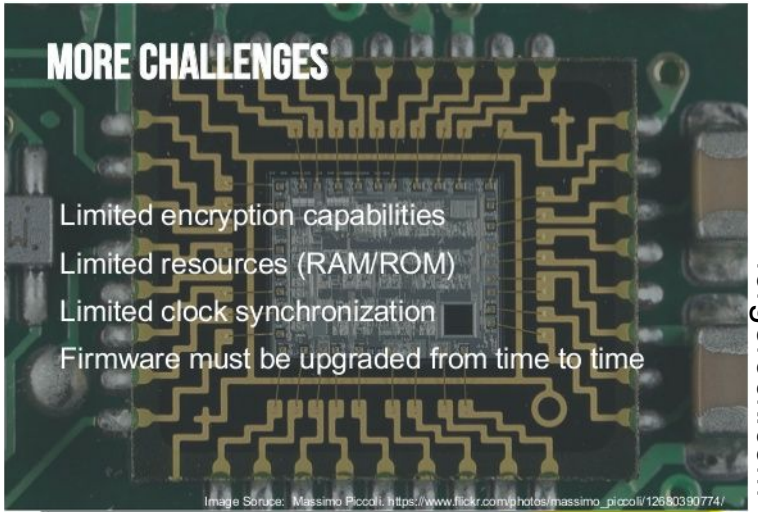
The Internet of Unpatched Things

Sarthak Grover and Nick Feamster
Princeton University

PrivacyCon ’16

Current State of Consumer Smart Devices

- Many different manufacturers, small startups, novice programmers
- Low capability hardware, not enough for security protocols
- Most data goes to an online server on the cloud
- Even devices in the same home communicate via the cloud

