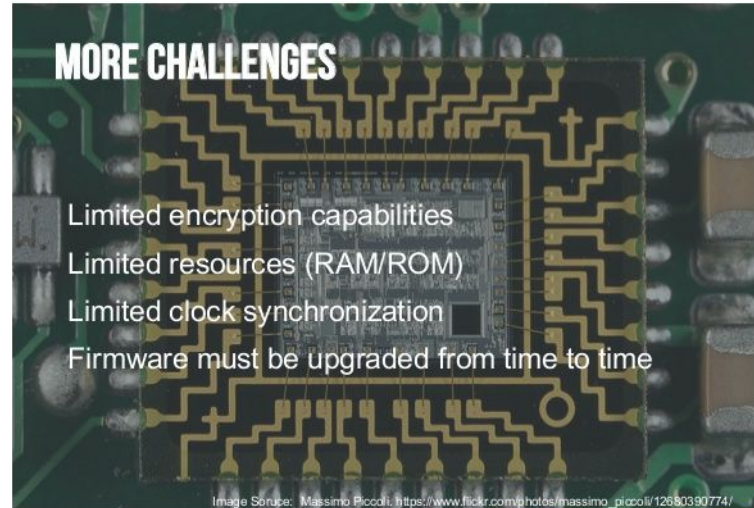


The Internet of Unpatched Things

Sarthak Grover and Nick Feamster
Princeton University

Current State of Consumer Smart Devices

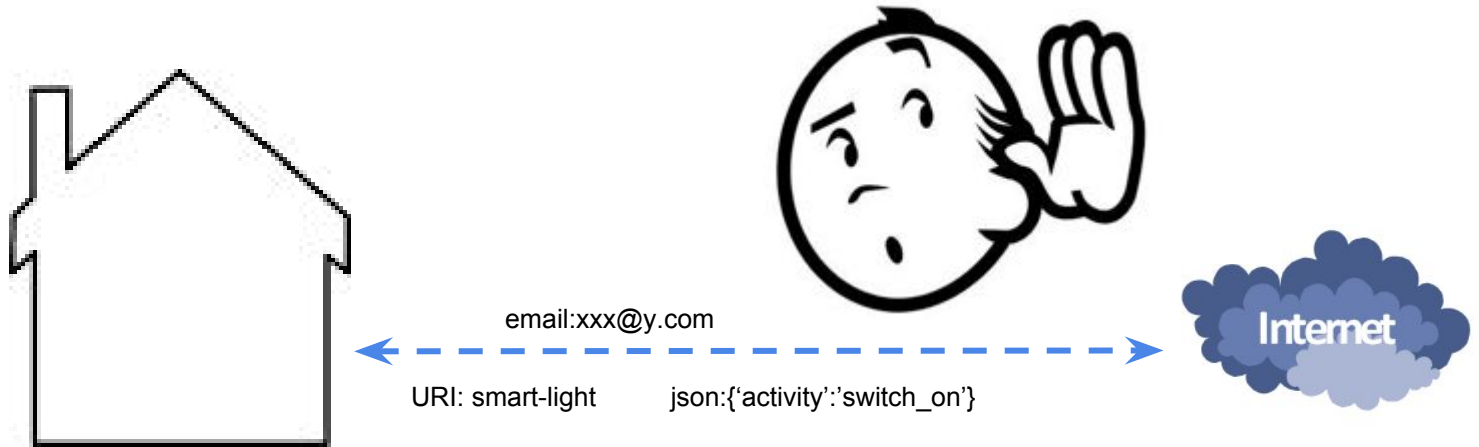
- Many different manufacturers, small startups, novice programmers
- Low capability hardware, not enough for security protocols
- Most data goes to an online server on the cloud
- Even devices in the same home communicate via the cloud



