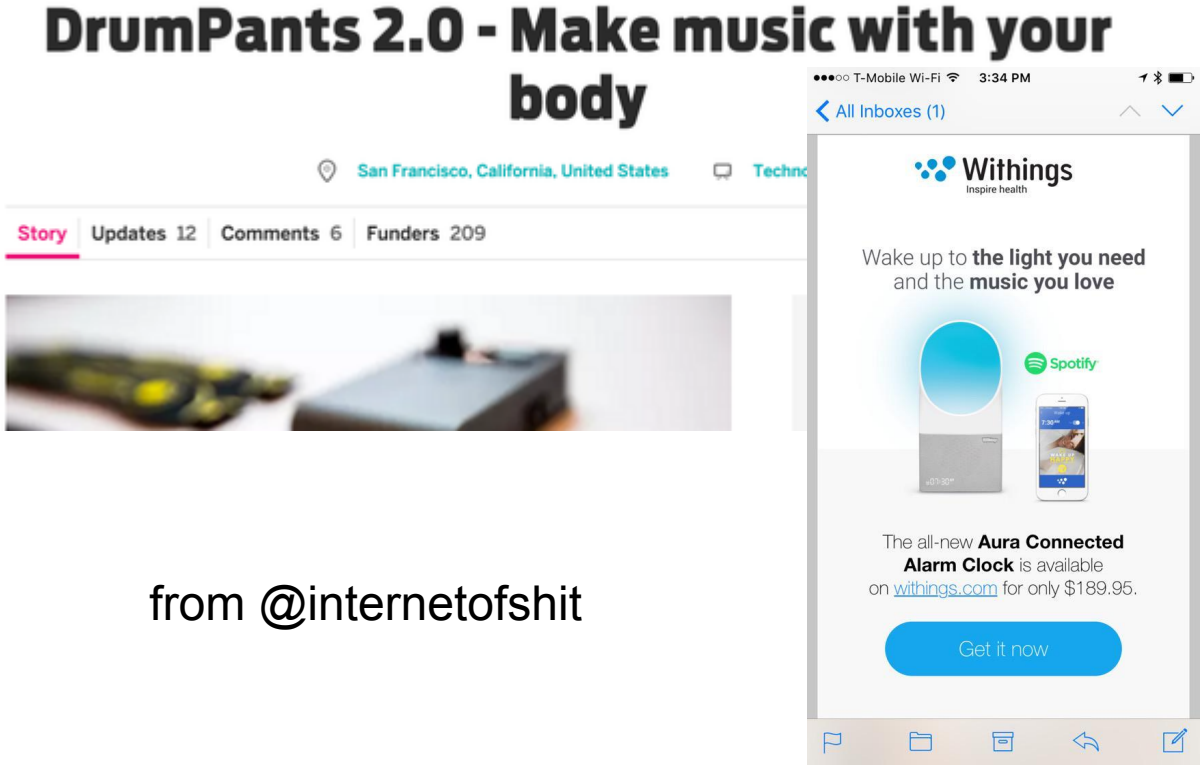
So What is Being Exposed From IoT Devices?

Ming Chow
mchow@cs.tufts.edu
Twitter: @0xmchow
The Security of Things Forum
September 9, 2015

Absurdities



LG's SmartThinQ Sensor

For example, when attached to a washing machine, the device can let you know when a laundry cycle is complete. Stick it on your fridge and it'll alert you when a particular food item is about to expire.

from @internetofshit

Absurdities (continued)

https://www.vibease.com/

Conan O'Brien
@ConanOBrien

Follow

So many useless new gadgets coming out every day. Is it too much to ask for a simple set of sturdy nail clippers with reliable Wi-Fi?

RETWEETS	FAVORITES
1,142	2,754

7:06 PM - 10 Jun 2015

Scope of This Talk

- Ingress and egress from devices (more of the latter)
- From what devices? Commonly used devices, not from an infinitely wide range of stuff (mostly fad)

What This Talk Will Not Cover

- Breaking and exploiting the devices
- Reverse engineering
- Attacking devices (e.g., Denial of Service)
- Defense and fixing the problem
- Web vulnerabilities (e.g., XSS, CSRF)
- Threat profile of mobile and mobile apps

Commonly Exposed from Devices

- **Status Data**: binary - on or off, available or not
- **Identification Data**: product, serial numbers
- **Location Data**: (e.g., where) latitude and longitude
- **Automation Data**: including sensor data
- **Action Data**: inferred or determined from status data and/or location data
- **Open ports**
- **Administration web interfaces**

