallish number of locations

L. Oppenheim & S. Tal
CCC Congress 2014

Ghost traffic

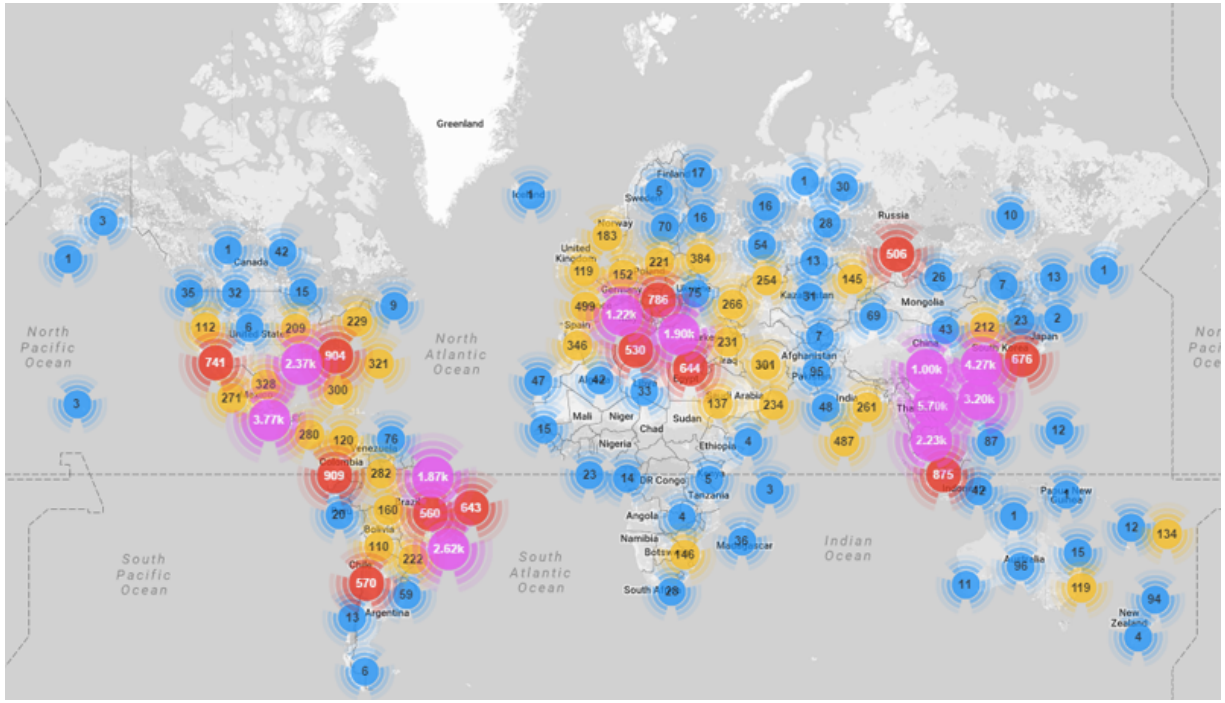


> Subsequently, we determined the sources of this flooding to be hundreds of thousands of real Internet hosts throughout the world. The root causes were serious flaws in the design of Netgear's low-cost Internet products targeted for residential use. Specifically, this unwanted traffic was traced to four models of residential broadband and wireless routers, which were found to have at least two problems. First, the University of Wisconsin's NTP server IP address was embedded in the firmware and was not configurable by the end user. Second, when these flawed devices do not receive a response to their Simple Network Time Protocol (SNTP [7]) queries, they retry continually at *one second* intervals.

"The Internet of Things Old and Unmanaged"
Plonka & Boschi, *IAB IoTSU workshop*, 2016

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

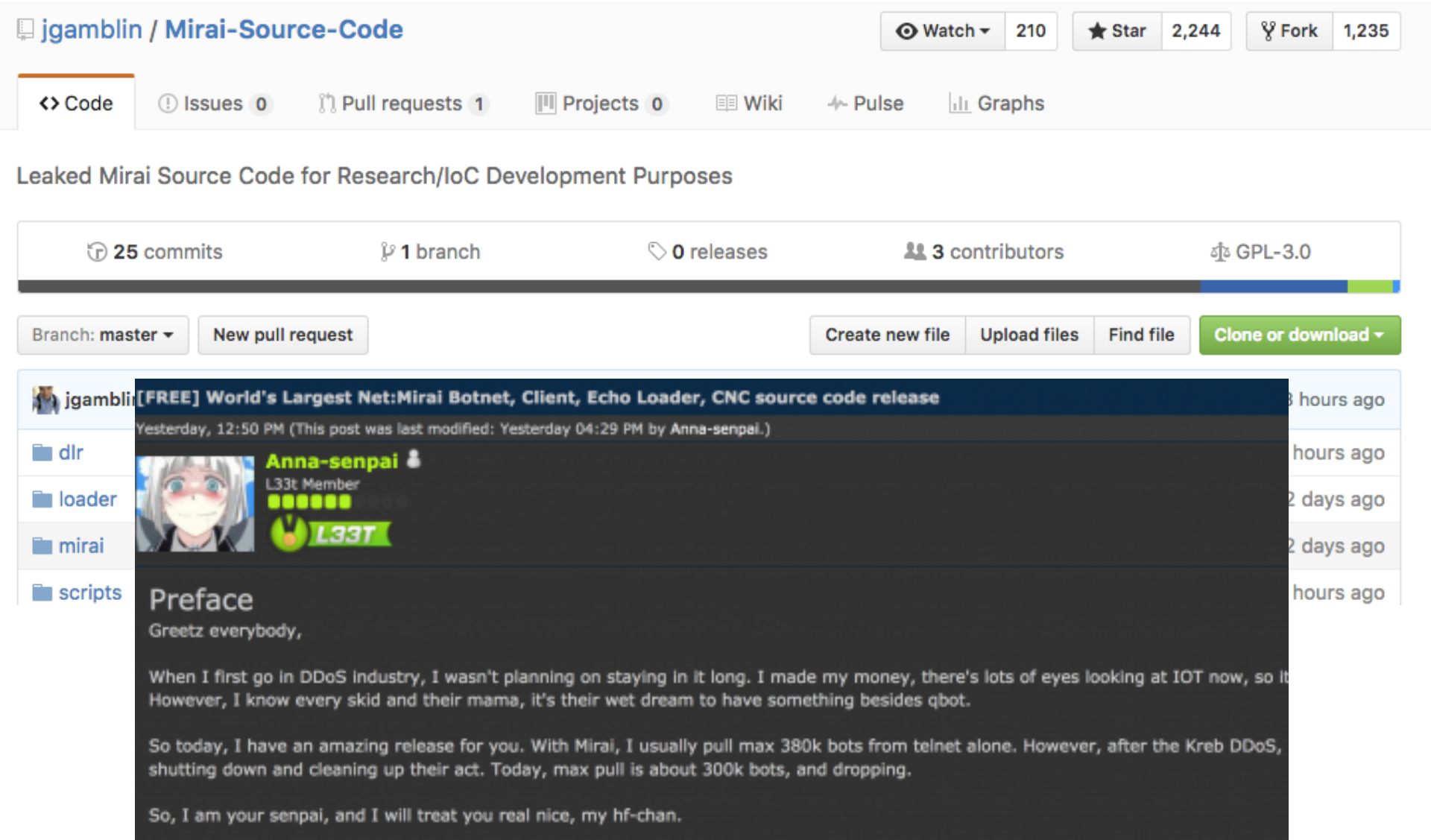


xc3511 vizxv
admin 888888
xmhdipc
default
123456 54321
support

Mirai botnet

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

Mirai source code available 09/30/2016



Attack time line

Attack Timeline

Starting at approximately 7:00 am ET, Dyn began experiencing a DDoS attack. While it's not uncommon for Dyn's Network Operation Center (NOC) team to mitigate DDoS attacks, it quickly became clear that this attack was different (more on that later). Approximately two hours later, the NOC team was able to mitigate the attack and restore service to customers. Unfortunately, durin that time, internet users directed to Dyn servers on the East Coast of the US were unable to reach some of our customers' sites, including some of the marquee brands of the internet. We should note that Dyn did not experience a system-wide outage at any time – for example, users accessing these sites on the West Coast would have been successful.

After restoring service, Dyn experienced a second wave of attacks just before noon ET. This second wave was more global in nature (i.e. not limited to our East Coast POPs), but was mitigated in just over an hour; service was restored at approximately 1:00 pm ET. Again, at no time was there a network-wide outage, though some customers would have seen extended latency delays during that time.

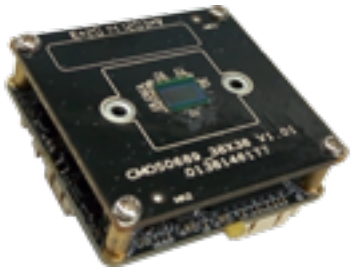
News reports of a third attack wave were verified by Dyn based on our information. While there was a third attack attempted, we were able to successfully mitigate it without customer impact.

Hangzhou Xiongmai Technology

"Idle boast the strong pass is a wall of iron, with firm strides we are crossing its summit."

Hangzhou Xiongmai Technology Co.,Ltd concentrates on security surveillance ,Video intelligent research and development. We devote ourselves to providing good products, technical services for manufacturers, wholesaler and service provider , in order to offer better experience for our customers. We are global leading providers in security video products and technology. Established from 2009, many years development, the headquarter of XM locate in Yinhu Innovation Center, Fuyang district, Hangzhou now. Total registered capital reach to 60 million. Now we owns nearly 2000 employees including a strong R&D team (more than 300 experienced engineers). Besides,we owns more than 100 acres which contained owned or leased offices, more than 80000 square meters in total.