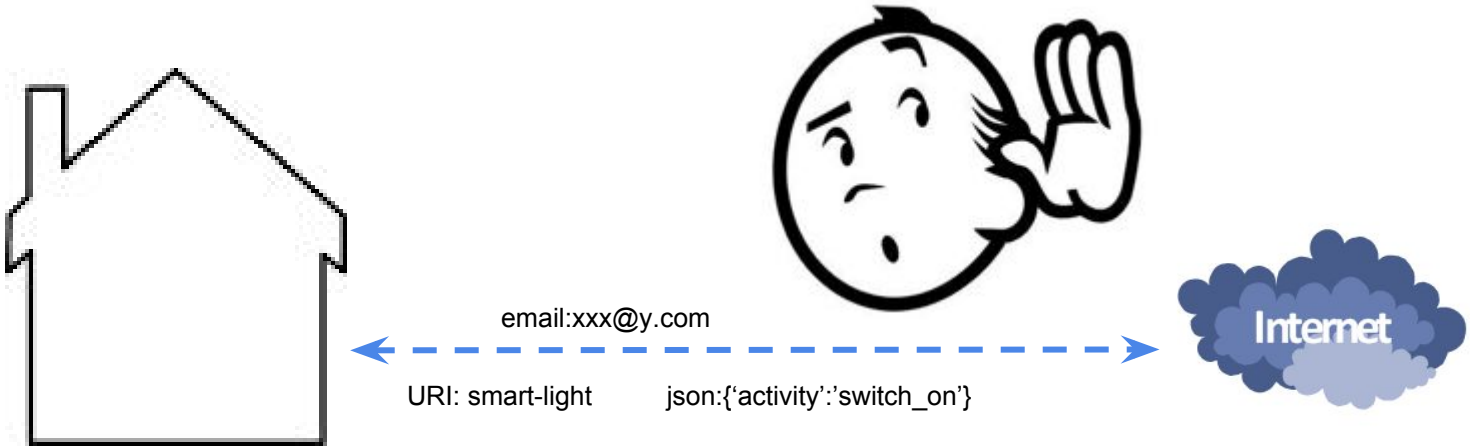


forgerock.com

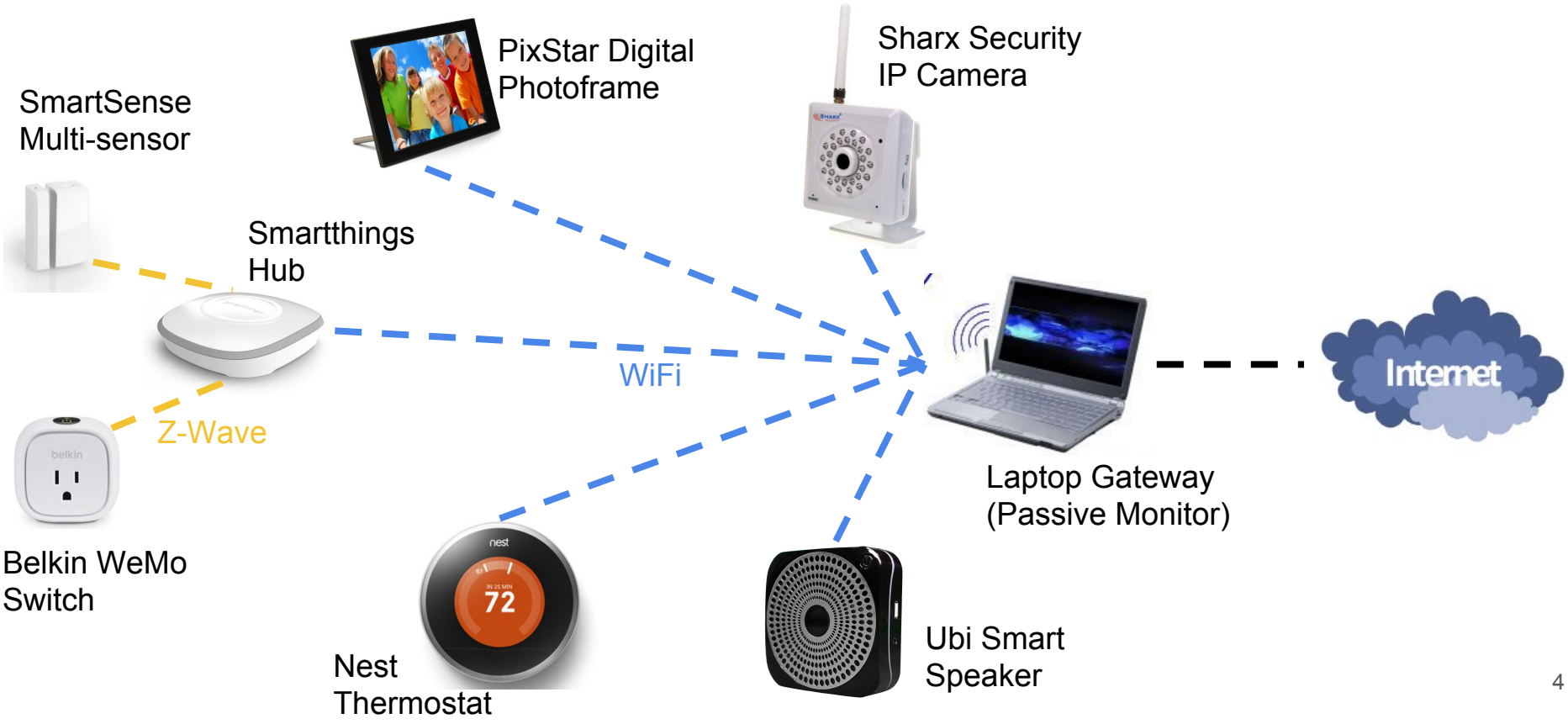
Unpatched IoT Devices Put Our Privacy at Risk

IoT device network traffic:

- Leaks user information
- Identifies the device being used
- May also identify current user activity and behavior!