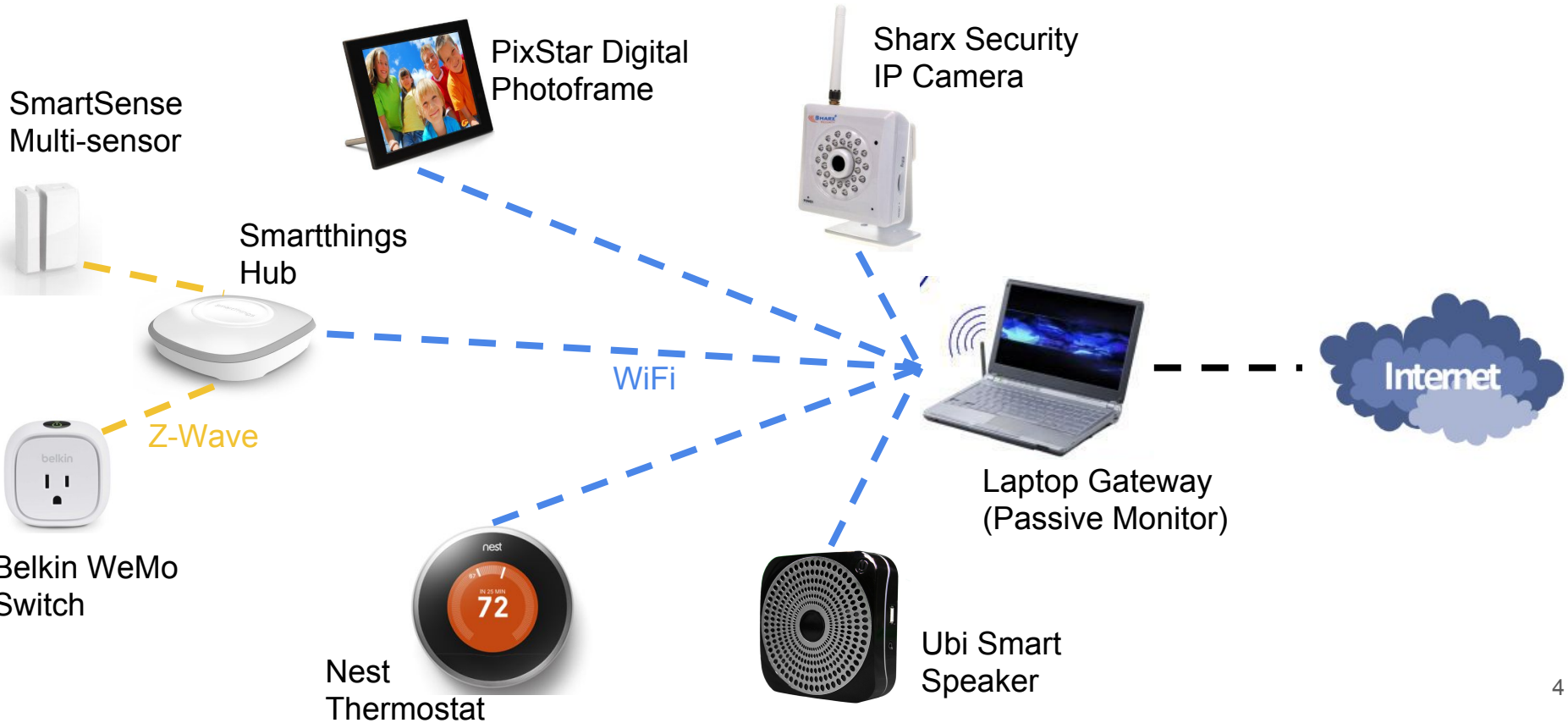
Unpatched IoT Devices Put Our Privacy at Risk