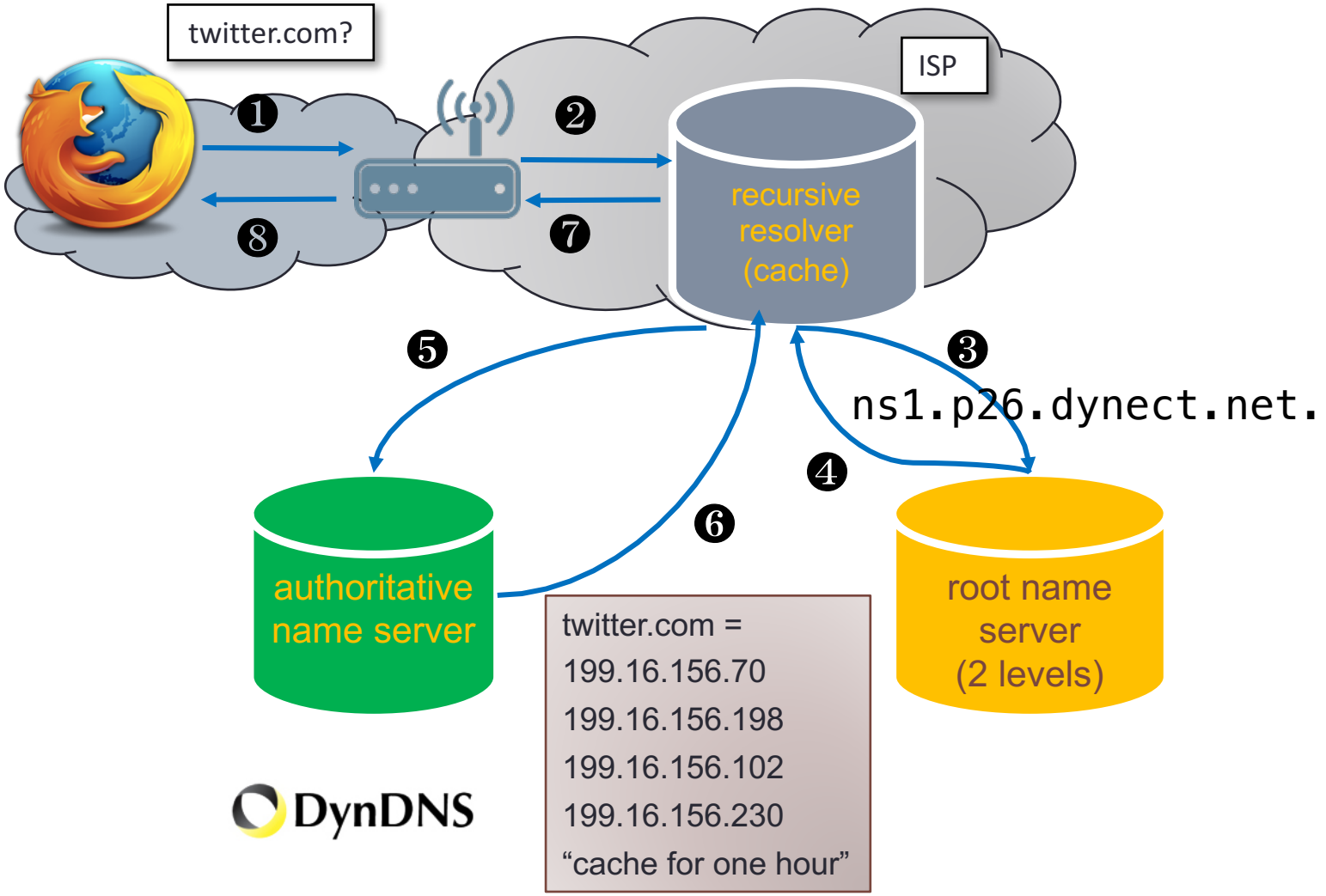
Our business mainly involves in security monitoring module, main board, supporting software and product solutions which contains AHD models as well as its motherboards, network HD models as well as its motherboards, AHD/network integration movements, automatic focusing modules, QQ content couplet modules , CMS, VMS, SNVR, MYEYE monitoring platform software, cloud services and so on. Since Xiongmai was founded in 2009, we always pay close attention to products.we demand quality strives to be perfect,so the product has high compatibility, high resolution, high cost-effective, high professionalism and experience. Now our products and solutions that provide services for security industries have been applied to the world.



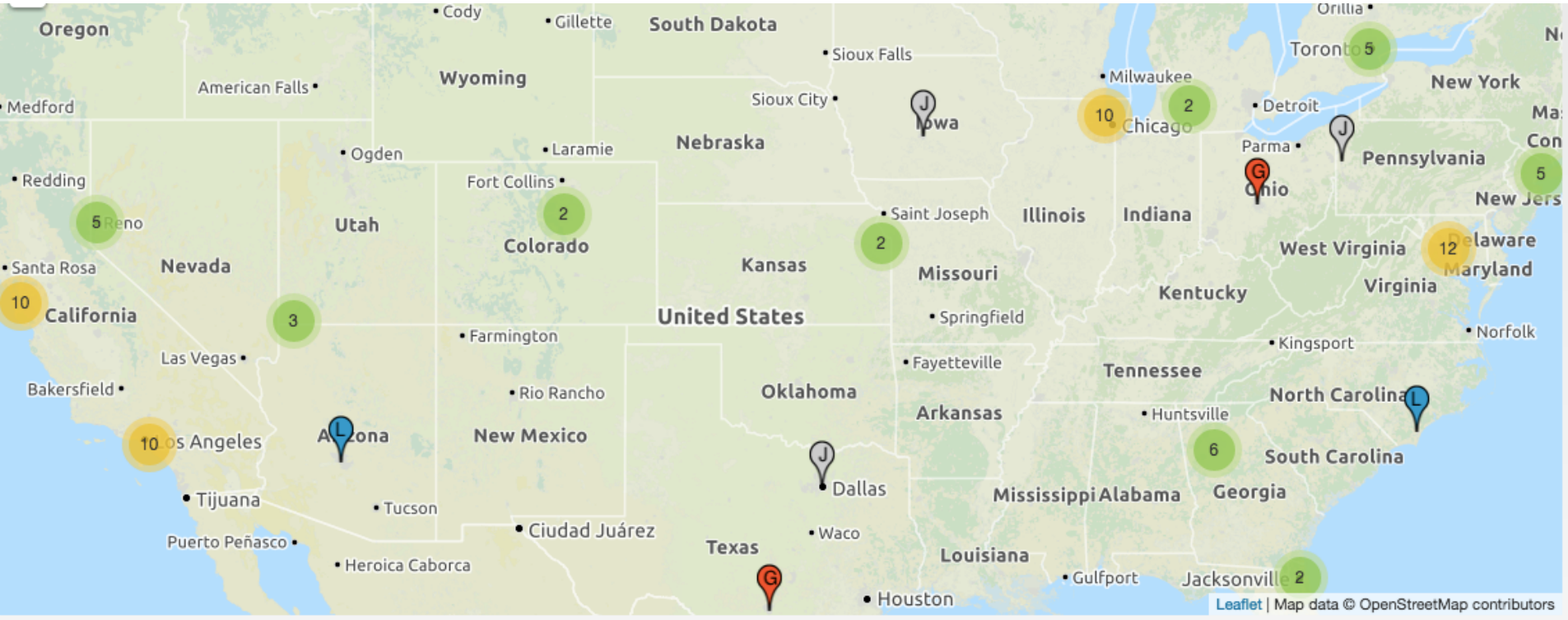
Dahua Security

Dahua Technology USA … total security solutions to the North American market …. With the world's second-largest market share …, Dahua's surveillance solutions … while demonstrating the company's commitment to video data security. … 3,000 R&D professionals that have developed 592 product patents. A leading name in video surveillance in China for more than 20 years ….