Techniques

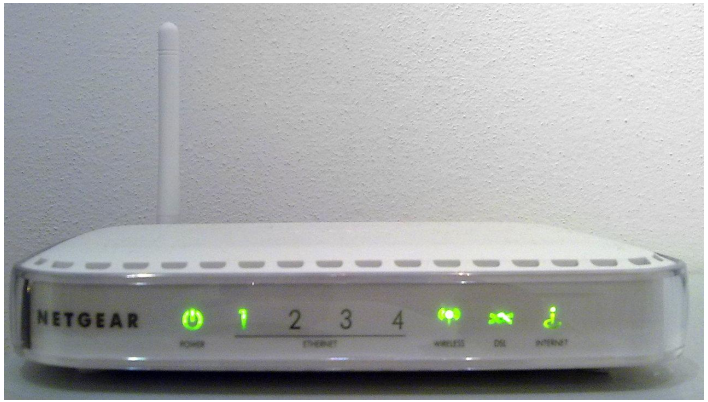
- Scanning
- Search engines:
  - Google
  - SHODAN - https://www.shodan.io/
  - Thingful - https://thingful.net/
- Social media

Webcams

- Example: AVTECH AVN801: used for surveillance
  - http://www.amazon.com/AVTECH-AVN801-Megapixel-Video-Camera/dp/B008FPDEPK
- 153,998 results on SHODAN: `linux upnp avtech product:"Avtech AVN801 network camera"`
- Ports exposed: 80, 4567, 8080, to name a few
- Admin interface exposed, many don’t even have them

Small Office Home Office (SOHO) Routers

- NETGEAR DG834G
  - http://www.amazon.com/NETGEAR-DG834G-Wireless-G-Router-Built/dp/B0000D8HK1
- 20,311 results on SHODAN: `NETGEAR DG834G`
- Ports exposed: 80, 7547 (modem), 8080, to name a few
- Admin interface exposed (HTTP)



Light Bulbs and Amazon Dash

- Many thanks to my colleague Ben Shapiro at the University of Colorado, Boulder. He can't resist playing with this stuff and send me stuff of what can you do with all this stuff (or whatcouldpossiblygowrong)
- Belkin WeMo line of home automation devices. In this example, a light bulb http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/
- Python API to Belkin WeMo devices: ouimeaux
  - GitHub: https://github.com/iancmcc/ouimeaux
  - Python Package Doc: https://ouimeaux.readthedocs.org/en/latest/readme.html
- Amazon Dash: device to buy home necessities (e.g., food) http://www.amazon.com/b?node=10667898011
- Belkin WeMo light bulb + Amazon Dash …….

Source Code For Amazon Dash + WeMo Light (thanks again Ben)

```
from scapy.all import *
import os

def arp_display(pkt):
  if pkt[ARP].op == 1: #who-has (request)
    if pkt[ARP].psrc == '0.0.0.0': # ARP Probe
      if pkt[ARP].hwsrc == 'a0:02:dc:da:8c:58': # Mac n Cheese
        print "Pushed Mac n Cheese... toggle bedroom lights"
        os.system('wemo -f switch "Bedroom switch" toggle')
      else:
        print "ARP Probe from unknown device: " + pkt[ARP].hwsrc

while True: sniff(prn=arp_display, filter="arp", store=0, count=999)
```

The point: ouimeaux is an application programming interface (API) that provides “command-line tool to discover and control (WeMo) devices in your environment; REST API to obtain information and perform actions on devices”. *Any device on network can send requests.*

Fitbit Ingress

- Body fat
- Weight
- Alarms
- Food
- Water
- Friends
- Heart rate
- Sleep
- Source: https://dev.fitbit.com/docs