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

```
805 789.12607306 176.31.232.79 10.42.0.22 80 55833 HTTP/XML
20613 800.90983706 176.31.232.79 10.42.0.22 80 55838 HTTP
20683 846.60266706 10.42.0.22 176.31.232.79 43560 80 HTTP
20685 846.71147606 176.31.232.79 10.42.0.22 80 43560 HTTP/XML
20693 846.86485306 10.42.0.22 176.31.232.79 43561 80 HTTP
20696 846.86538306 10.42.0.22 176.31.232.79 43562 80 HTTP
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 200
    Response Phrase: OK
    Server: nginx/1.4.1\r\n
    Date: Tue, 03 Feb 2015 21:02:31 GMT\r\n
    Content-Type: application/xml;charset=UTF-8\r\n
    Content-Length: 171\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.108809000 seconds]
    [Request in frame: 20683]
  eXtensible Markup Language
    <xml>
      <status
        SLEEPING="0"
        ADDRESS="livinglab@mypixstar.com"
        ALBUM="1"
        RADIO="1422997193"
        EMAIL="0"
        DEFAULT="0 0"
        FIRMWARE="1.023"
        SYNC_TIME="80"
        CONTACTS_TIME="1"/>
      </xml>
```

email

current activity

```
Hypertext Transfer Protocol
  GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n]
    GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n
Hypertext Transfer Protocol
  GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n]
    [GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres
    Request Version: HTTP/1.1
```

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 TSeq=17
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 TSval=1256532 TSeq=60649
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 TSeq=23
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 SACK_PERM=1 TSval=1256550 TSeq=60649
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 TSeq=60649
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 TSeq=59
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=2584500 TSeq=60649
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=2584500 TSeq=60649
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

```
..../... .....)
..POST / ubi/v2/s
ensor?ac cessToke
n=89da8e e0-7f66-
4796-9f9 0-1a436a
1f58ce H TTP/1.1.
.Accept: applica
tion/jso n..Conne
ction: C lose..Co
ntent-Ty pe: appl
ication/ json..Us
er-Agent : Dalvik
/1.6.0 ( Linux; U
; Androi d 4.4.2;
UBI MK8 02IV Bui
ld/K0T49 H)..Host
: portal .theubi.
com..Acc ept-Enco
ding: gz ip..Cont
ent-Leng th: 311.
... [{"se nsorName
": "sound level",
sensorVa lue": "66
.28", "ti meDetect
ed": 1427 07436052
6}, {"sen sorName"
: "temper ature",
sensorVa lue": "20
.31", "ti meDetect
ed": 1427 07436173
9}, {"sen sorName"
: "light", "sensor
Value": " 221.0",
timeDete cted": 14
27074361 740}, {"s
ensorNam e": "humi
dity", "s ensorVal
ue": "41. 73", "tim
eDetecte d": 14270
74361741 }]
```

current state

```
▼ JavaScript Object Notation: application/json
  ▼ Array
    ▼ Object
      ▼ Member Key: "category"
        String value: UTTERANCE
      ▼ Member Key: "message"
        String value: how do I talk to you
      ▼ Member Key: "type"
        String value: FROMUSER
      ▼ Member Key: "time"
        Number value: 1427075208996
```

```
▼ Object
  ▼ Member Key: "category"
    String value: UTTERANCE
  ▼ Member Key: "message"
    String value: I am not fond of me at all
  ▼ Member Key: "type"
    String value: FROMUBI
  ▼ Member Key: "time"
    Number value: 1427075209004
```

current activity

I am not fond of me at all

FROMUSER

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-rt01-iad01.devices.nest.net. transport01-rt04-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.

```
{HTTP/1 .1 200 0
K..Content-Type:
  applica tion/jso
n..Content-Lengt
h: 7531. .Connect
ion: kee p-alive.
...{"085 42,US":{
"locatio n":{"sta
tion_id" : "KNJPRI
NC11", "c ountry":
"US", "la t": "40.3
5179138" , "lon": "
-74.6601 6388", "s
hort_nam e": "Prin
ceton, NJ ", "timez
one": "ED T", "time
zone_lon g": "Amer
ica/New_ York", "g
mt_offse t": "-4.0
0", "full_name": "
Princeto n, NJ 085
42 US", "city": "P
rinceton ", "state
": "NJ", " zip": "08
542"}, "c urrent":
{"temp_f ": 36.6, "
temp_c": 2.6, "con
dition": "Clear",
```

user zip code*

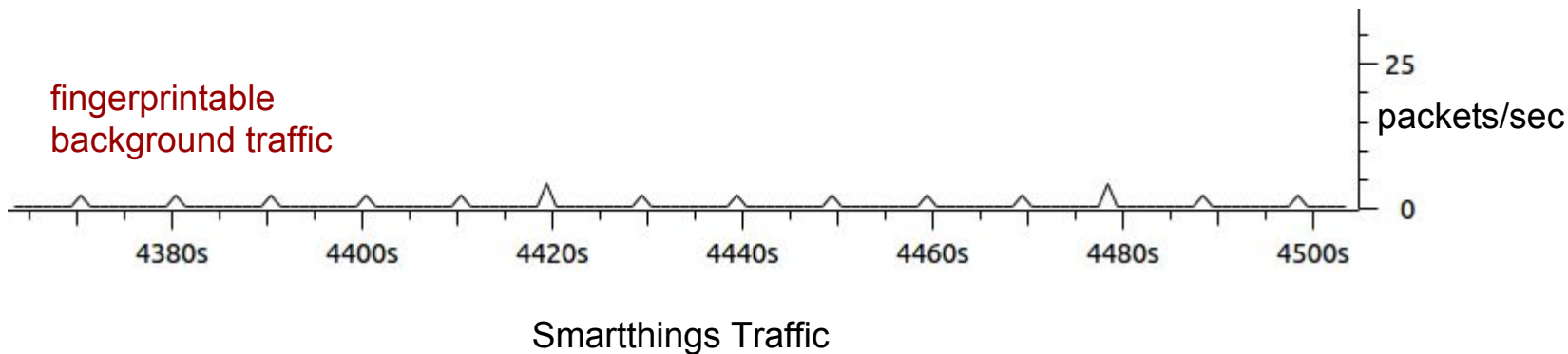
Smarthings Hub: Traffic Analysis

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



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?

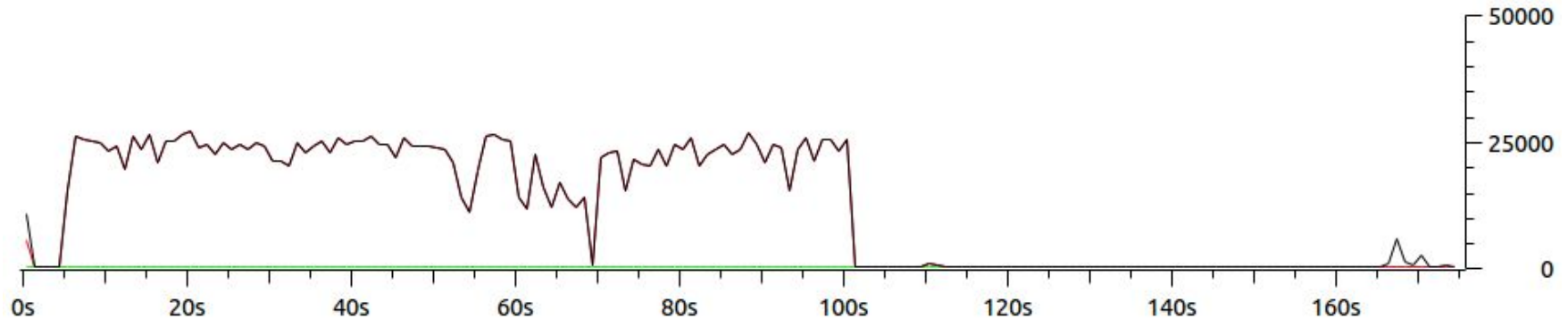
Can we solve this on the network? If so, how?

- 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!

Smarthings: 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



Smarthings 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.smarthings.com/compatible-products>
- Associate network pattern with activity
- Eavesdrop to predict user behavior