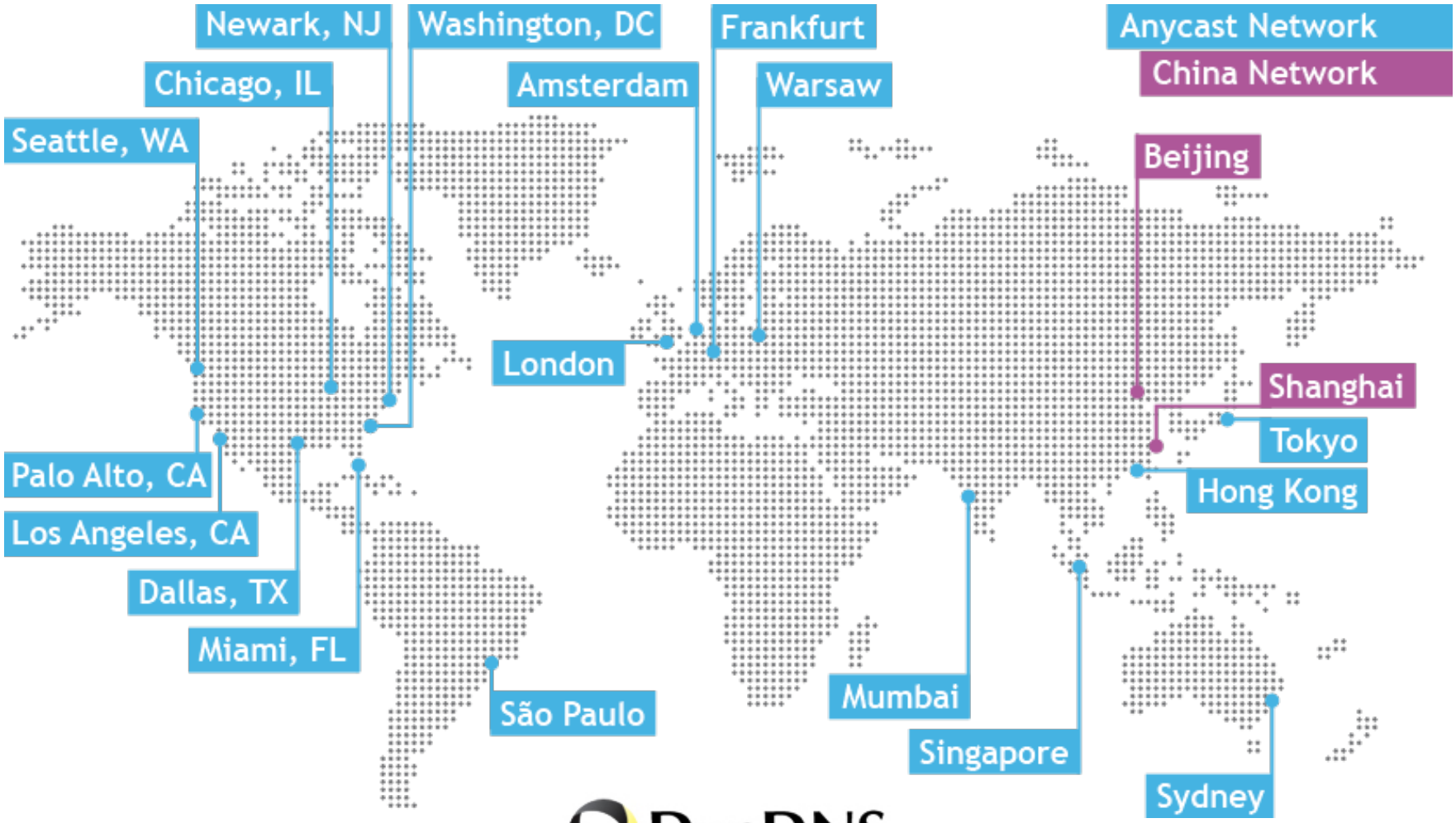
Background: DNS resolution



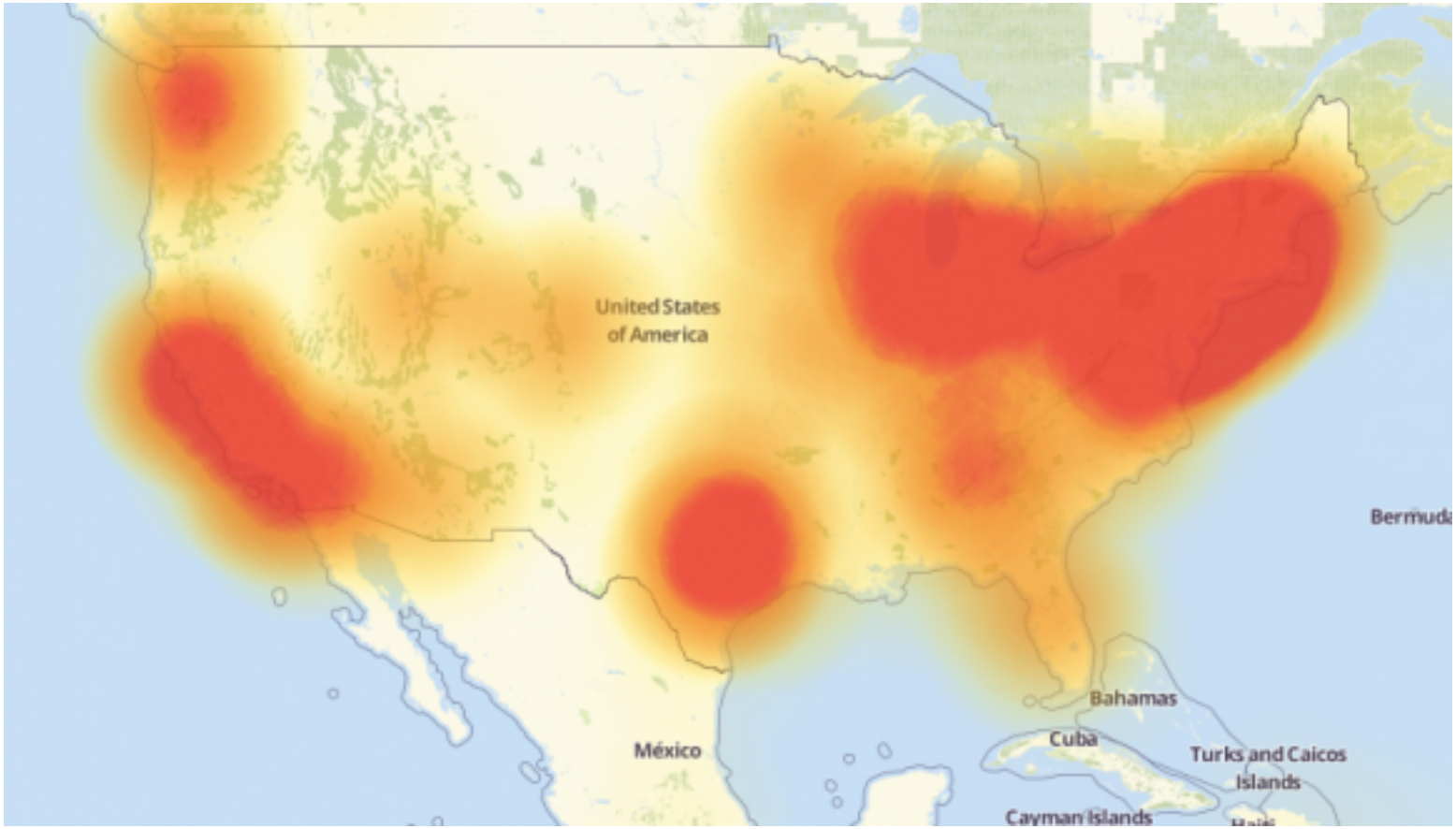
root-servers.org



Who is dynDNS?



Outage map Oct. 21 (downdetector.com)



Sites affected

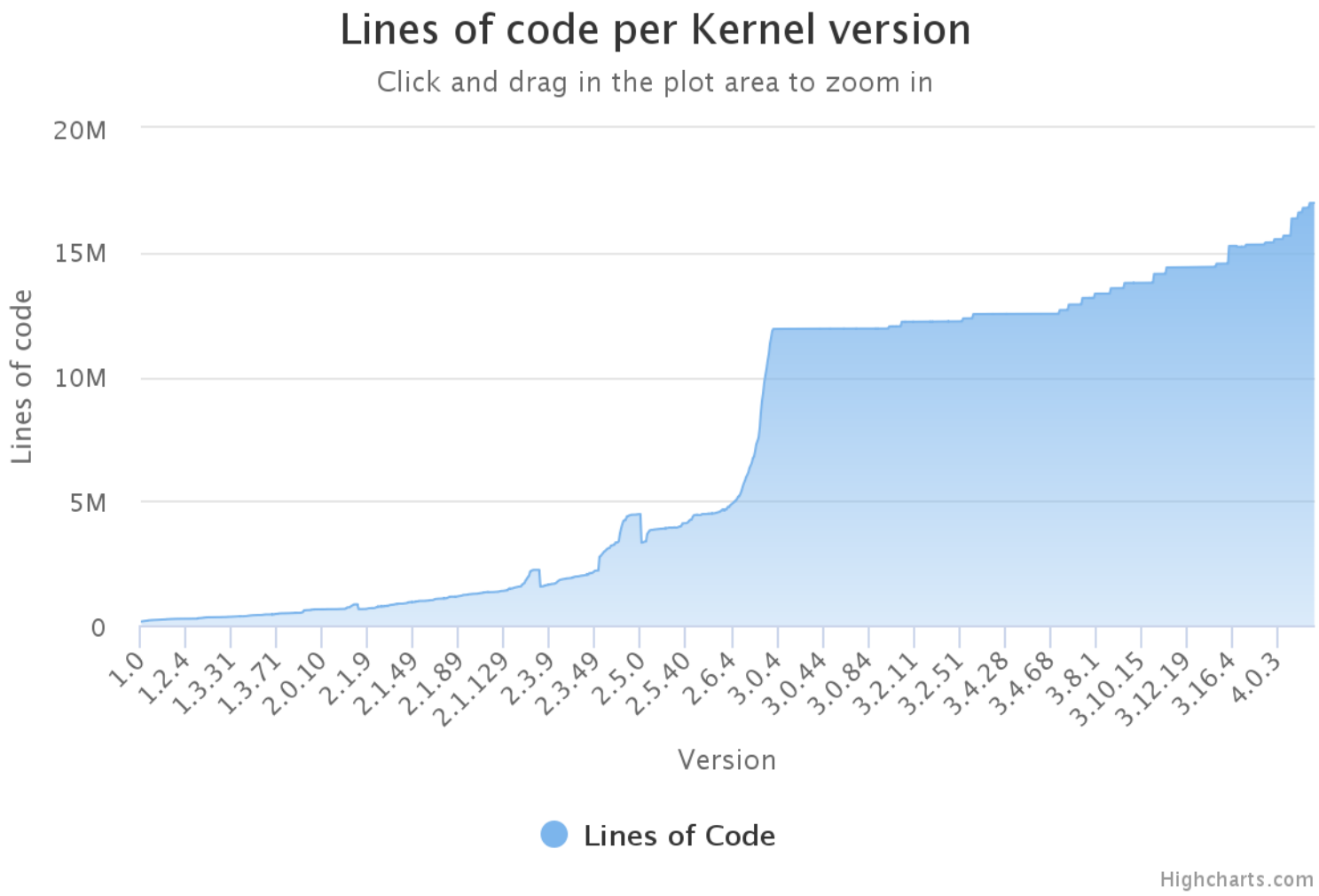
ActBlue
Basecamp
Big cartel
Box
Business Insider
CNN
Cleveland.com
Etsy
Github
Grubhub
Guardian.co.uk
HBO Now
Iheart.com (iHeartRadio)
Imgur
Intercom
Intercom.com
Okta
PayPal
People.com
Pinterest
Playstation Network
Recode

Reddit
Seamless
Spotify
Squarespace Customer Sites
Starbucks rewards/gift cards
Storify.com
The Verge
Twillo
Twitter
Urbandictionary.com (lol)
Weebly
Wired.com
Wix Customer Sites
Yammer
Yelp
Zendesk.com
Zoho CRM
Credit Karma
Eventbrite
Netflix
NHL.com
Fox News

Disqus
Shopify
Soundcloud
Atom.io
Ancestry.com
ConstantContact
Indeed.com
New York Times
Weather.com
WSJ.com
time.com
xbox.com
dailynews.com
Wikia
donorschoose.org
Wufoo.com
Genonebiology.com
BBC
Elder Scrolls Online
Eve Online
PagerDuty
Kayak

youneedabudget.com
Speed Test
Freshbooks
Braintree
Blue Host
Qualtrics
SBNation
Salsify.com
Zillow.com
nimbleschedule.com
Vox.com
Livestream.com
IndieGoGo
Fortune
CNBC.com
FT.com
Survey Monkey
Paragon Game
Runescape

Linux kernel lines of code



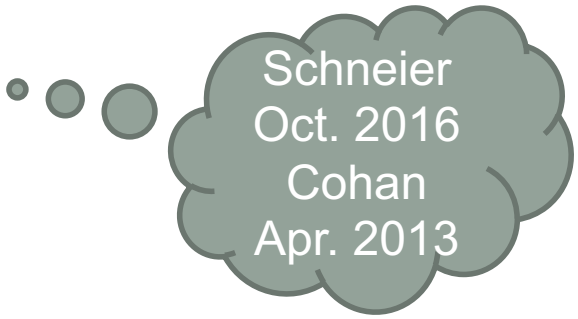
BusyBox:
177,650 SLOC

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



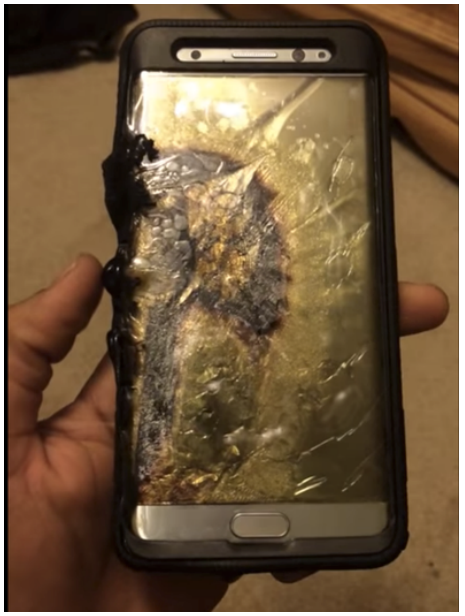
- DDOS as externality
  - device owners don't care:
    - barely slows down their Internet service
    - device still functions normally
    - don't know victims, generally
  - vendors don't care (enough)
    - not liable for damage (right now) – public nuisance?
    - only marginally affects their business 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

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

- 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 you really need to talk to strangers?
- 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!)