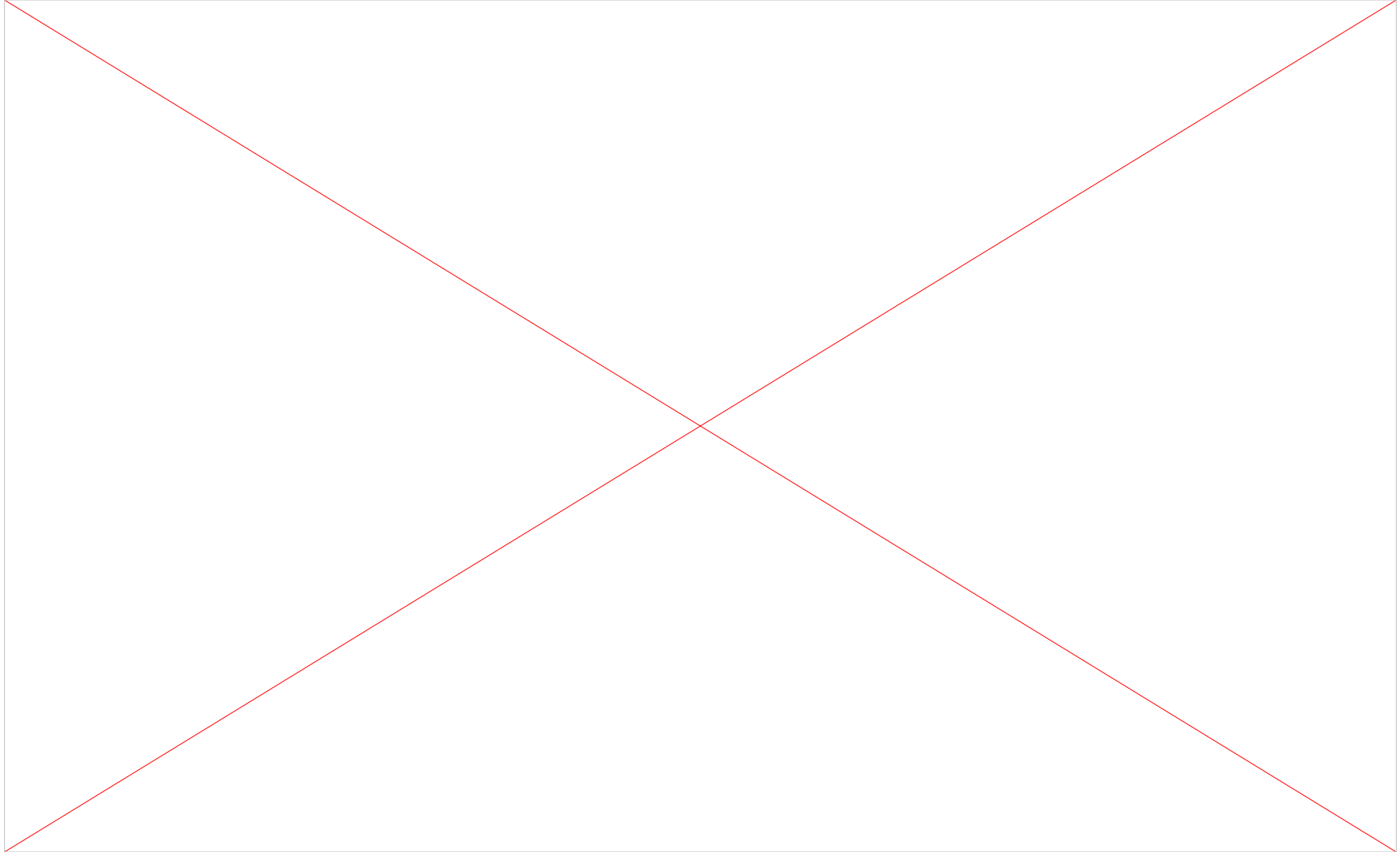
Fitbit Egress

- Source: https://dev.fitbit.com/docs/activity/
- “Fitbit Data Now Being Used In The Courtroom” http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