Case Study of Some Common Home IoTs

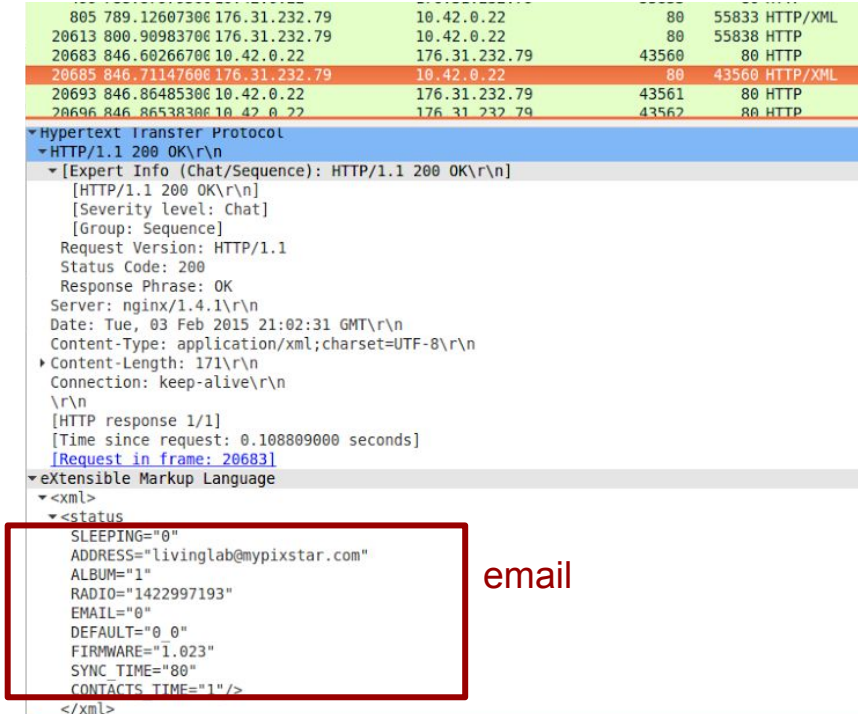


Digital Photoframe: Traffic Analysis

- All traffic and feeds (RSS) cleartext over HTTP port 80
- All actions sent to server in HTTP GET packet
- Downloads radio streams in cleartext over different ports
- DNS queries: api.pix-star.com, iptime.pix-star.com

Photoframe: Privacy Issues

- User **email ID is in clear** text when syncing account
- Current **user activity** in clear text in HTTP GET
- DNS queries and HTTP traffic identifies a pix-star photoframe



IP Camera: Traffic Analysis

- All traffic over cleartext HTTP port 80, even though viewing the stream requires login password
- Actions are sent as HTTP GET URI strings
- Videos are sent as image/jpeg and image/gif in the clear
- FTP requests also sent in clear over port 21, and FTP data is sent in clear text over many ports above 30,000
- DNS query: www.sharxsecurity.com

IP Camera: Privacy Issues

- **Video can be recovered** from FTP data traffic by network eavesdropper
- DNS query, HTTP headers, and ports identify a Sharx security camera

private user data

8	14.679939000	10.42.0.44	46.252.157.130	45962	21	FTP	74 Request: TYPE I
9	14.820736000	46.252.157.130	10.42.0.44	21	45962	FTP	96 Response: 200 TYPE is now 8-bit binary
10	14.821660000	10.42.0.44	46.252.157.130	45962	21	TCP	66 45962→21 [ACK] Seq=17 Ack=88 Win=8280 Len=0 TSval=1256532 TSe
11	14.823297000	10.42.0.44	46.252.157.130	45962	21	FTP	72 Request: PASV
12	14.957638000	46.252.157.130	10.42.0.44	21	45962	FTP	117 Response: 227 Entering Passive Mode (46,252,157,130,124,42)
13	14.959068000	10.42.0.44	46.252.157.130	60649	31786	TCP	74 60649→31786 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 T
14	14.995413000	10.42.0.44	46.252.157.130	45962	21	TCP	66 45962→21 [ACK] Seq=23 Ack=139 Win=8280 Len=0 TSval=1256550 TS
15	15.092593000	46.252.157.130	10.42.0.44	31786	60649	TCP	74 31786→60649 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 S
16	15.093262000	10.42.0.44	46.252.157.130	60649	31786	TCP	66 60649→31786 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=1256559 TS
17	15.096021000	10.42.0.44	46.252.157.130	45962	21	FTP	102 Request: STOR M 2015-03-17 17-37-23 348.jpg
18	15.230540000	46.252.157.130	10.42.0.44	21	45962	FTP	96 Response: 150 Accepted data connection
19	15.231793000	10.42.0.44	46.252.157.130	45962	21	TCP	66 45962→21 [ACK] Seq=59 Ack=169 Win=8280 Len=0 TSval=1256573 TS
20	15.233158000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes
21	15.233544000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes
22	15.233885000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1414 FTP Data: 1348 bytes
23	15.371483000	46.252.157.130	10.42.0.44	31786	60649	TCP	66 31786→60649 [ACK] Seq=1 Ack=1375 Win=17280 Len=0 TSval=258450
24	15.371922000	46.252.157.130	10.42.0.44	31786	60649	TCP	66 31786→60649 [ACK] Seq=1 Ack=2749 Win=20096 Len=0 TSval=258450
25	15.372409000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes
26	15.372557000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes
27	15.372976000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes
28	15.373113000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440 FTP Data: 1374 bytes

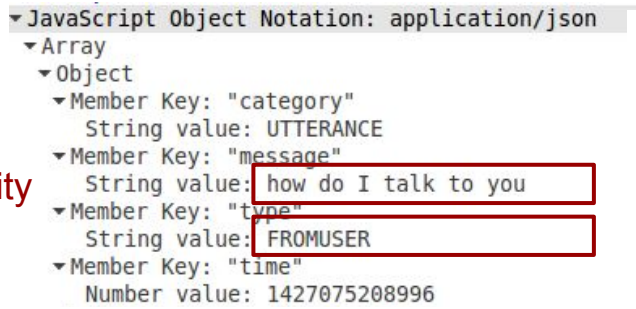
Ubi: Traffic Analysis

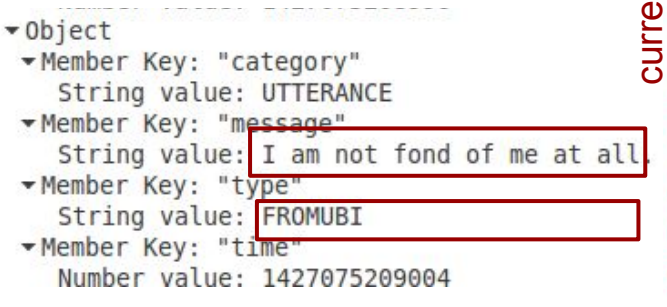
- All voice-to-text traffic sent in clear over port 80
- Activities sent in clear, and radio streamed over port 80
- Sensor readings are synced with server in the background over port 80
- Only communication with google API used HTTPS on port 443 and port 5228 (google talk)
- DNS query: portal.theubi.com, www.google.com, mtalk.google.com, api.grooveshark.com

Ubi: Privacy Issues

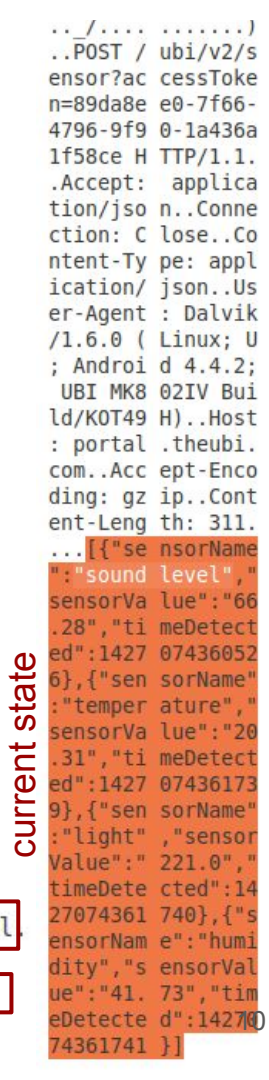
- Although HTTPS is clearly available, Ubi still uses HTTP to communicate to its portal. Eavesdropper can intercept **all voice chats and sensor readings** to Ubi's main portal
- Sensor values such as sound, temperature, light, humidity can identify if the user is home and currently active
- **Email in the clear** can identify the user
- DNS query, HTTP header (UA, Host) clearly identifies Ubi device

current activity





current state

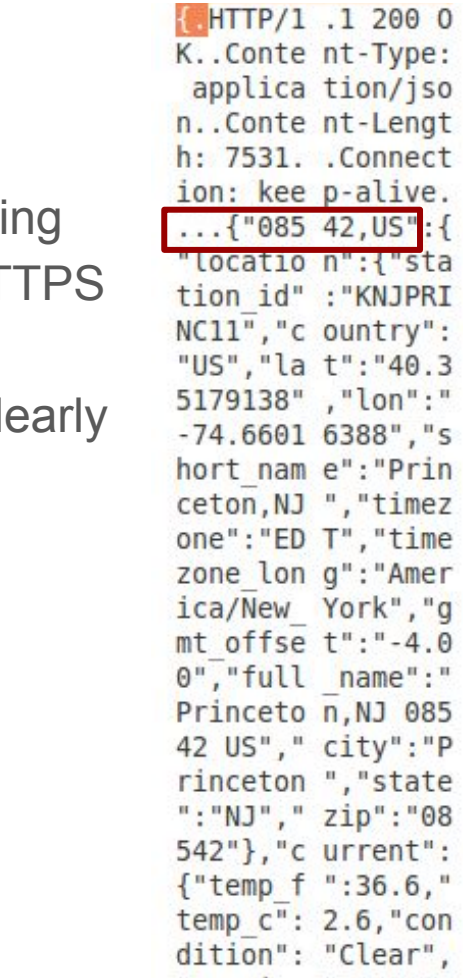


Nest Thermostat: Traffic Analysis

- All traffic to nest is HTTPS on port 443 and 9543
- Uses TLSv1.2 and TLSv1.0 for all traffic
- We found some incoming weather updates containing location information of the home and weather station in the clear. **Nest has fixed this bug after our report.**
- DNS query: time.nestlabs.com, frontdoor.nest.com, log-rts01-iad01.devices.nest.net. transport01-rts04-iad01. transport.home.nest.com

Nest: Privacy Issues

- Fairly secure device: all outgoing personal traffic, including configuration settings and updates to the server, use HTTPS
- *User zip code bug has been fixed
- DNS query as well as the use of the unique port 9543 clearly identifies a Nest device.

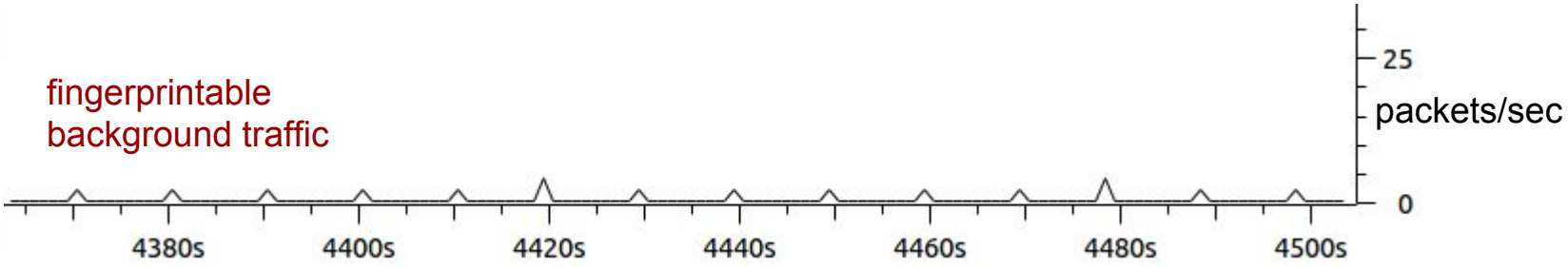


Smartthings Hub: Traffic Analysis

- All traffic over HTTPS on port 443 using TLS v1.2
- No clear text port 80 traffic
- Flows to an Amazon AWS instance running smartthings server
- 3-5 packets update every 10 sec in the background
- DNS query: dc.connect.smartthings.com

Smartthings: Privacy Issues

- Very secure: No information about IoT devices attached to hub is leaked
- Background updates every 10 seconds (over HTTPS) fingerprint the hub
- DNS query identifies Smartthings hub, but not individual devices



Smartthings Traffic

Conclusion: Be Afraid!

- Very difficult to enforce security standards
  - Multiple manufacturers
  - Low capability devices
  - Use of non-standard protocols and ports

- Difficult to maintain and patch due to low workforce and/or expertise
  - Who is responsible? (ISPs? Consumers? Manufacturers?)
  - Who is liable? Who should pay?

Conclusion: Be Afraid!

- Very difficult to enforce security standards
  - Multiple manufacturers
  - Low capability devices
  - Use of non-standard protocols and ports
- Difficult to maintain and patch due to low workforce and/or expertise
  - Who is responsible? (ISPs? Consumers? Manufacturers?)
  - Who is liable? Who should pay?

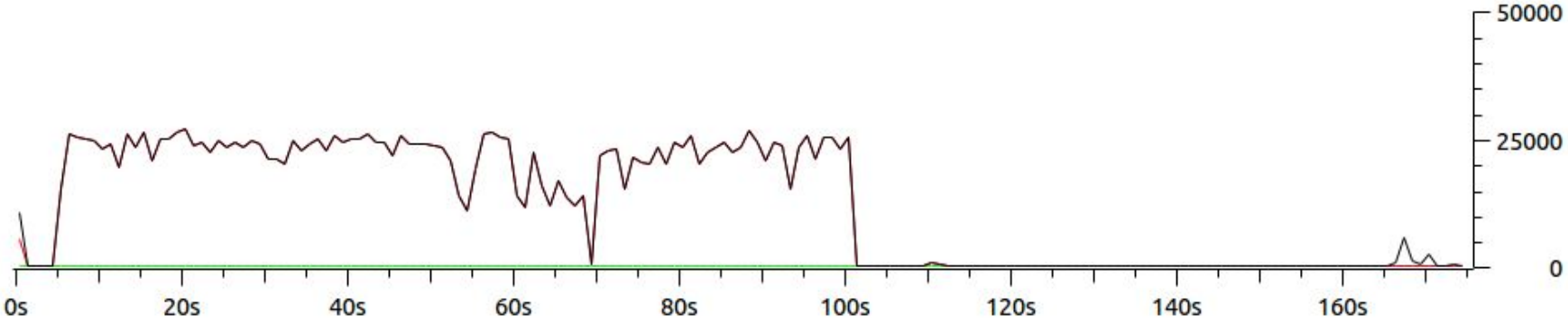
Can we solve this on the network? If so, how?

- How much information about user behavior do devices leak to the network?
- Can we offload device security to the home gateway or the cloud?

Thanks!

Smartthings: outlet and door sensor

- t=0 to t=100: Switch outlet ON and OFF repeatedly using mobile app
- >t=100: Background activity
- y-axis: Bytes per 10s



Smartthings hub (Work in progress)

- Difference in activity pattern for door sensor and smart outlet
- May identify type of user activity and device category (if not the exact device) from this limited list: http://www.smartthings.com/compatible-products
- Associate network pattern with activity
- Eavesdrop to predict user behavior