Windows XP, Corolla & Revolv

13 years

available 12/2001

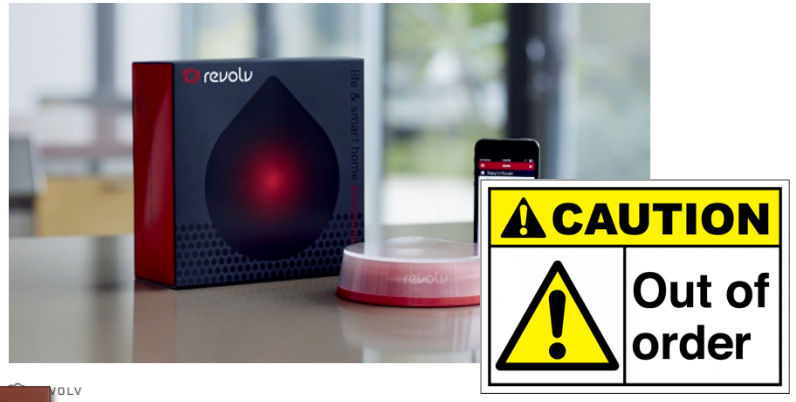
end of sales 6/2008

end support 4/2009

end install 10/2010

end ext. support 4/2014

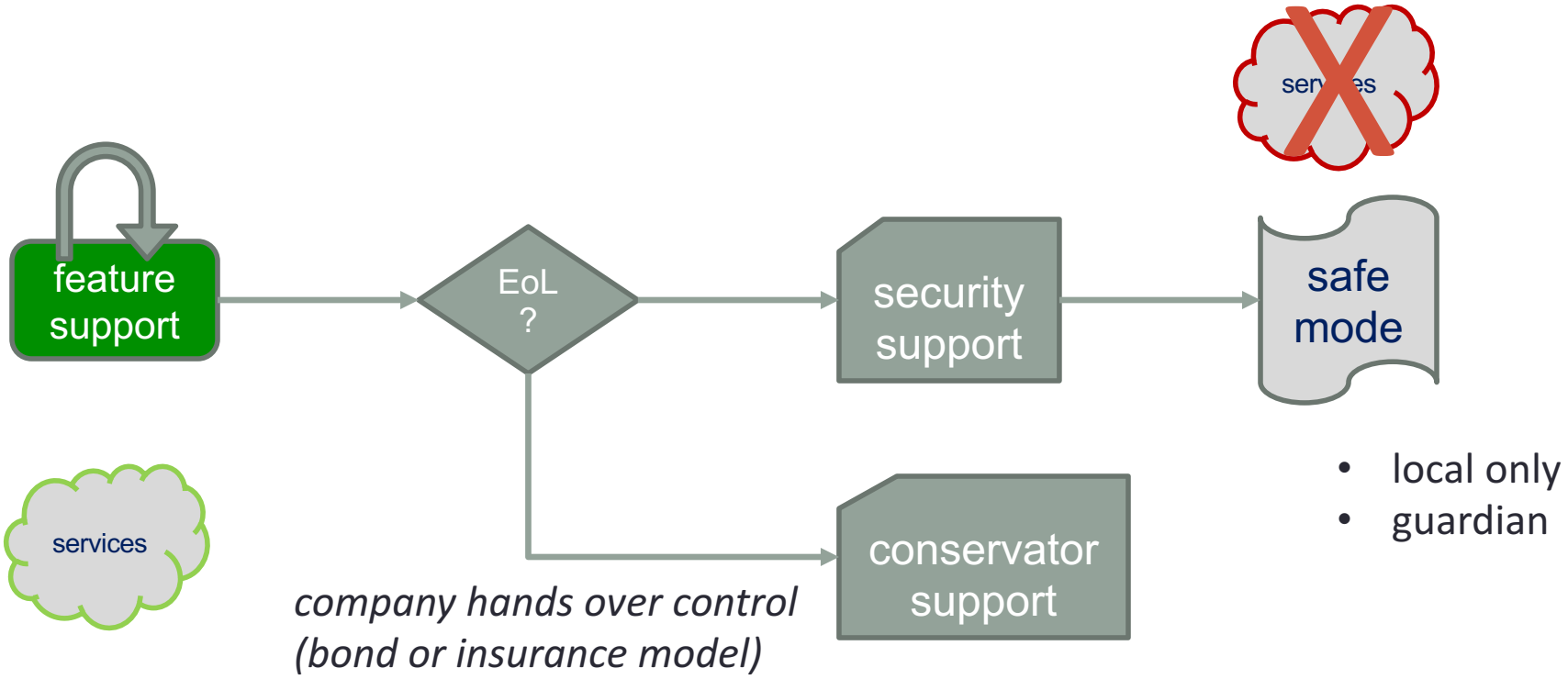
NEST'S HUB SHUTDOWN PROVES YOU'RE CRAZY TO BUY INTO THE INTERNET OF THINGS



founded 2012
acquired by Nest 2014
shut down May 2016

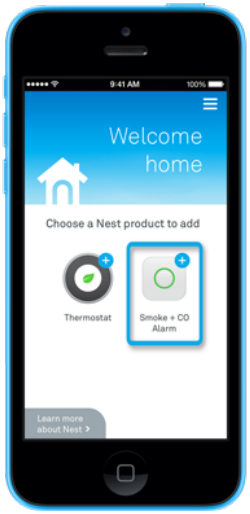
IF YOU WERE one of the people who shelled out $300 for Revolv's smart home hub, you've probably already heard the bad news: the web service that powers the little gadget is shutting down next month, which will render the thing effectively useless.

IoT needs a life cycle model

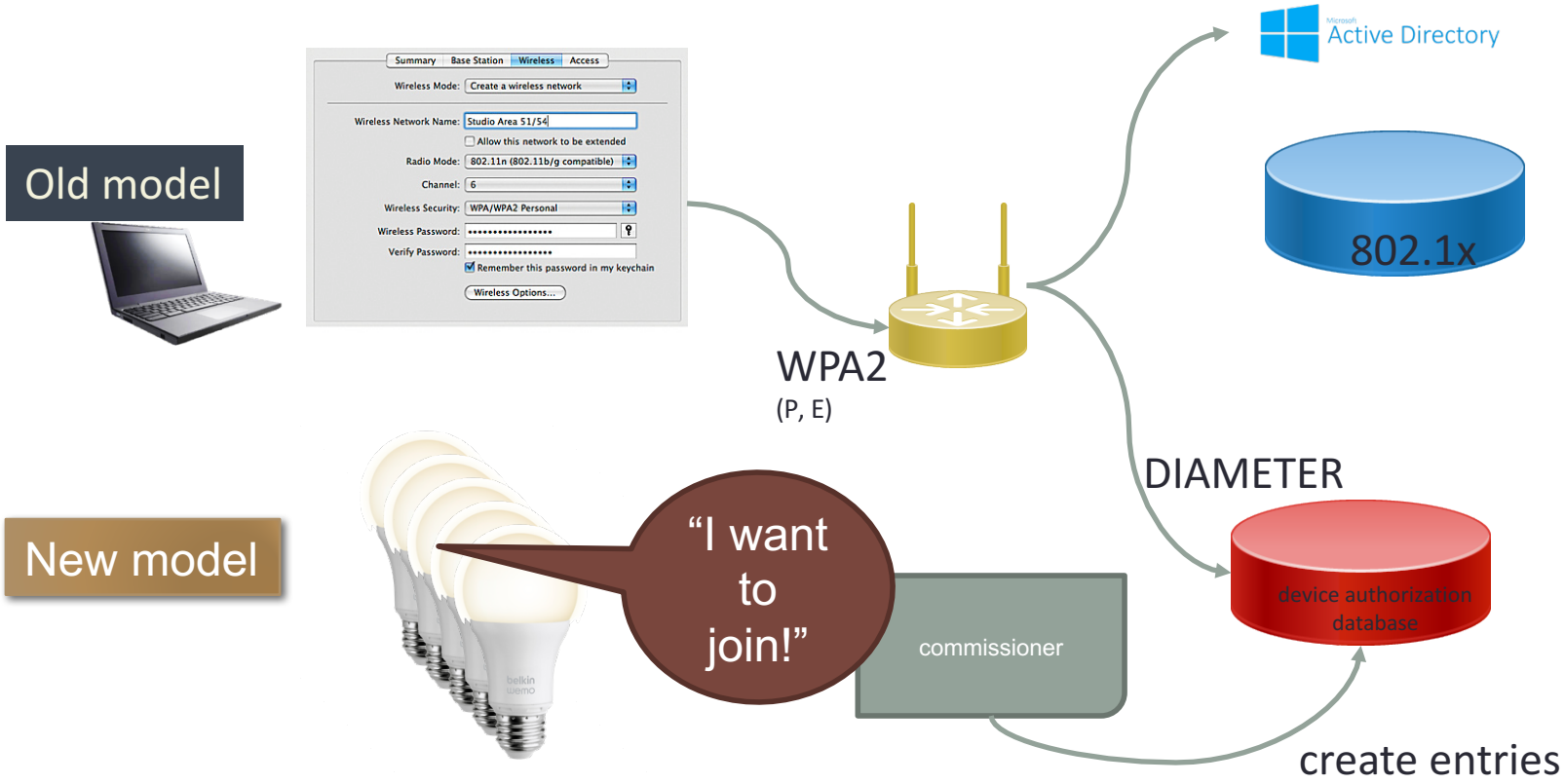


Challenge: enrollment

- 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?



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.

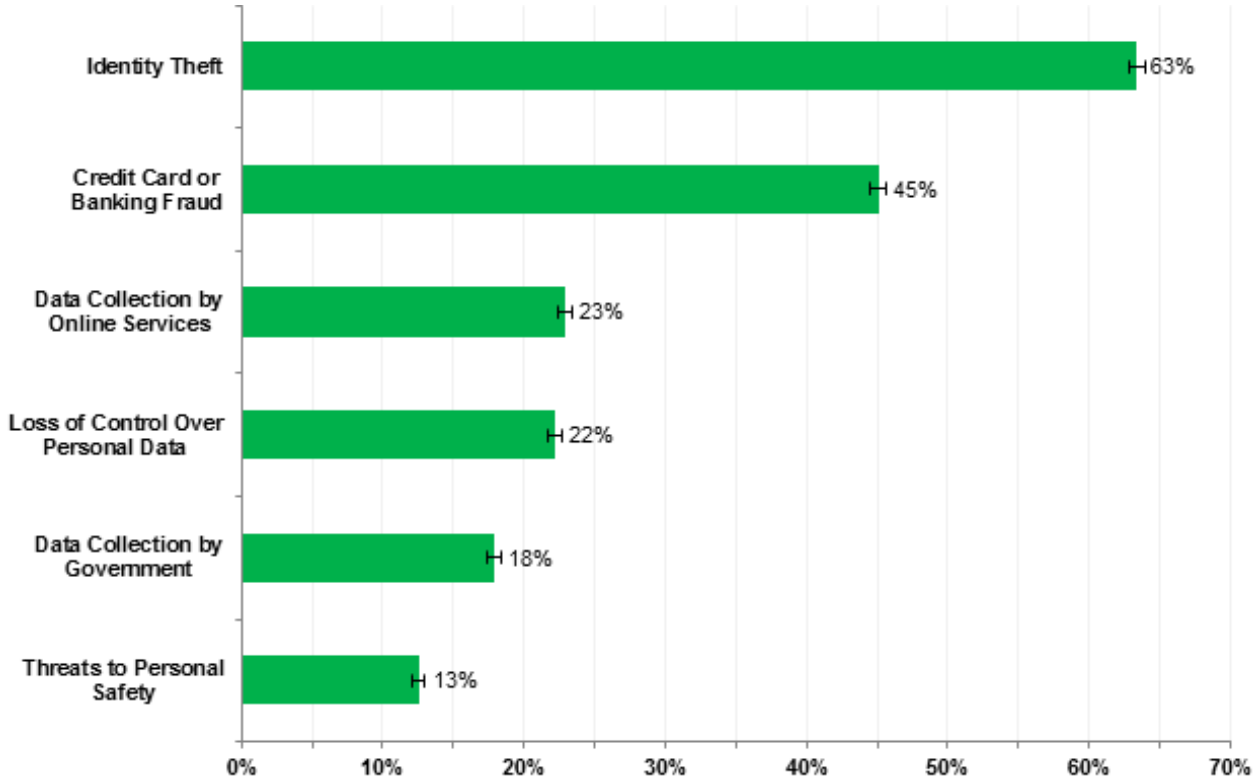
4. Switch to target Wi-Fi network

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

PRIVACY

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

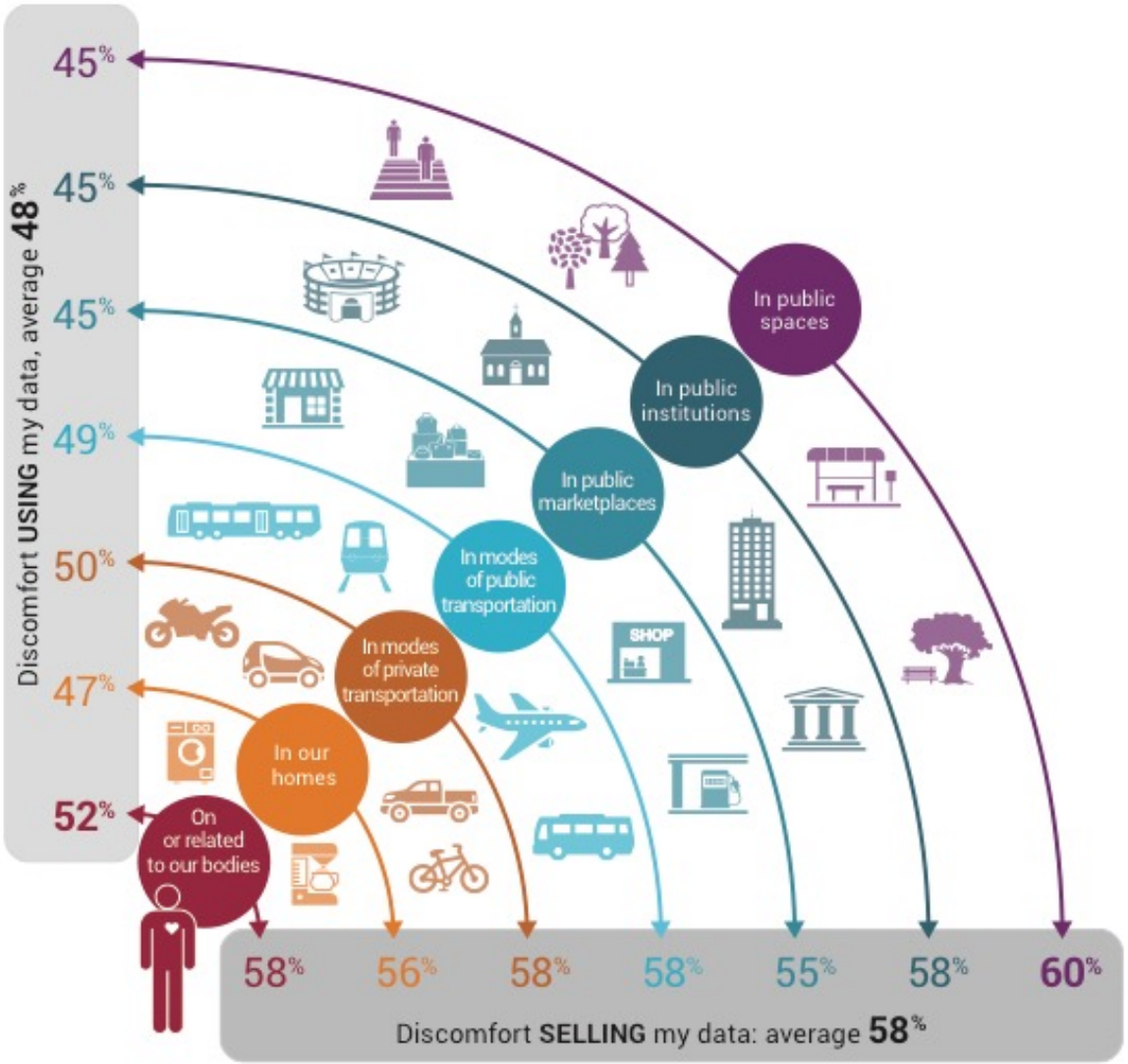
Privacy fears deter usage



NTIA
May 2016

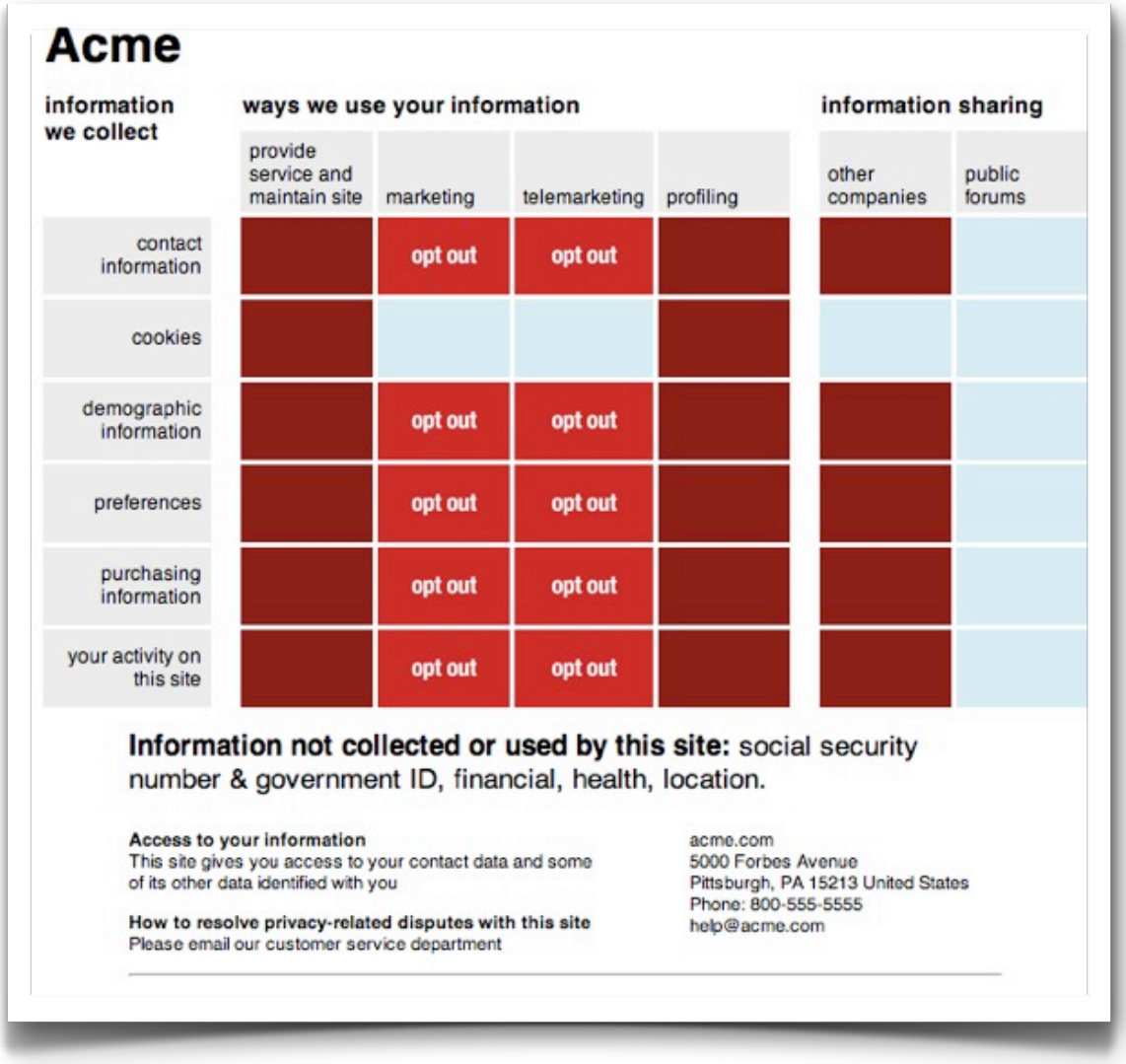
Major Concerns Related to Online Privacy and Security Risks, Percent of Households with Internet Users, 2015

Roughly half of consumers uncomfortable



Altimeter Group
June 2015

Privacy label?



Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
preferences		opt out	opt out			
purchasing information		opt out	opt out			
your activity on this site		opt out	opt out			

Information not collected or used by this site: social security number & government ID, financial, health, location.

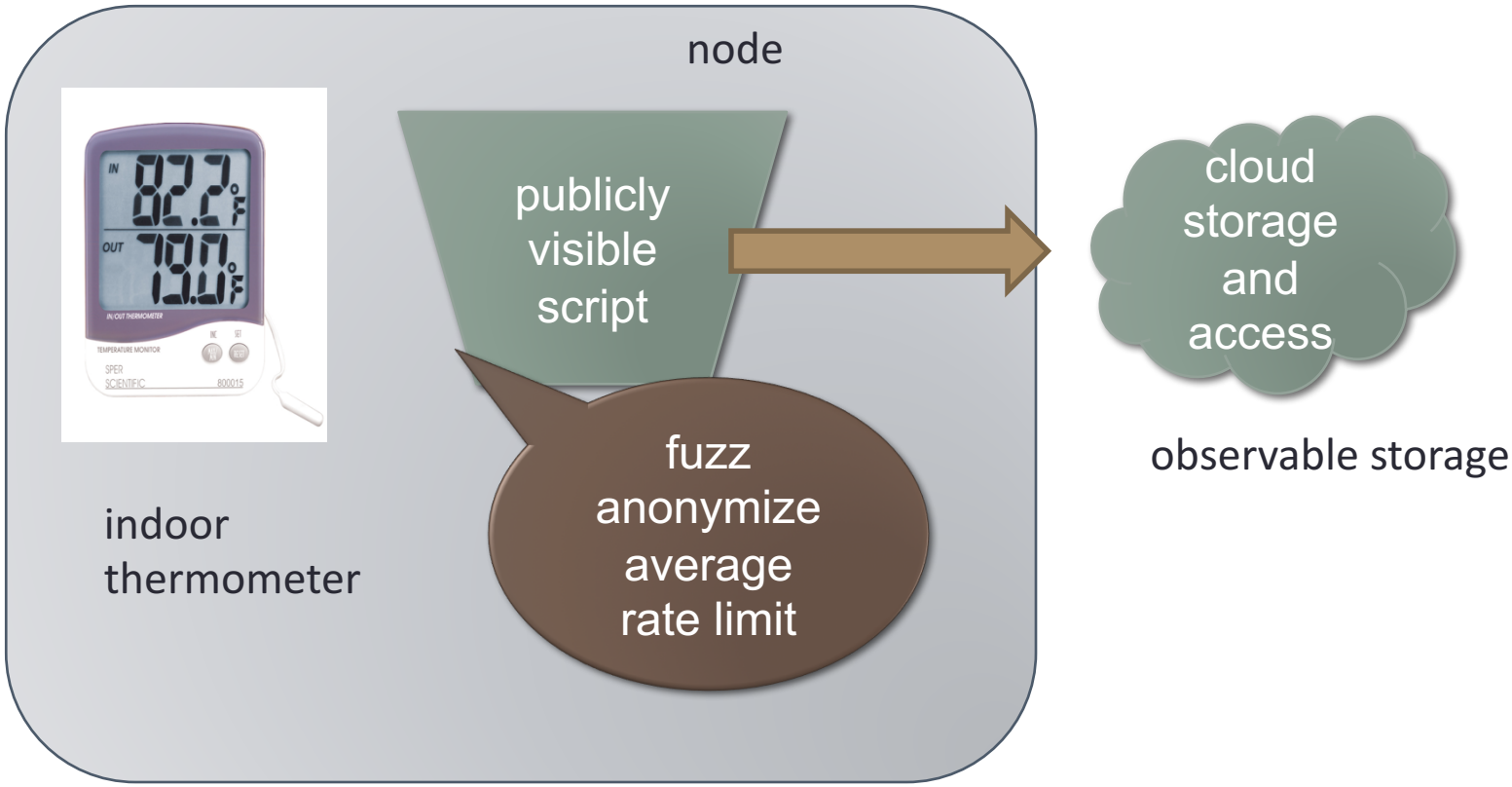
Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