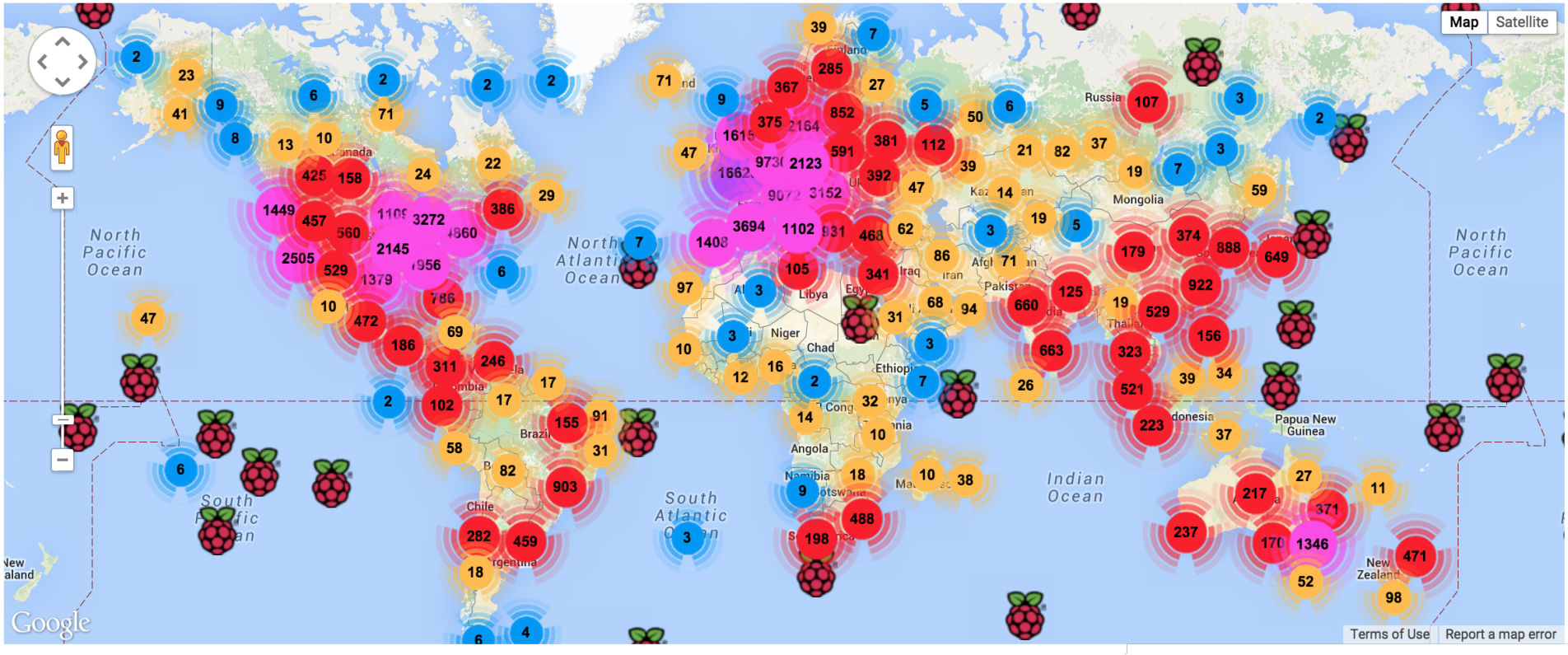

```
{
    "activities":[
        {
            "activityId":51007,
            "activityParentId":90019,
            "calories":230,
            "description":"7mph",
            "distance":2.04,
            "duration":1097053,
            "hasStartTime":true,
            "isFavorite":true,
            "logId":1154701,
            "name":"Treadmill, 0% Incline",
            "startTime":"00:25",
            "steps":3783
        }
    ],
    "goals":{
        "caloriesOut":2826,
        "distance":8.05,
        "floors":150,
        "steps":10000
     },
    "summary":{
        "activityCalories":230,
        "caloriesBMR":1913,
        "caloriesOut":2143,
        "distances":[
            {"activity":"tracker", "distance":1.32},
            {"activity":"loggedActivities", "distance":0},
            {"activity":"total","distance":1.32},
            {"activity":"veryActive", "distance":0.51},
            {"activity":"moderatelyActive", "distance":0.51},
            {"activity":"lightlyActive", "distance":0.51},
            {"activity":"sedentaryActive", "distance":0.51},
            {"activity":"Treadmill, 0% Incline", "distance":3.28}
        ],
        "elevation":48.77,
        "fairlyActiveMinutes":0,
        "floors":16,
        "lightlyActiveMinutes":0,
        "marginalCalories":200,
```

Raspberry Pi

- $35 computers
- Runs a complete Linux distribution off SD card
- Popular for hacking, IoT experiments, home automation
- Via Thingful: well over 9999+ results. Where does it get data from? Rastrack: 94845 results