P. Kelley et al.
SIGCHI 2010

Local processing for ~~efficiency~~ privacy



fog computing model

BUILDING LARGE IOT SYSTEMS

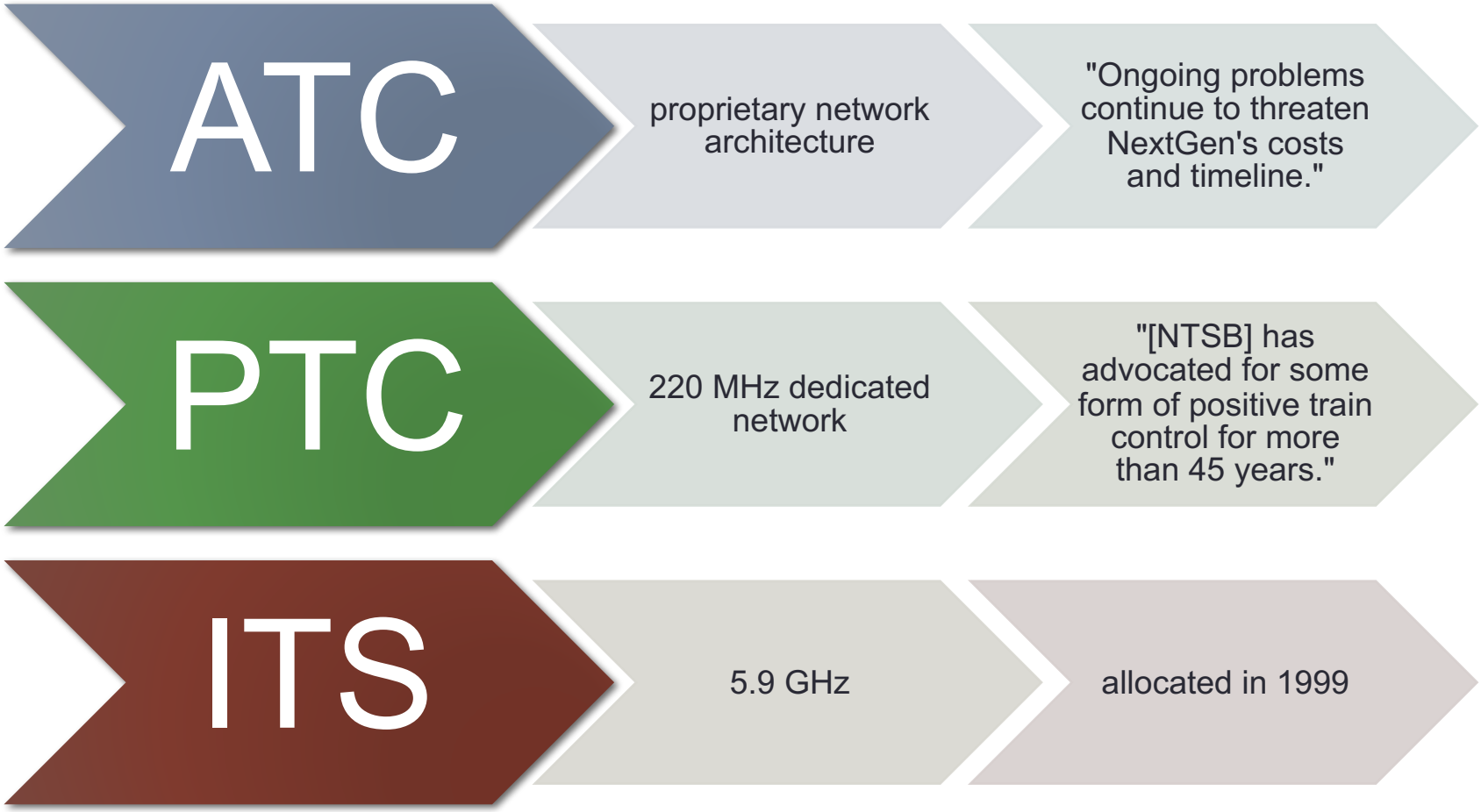
IoT = Internet at scale

- *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)



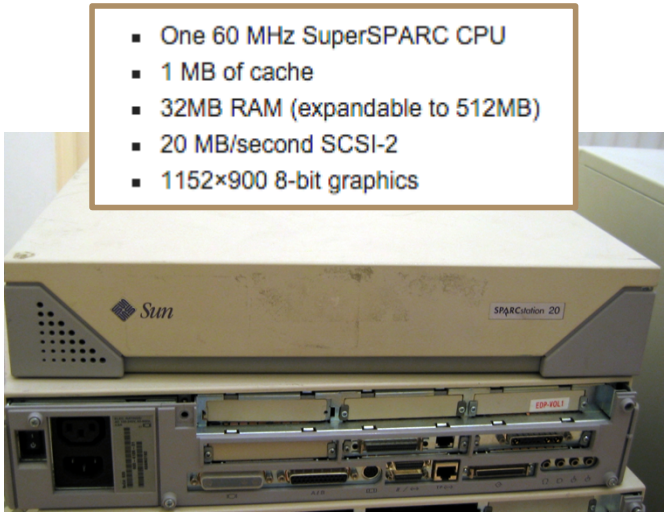
Lesson: sensor networks may be (tiny) niche

- 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

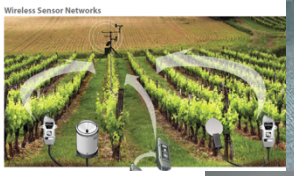


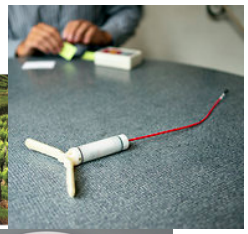
http://eschatologist.net/blog/?p=266

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

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?

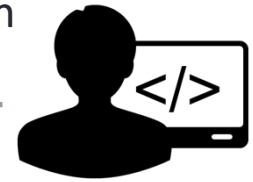
SENML?
LWM2M?

cloud, fog, …

SQL (via HTTP RESTful API)

Streaming (JSON web stream … RT

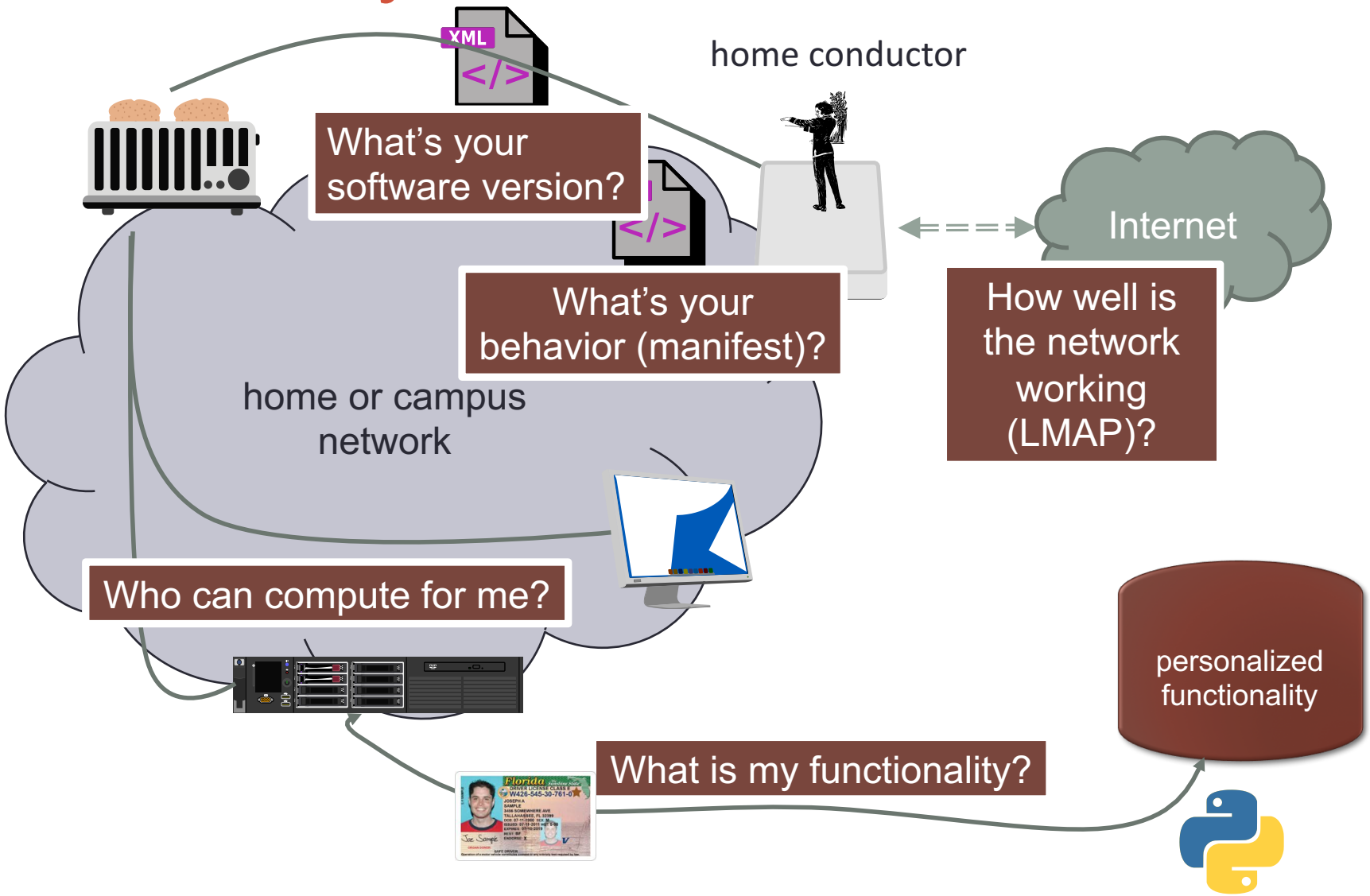
event notification



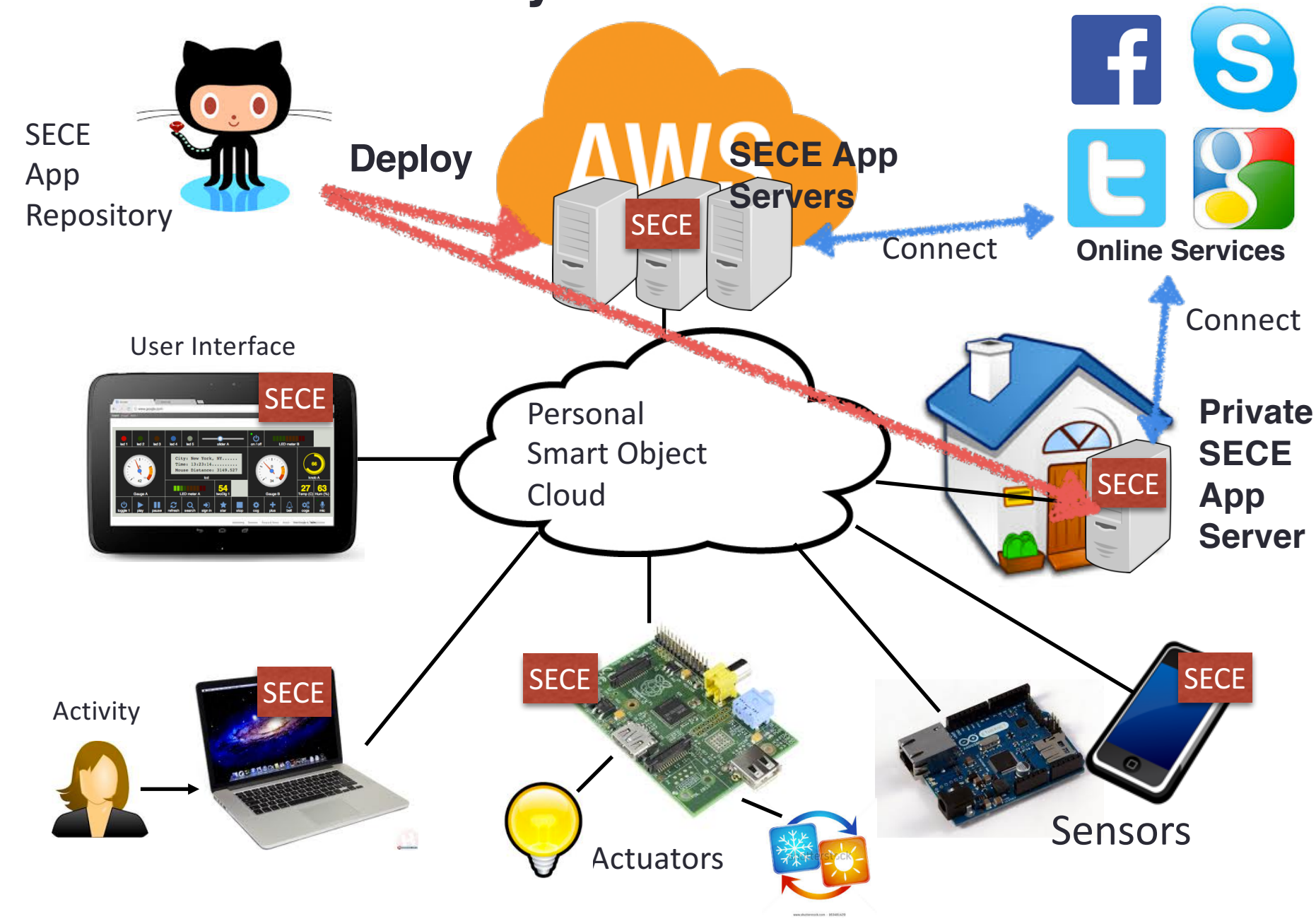
mediate access

user-delivered code

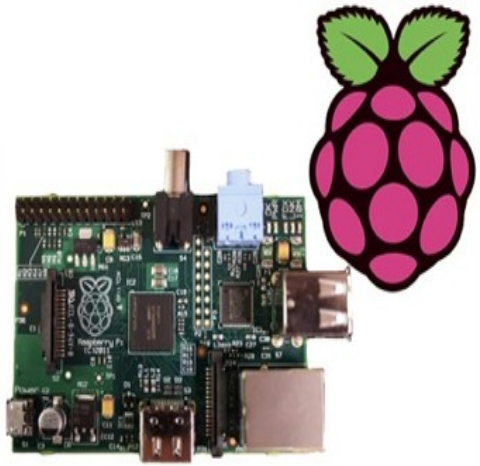
With security added in



SECE System Architecture



Challenge: integrate embedded, mobile & virtual



magnetometer
accelerometer
location
gyroscope

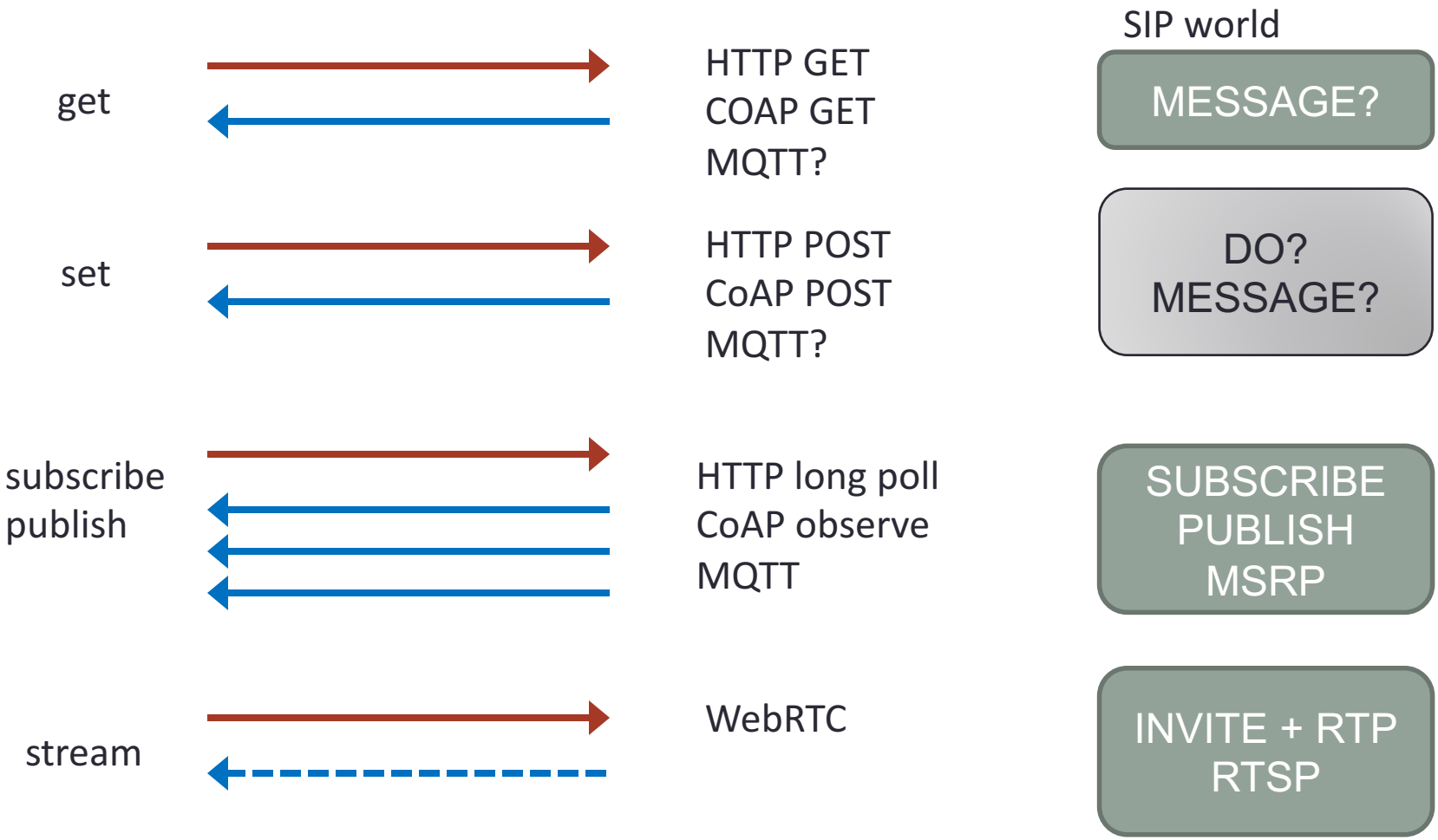
Some of IoT is streaming

Protocols

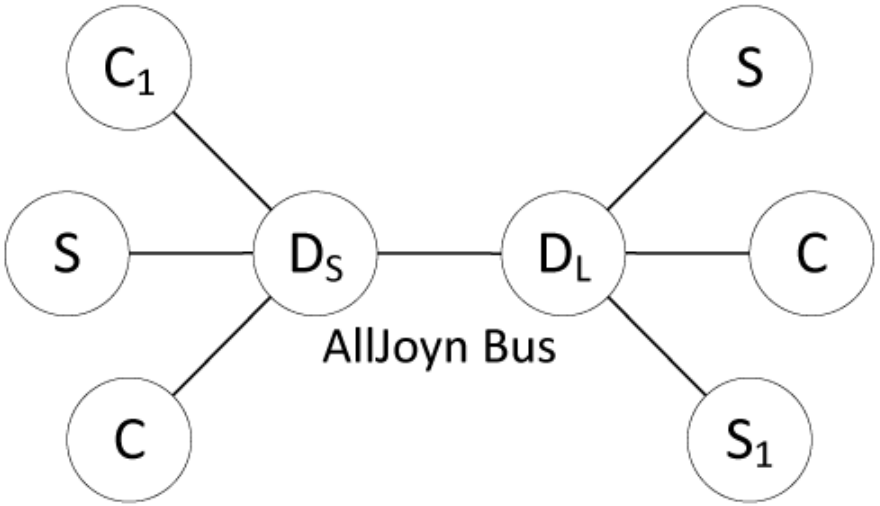
TCP/IP, DHCP, SMTP, DNS, RTSP, RTCP, RTP, HTTP, TCP, UDP, STUN, TURN, XMPP, uPNP, SNTP, IPv4, ICMP, Bonjour, SUNAPI

update rate of 10 to 250 Hz

IoT communication modalities

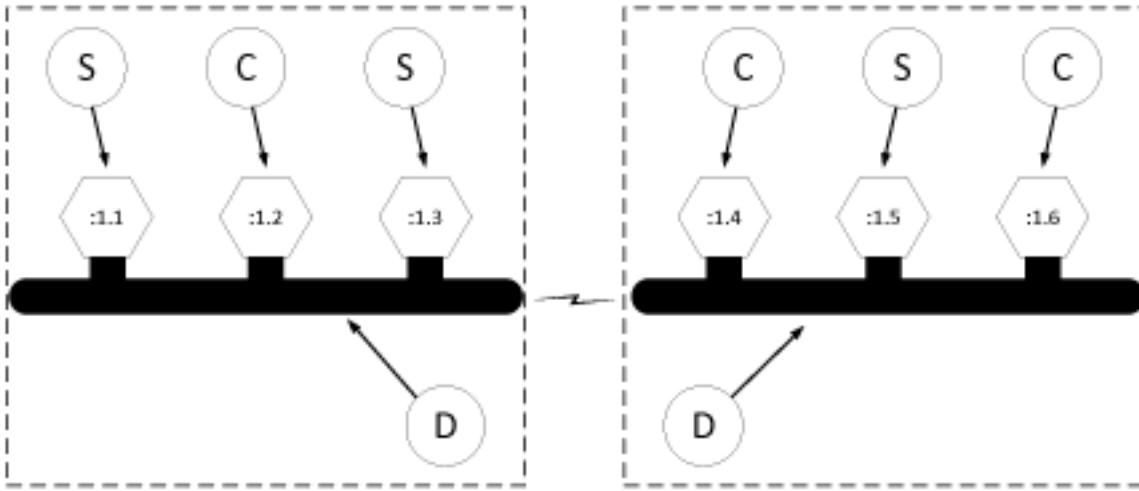


Example: AllJoyn bus



publish-subscribe model (implicit)

Wi-Fi
UDP multicast
BT SDP

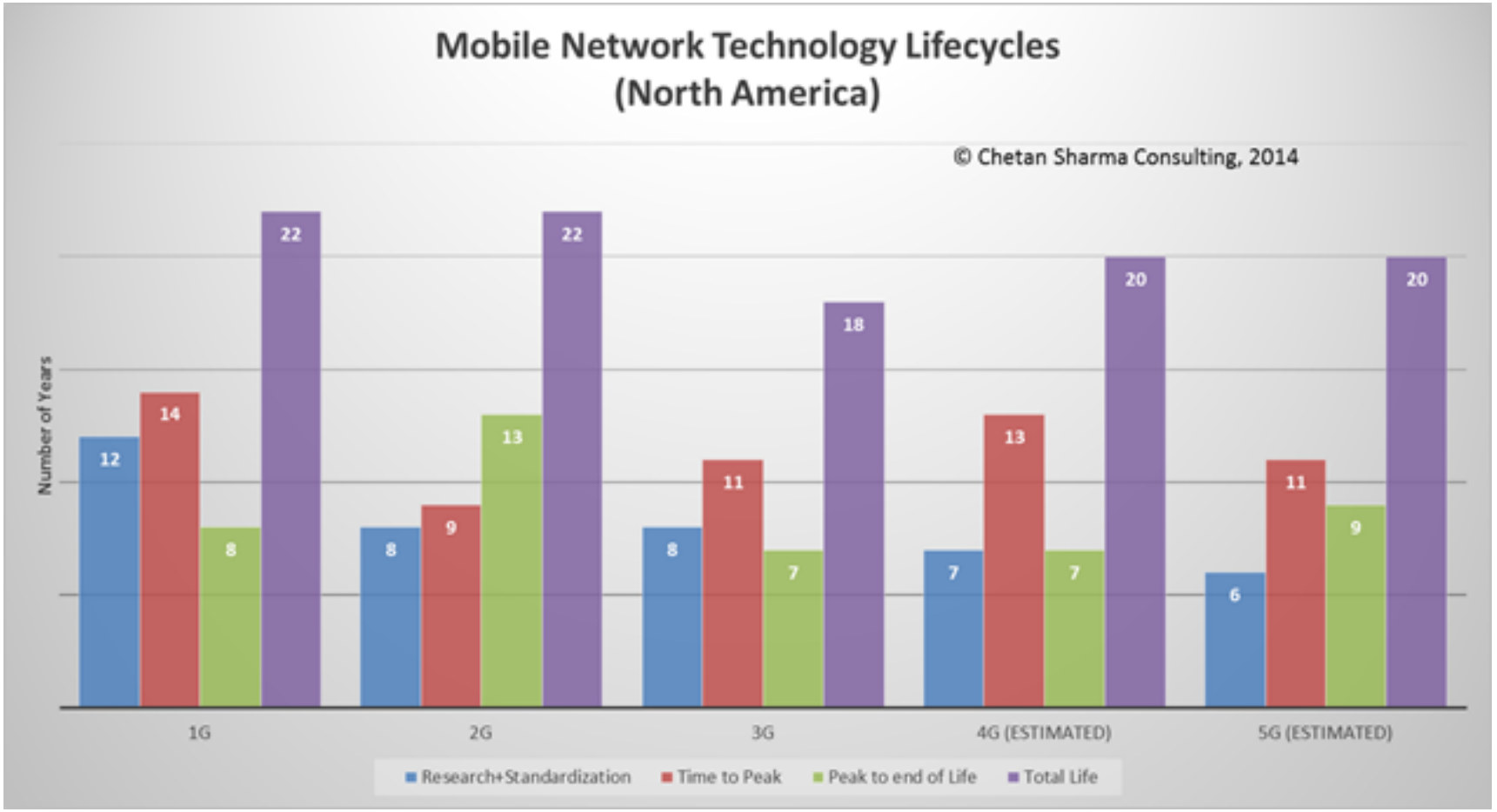


We could do better

- 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

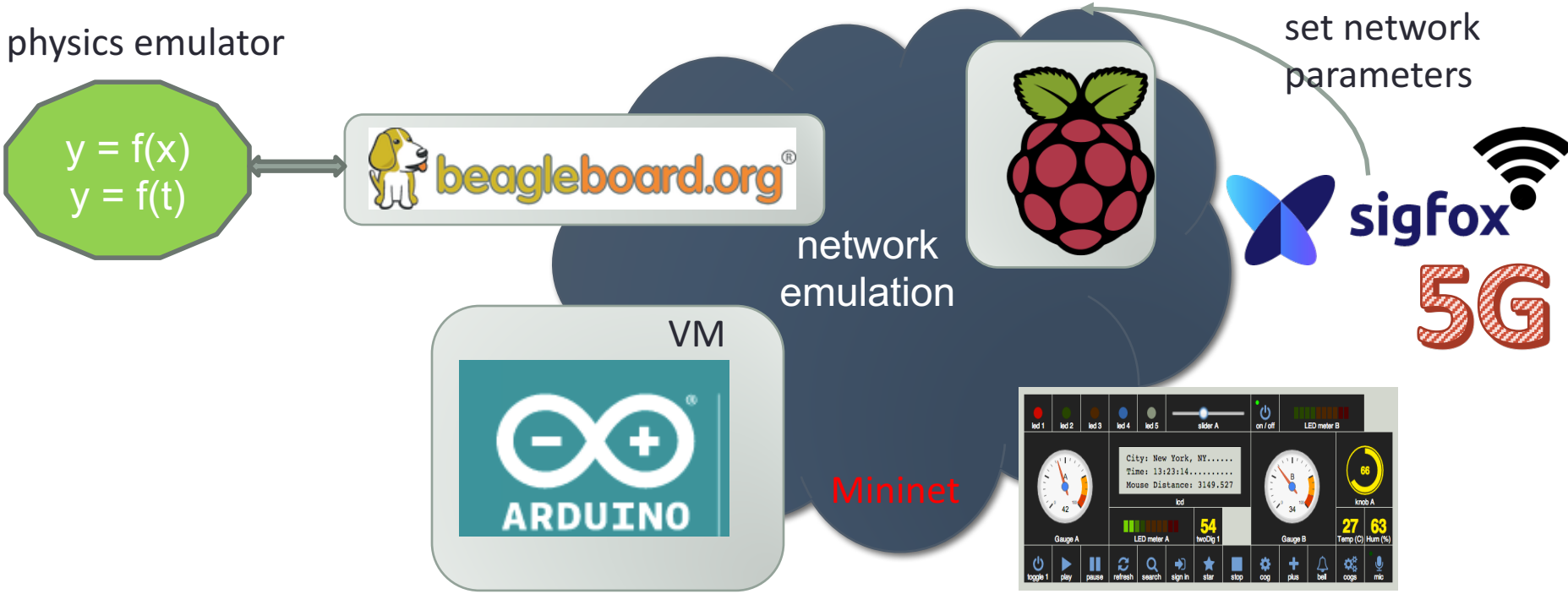
LIFECYCLE

Design for 20 years



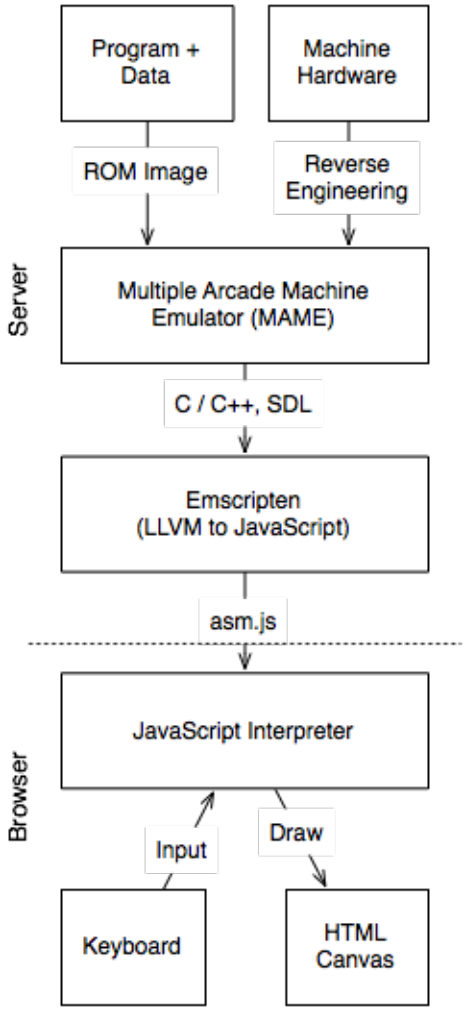
Development lifecycle

- Currently, hard to design large-scale reliable systems
  - failure modes, server load, control algorithms, …



http://mininet.org/

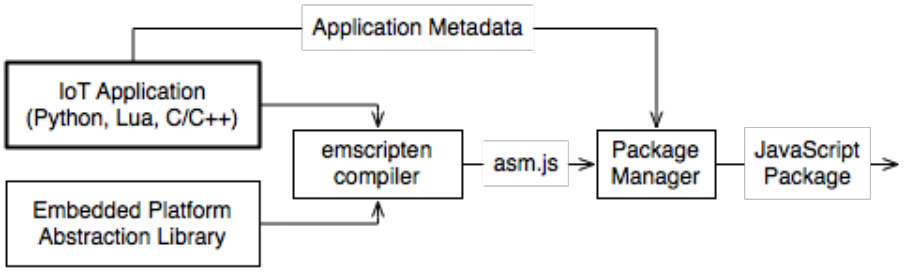
JavaScript IoT Device Emulation



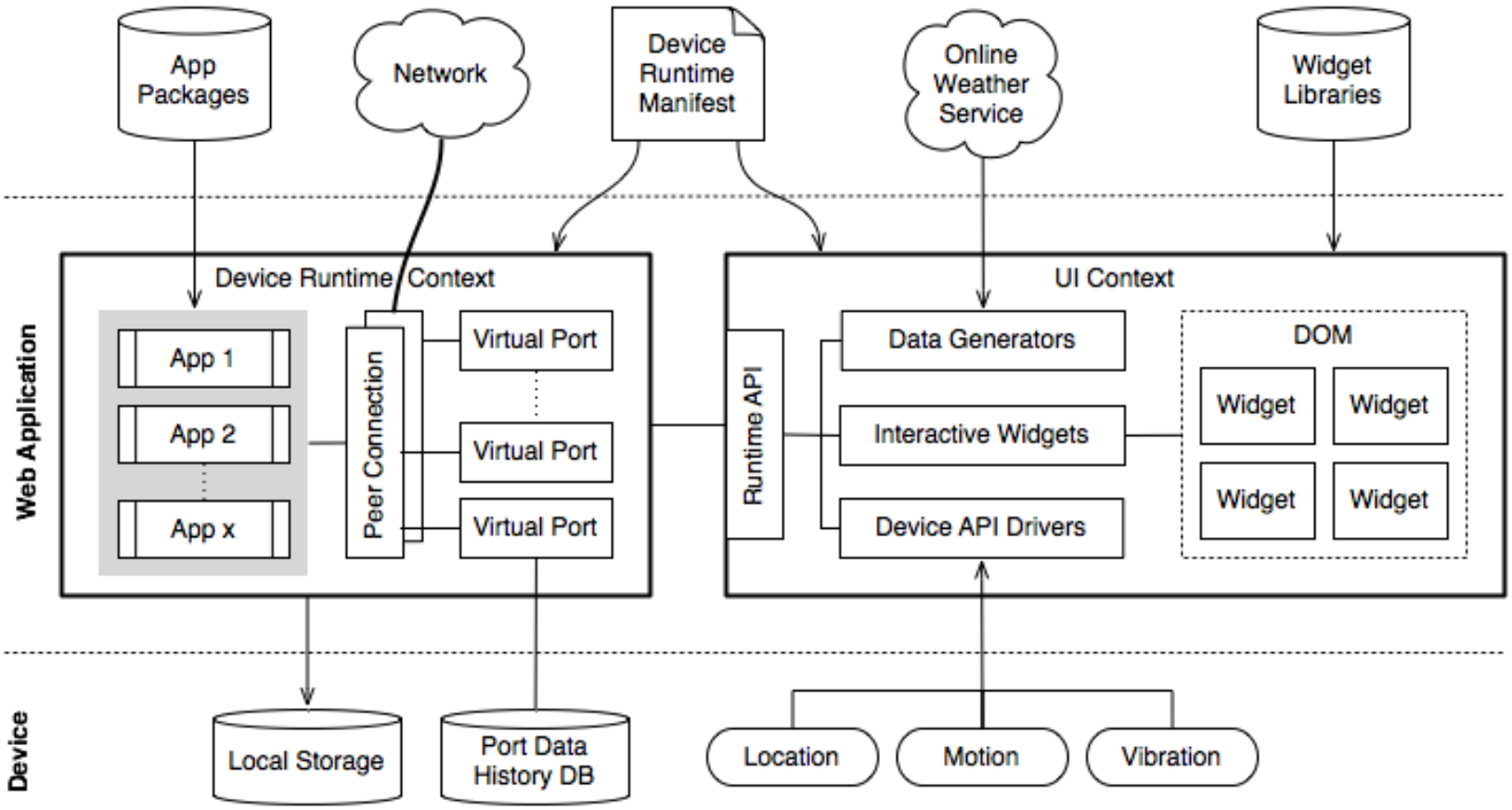
Internet Arcade

Work in Progress

IoT Devices



SECE JS Framework



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

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