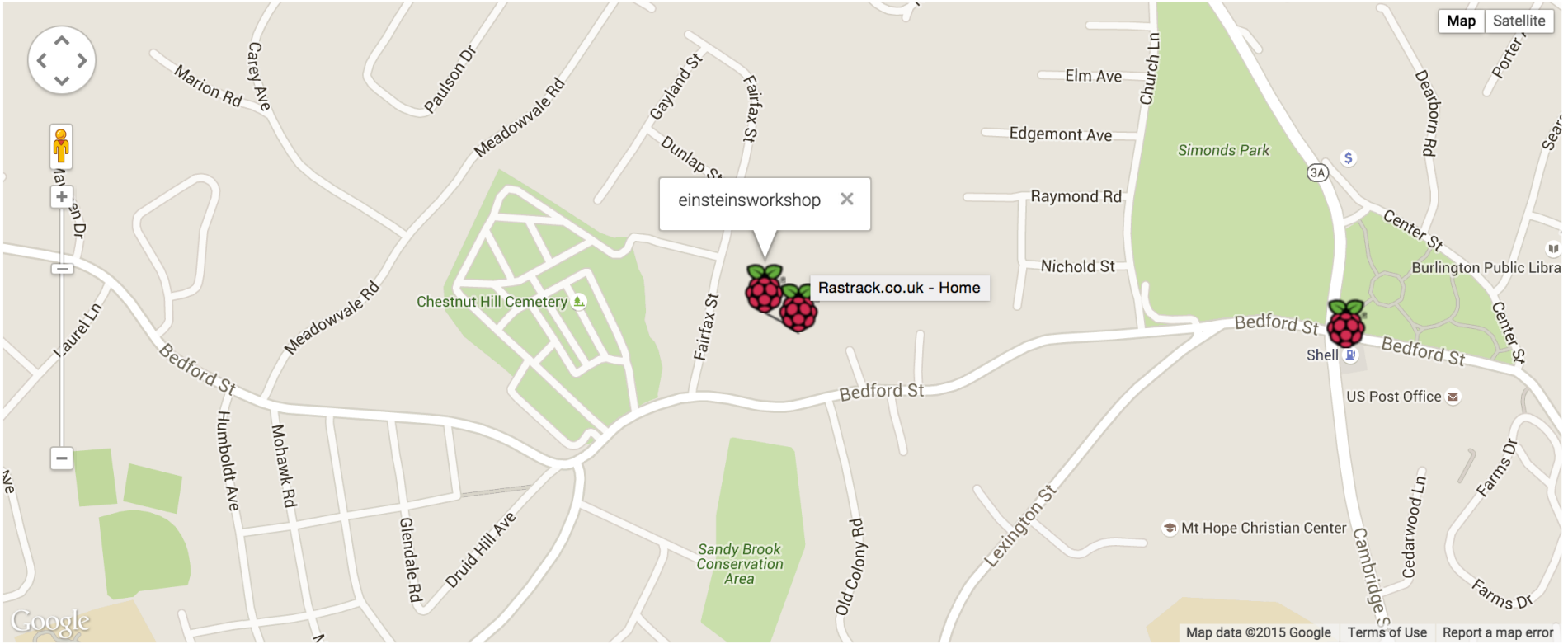


Rastrack Home Add Your Pi Change Your Details FAQ Contact



Rastrack.co.uk V2, © Ryanteck LTD. 2014, Made By Ryan Walmsley
Raspberry Pi Logo ™ Raspberry Pi Foundation
Powered by Google Maps & Digital Ocean (NGINX,PHP&MongoDB), Designed using Bootstrap. Tracking 94845 Raspberry Pis

Rastrack Home Add Your Pi Change Your Details FAQ Contact



The Future

- My hope: the data that you've seen today will help you understand *why* security and privacy issues are getting major visibility in the IoT space.
- What's impressive and scary: the scale of data going in and alas, going out
- API documentation is valuable
- "The Internet of Way Too Many Things" http://www.nytimes.com/2015/09/06/opinion/sunday/allison-arieff-the-internet-of-way-too-many-things.html
- Unfortunately, these devices will sell as people generally good at impulse buys.
- *Do really we need all this stuff?*

Déjà Vu: Who to Blame

- (heard from Bruce Schneier at USENIX 2004 in Boston)
- Developers
- Users
- Technology
- Politics and "dumb laws"

References

- Dhanjani, N, “Abusing the Internet of Things Blackouts, Freakouts, and Stakeouts”, O’Reilly Media, August 2015
- https://www.blackhat.com/docs/asia-14/materials/Dhanjani/Asia-14-Dhanjani-Abusing-The-Internet-Of-Things-Blackouts-Freakouts-And-Stakeouts.pdf
- http://www.wired.com/insights/2015/03/internet-things-data-go/
- http://readwrite.com/2015/08/13/five-types-data-internet-of-things
- https://recode.net/2015/04/07/a-hackers-eye-view-of-the-internet-of-things/
- http://www.computerworld.com/article/2944680/internet-of-things/the-internet-of-things-your-worst-nightmare.html
- http://thenextweb.com/insider/2012/12/09/the-future-of-the-internet-of-things/
- http://hackaday.com/2013/01/31/turning-the-belkin-wemo-into-a-deathtrap/
- http://www.networkworld.com/article/2226371/microsoft-subnet/500-000-belkin-wemo-users-could-be-hacked--cert-issues-advisory.html
- https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors