Real World Surface Attack

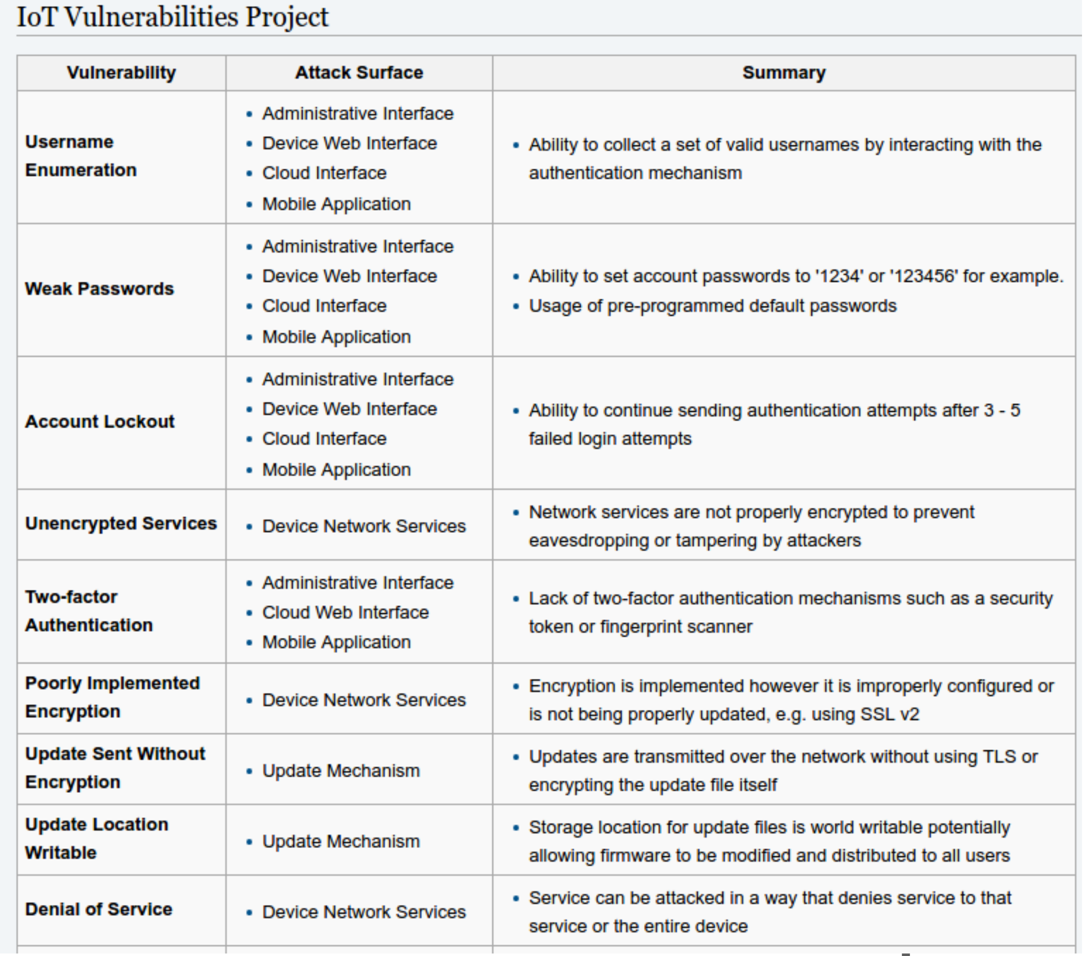
What’s the attacker surface?

What are the attacker weapons?

Once broken, how to exploit the “things”?

Top 10 OWASP

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption /Integrity Verification
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security



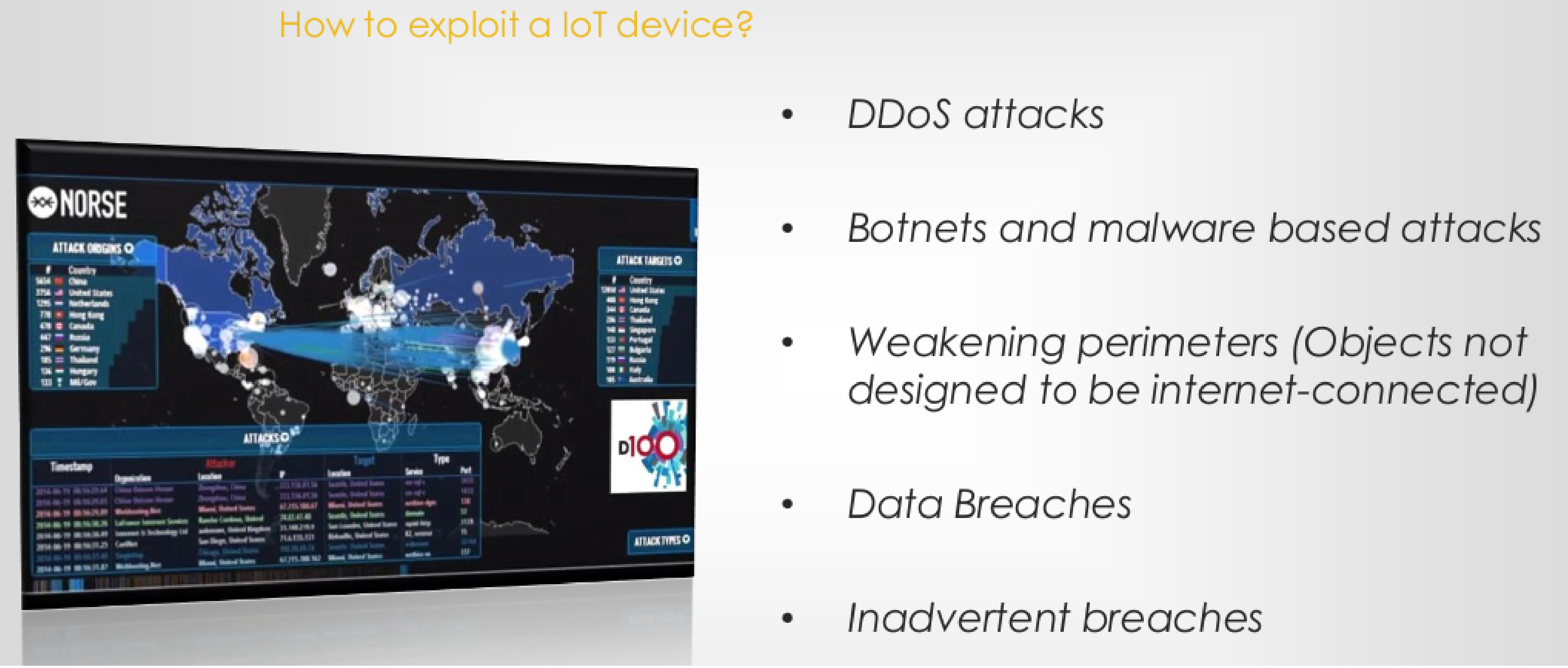
IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Username Enumeration	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to collect a set of valid usernames by interacting with the authentication mechanism
Weak Passwords	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to set account passwords to '1234' or '123456' for example. • Usage of pre-programmed default passwords
Account Lockout	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to continue sending authentication attempts after 3 - 5 failed login attempts
Unencrypted Services	• Device Network Services	• Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
Two-factor Authentication	• Administrative Interface • Cloud Web Interface • Mobile Application	• Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner
Poorly Implemented Encryption	• Device Network Services	• Encryption is implemented however it is improperly configured or is not being properly updated, e.g. using SSL v2
Update Sent Without Encryption	• Update Mechanism	• Updates are transmitted over the network without using TLS or encrypting the update file itself
Update Location Writable	• Update Mechanism	• Storage location for update files is world writable potentially allowing firmware to be modified and distributed to all users
Denial of Service	• Device Network Services	• Service can be attacked in a way that denies service to that service or the entire device

Top 10 OWASP

- IoT devices could be used to:
  - Send Spam
  - Coordinate an attack against a critical infrastructure.
  - Serve a malware.
  - Work as entry point within a corporate network.

Distributed

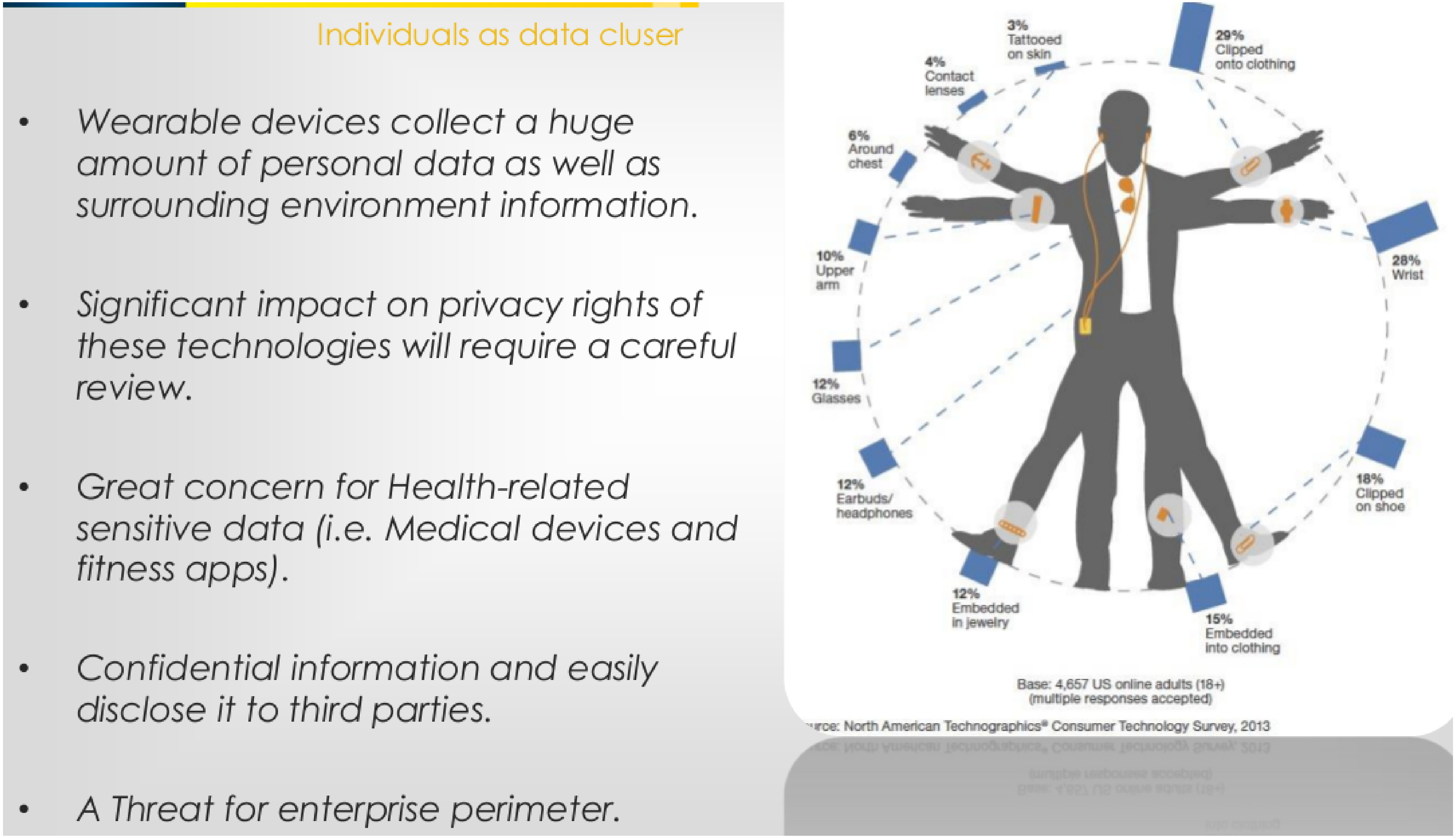


How to exploit a IoT device?

- *DDoS attacks*
- *Botnets and malware based attacks*
- *Weakening perimeters (Objects not designed to be internet-connected)*
- *Data Breaches*
- *Inadvertent breaches*

Source: Pierluigi Paganini: *“The internet of Things”*

Privacy Attacks



Individuals as data cluser

- *Wearable devices collect a huge amount of personal data as well as surrounding environment information.*
- *Significant impact on privacy rights of these technologies will require a careful review.*
- *Great concern for Health-related sensitive data (i.e. Medical devices and fitness apps).*
- *Confidential information and easily disclose it to third parties.*
- *A Threat for enterprise perimeter.*

Base: 4,657 US online adults (18+)
(multiple responses accepted)

urce: North American Technographics® Consumer Technology Survey, 2013

Source: Pierluigi Paganini: *“The internet of Things”*

ThingBot

- A ThingBot is a botnet consisting of devices within the Internet of things. Vulnerable or infected appliances that are connected to the Internet can potentially pose a risk to corporate networks (Kaspersky).

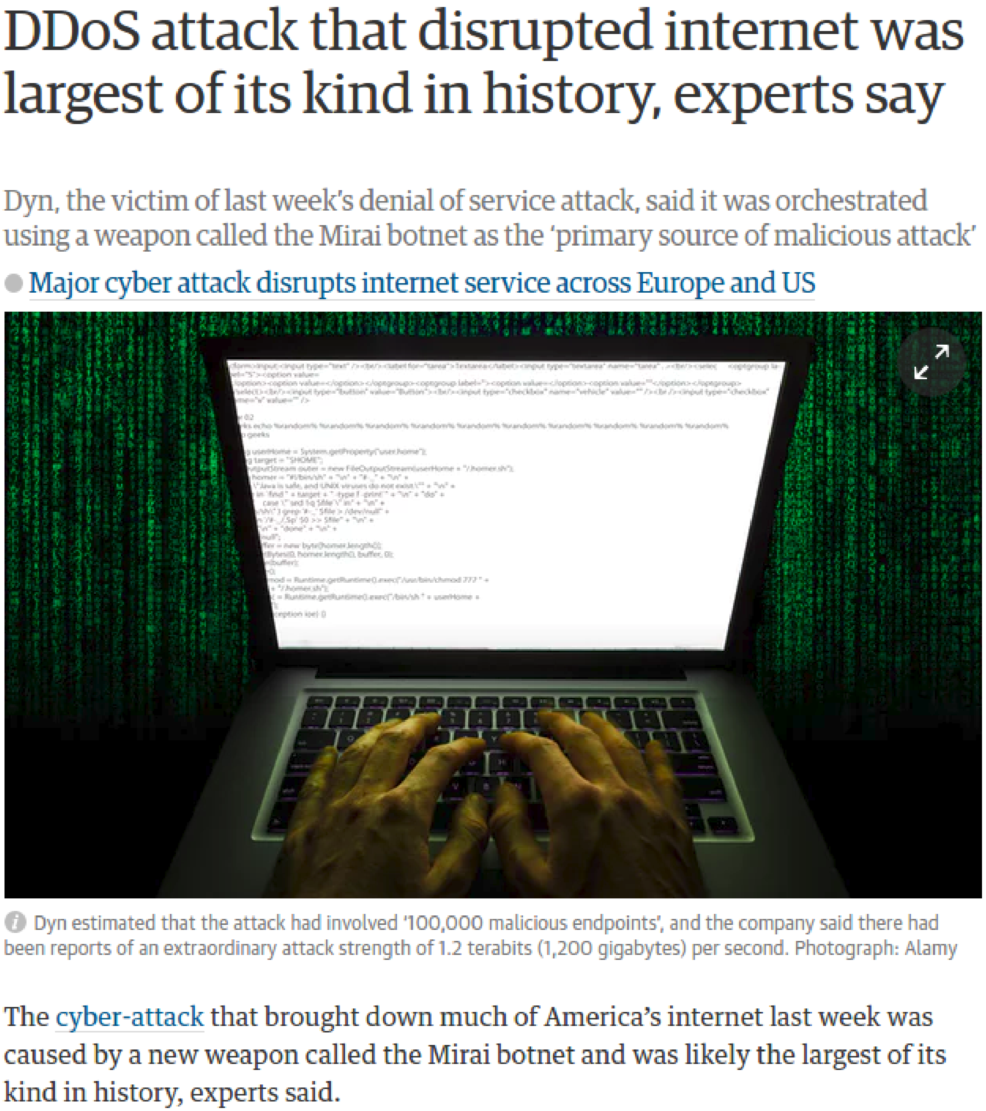
- Number of attacks against Routers, SmartTV, network-attached storage devices, gamingconsoles and various types of set-top boxes isincreasing.

- Many set-top boxes runs on embedded linux
  or apache operating systems of ARM-like microcomputers.

Source: Pierluigi Paganini: *“The internet of Things”*

Real Attack: Mirai @LiteSpeed

- DDos Attack with a botnet of more then 500K zombies over targeted victims as:
    - Brian Kreb Journalist
    - OVH web host
    - Dyn
        - Twitter
        - Reddit
        - Netflix
- A simple and easy malware (but of course extremly clever) that infected million of devices.



DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

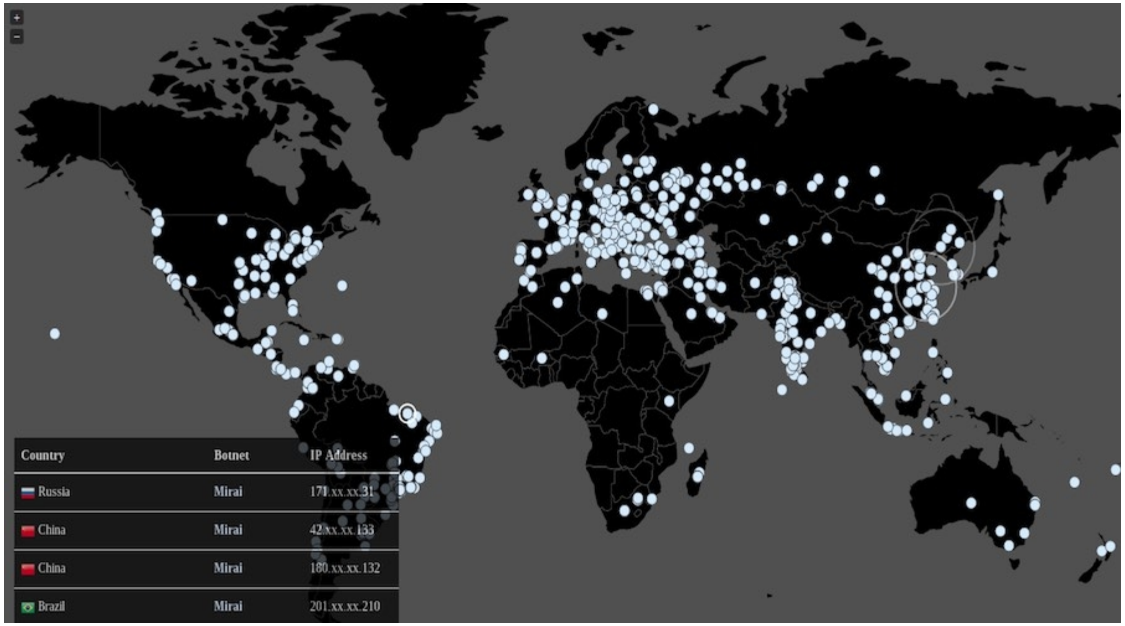
● Major cyber attack disrupts internet service across Europe and US

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The cyber-attack that brought down much of America's internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its kind in history, experts said.

Real Attack: Mirai

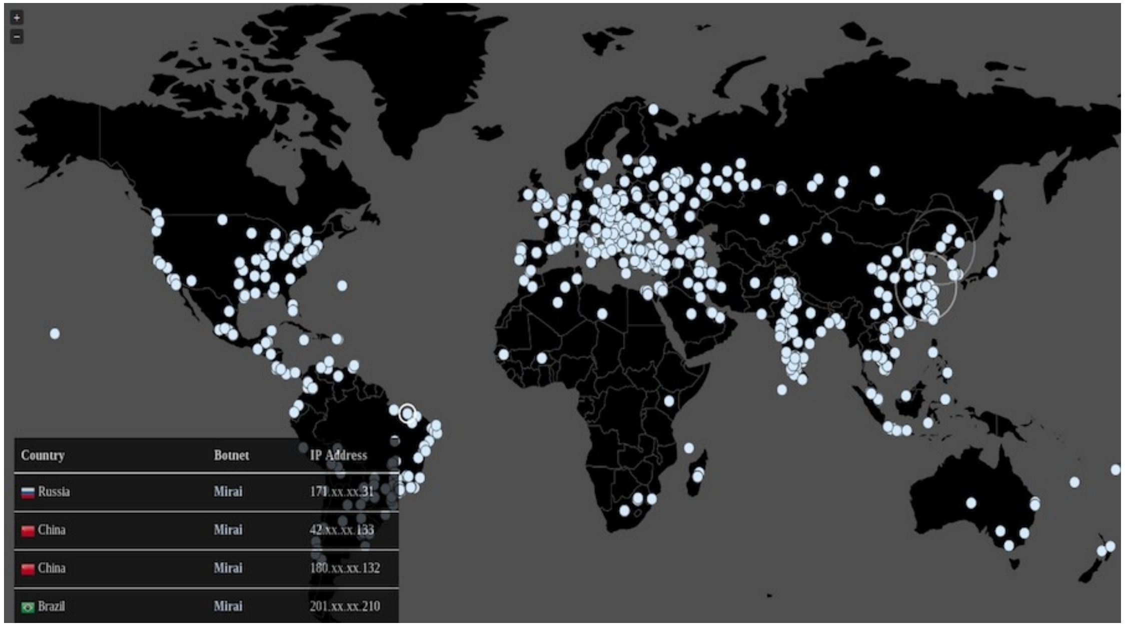
- Devices infected by Mirai continuously scan the internet for the IP address of IoT devices.
  - Why?
- Mirai then identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware.
  - Pros.



Country	Botnet	IP Address
Russia	Mirai	171.xx.xx.31
China	Mirai	42.xx.xx.133
China	Mirai	180.xx.xx.132
Brazil	Mirai	201.xx.xx.210

Real Attack: Mirai

- Devices infected by Mirai continuously scan the internet for the IP address of IoT devices.
  - Why?
- Mirai then identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware.
  - Pros.



Country	Botnet	IP Address
Russia	Mirai	171.xx.xx.31
China	Mirai	42.xx.xx.133
China	Mirai	180.xx.xx.132
Brazil	Mirai	201.xx.xx.210

Tip#1: MISCONFIGURATION IT’S A SERIOUS THREAT!

OT (Not really).

- Ongoing project on Security Lab:

  IoT Malware family classification through machine learning!

  - What's a malware family? (Ransomware, Cryptolocker, ecc)
    - E.g. CryptoWall, ZeuS,ecc

  - Do we have an IoT Cathegory?

  - Do we have a Mirai family?

- Quick TODO

  - Let's find the typical and common features of an IoT Malware
  - Collect a significant dataset of that
  - Let's use this feature to classify them with machine learning analysis.

Real Attack: Wearable Devices @Roman Unuchek

- Data sent between the Smartwatch and an Android mobile phone could be intercepted.
- An attacker that could be able to decode users' data,including text messages to Google Hangout chats and Facebook conversations.

Real Attack: Wearable Devices @Roman Unuchek

- Data sent between the Smartwatch and an Android mobile phone could be intercepted.
- An attacker that could be able to decode users' data,including text messages to Google Hangout chats and Facebook conversations.

DO YOU REMEMBER BLE(AH!!)???

Real Attack: Wearable Devices @Roman Unuchek

- The API Ble connection for most of the wearable devices are freely available.
- The attacker developed a mobile app that continuosly scan for new devices using BLE protocol
- Once identified i tried to pair with him using (and attacking):
  - Brute force digit pin (4/6 number)
  - MITM auth.
  - 0000 just work (the most difficult one)

RESULTS?

Source: https://securelist.com/how-i-hacked-my-smart-bracelet/69369/

Real Attack: Wearable Devices @Roman Unuchek

"From just six hours of scanning I was able to connect to 54 devices despite two serious restrictions"

"I was able to take control of the wristband, make it vibrate constantly and demand money to make it stop"

Tip#2: Your Smartwatch is like your laptop!

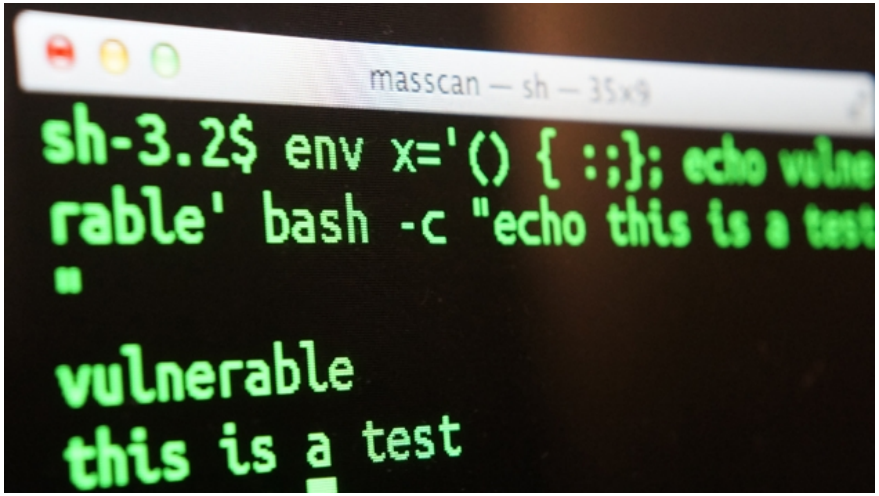
Real Attack: The BashBug (Shellshock) Bug

- Bash Bug (CVE-2014-6271) is a critical flaw in the widely used Unix Bash shell disclosed on 24 September 2014. Many IoT devices have Linux embedded and could not be easily patched.

- Many Internet-facing services use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands.

- Attackers could gain unauthorized access to a computer system and execute arbitrary code remotely.

- The impact is incredibly high because there are a lot of embedded devices that use CGI scripts (i.e. home appliances and wireless access points).



```
sh-3.2$ env x='() { :;}; echo vulne
rable' bash -c "echo this is a test
"
vulnerable
this is a test
```

Source: Pierluigi Paganini: *“The internet of Things”*

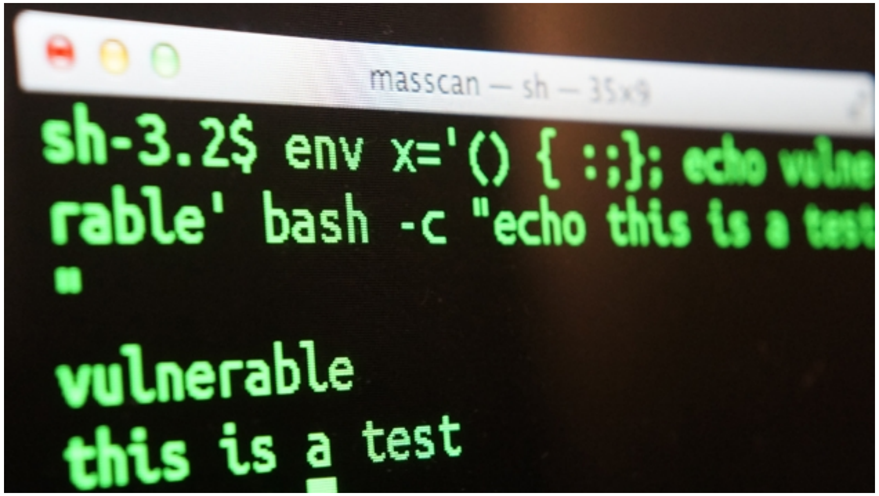
Real Attack: The BashBug (Shellshock) Bug

- Bash Bug (CVE-2014-6271) is a critical flaw in the widely used Unix Bash shell disclosed on 24 September 2014. Many IoT devices have Linux embedded and could not be easily patched.

- Many Internet-facing services use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands.

- Attackers could gain unauthorized access to a computer system and execute arbitrary code remotely.

- The impact is incredibly high because there are a lot of embedded devices that use CGI scripts (i.e. home appliances and wireless access points).



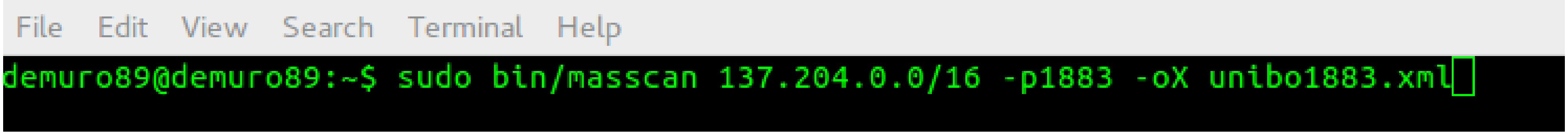
```
sh-3.2$ env x='() { :;}; echo vulne
rable' bash -c "echo this is a test
"

vulnerable
this is a test
```

Tip#3: Your IoT device must be upgradable and maintanable!

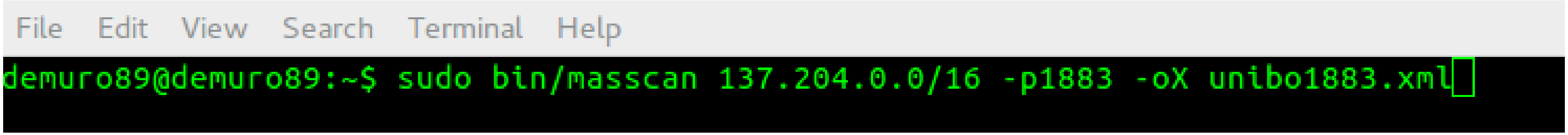
Source: Pierluigi Paganini: *"The internet of Things"*

Real Attack: MQTT Unibo @wildboar



```
demuro89@demuro89:~$ sudo bin/masscan 137.204.0.0/16 -p1883 -oX unibo1883.xml
```

Real Attack: MQTT on Unibo



```
demuro89@demuro89:~$ sudo bin/masscan 137.204.0.0/16 -p1883 -oX unibo1883.xml
```

Results:

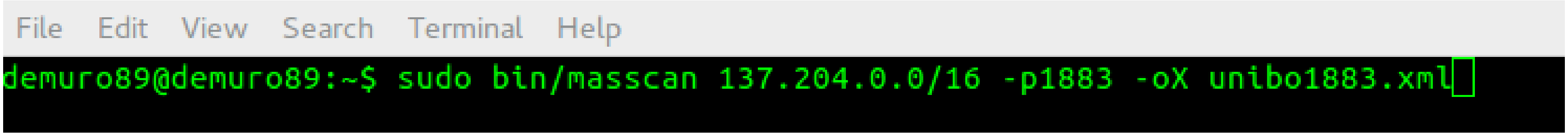
- “Connection Refused: not authorised.”

- /agraria/command HELO
  serre/command HELO

- "size":12,"time":1511254187516,"temp":23.27,"hum":24.47}

- owntracks/ebedeschi

Real Attack: MQTT on Unibo



```
demuro89@demuro89:~$ sudo bin/masscan 137.204.0.0/16 -p1883 -oX unibo1883.xml
```

Results:

- “Connection Refused: not authorised.”

“ A straight razor if you get too close to me”

- /agraria/command HELO serre/command HELO

Maybe in the future..

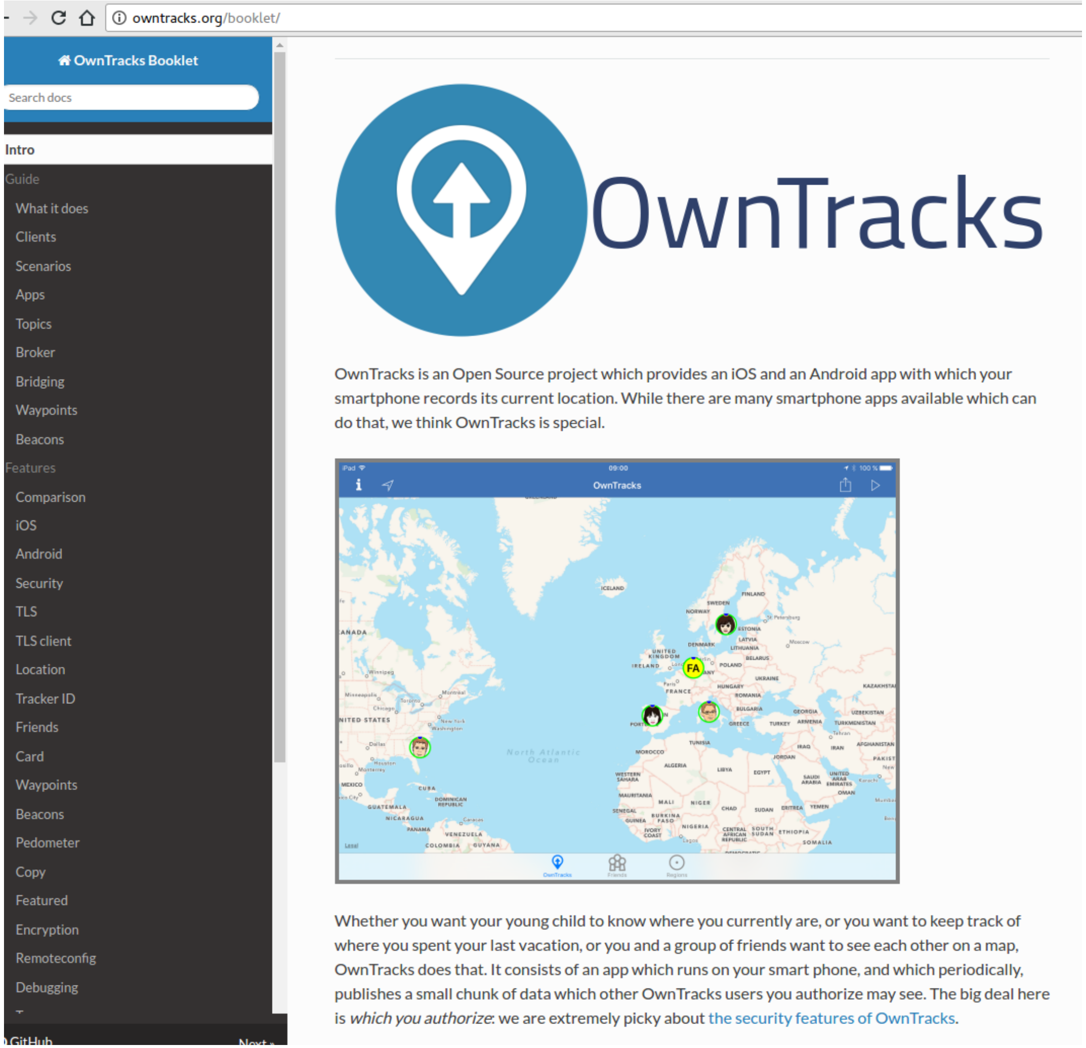
- "size":12,"time":1511254187516,"temp":23.27,"hum":24.47}

What’s the weather dude?

- owntracks/ebedeschi + (raw data)

…. seems interesting

Real Attack: MQTT on Unibo



owntracks.org/booklet/

OwnTracks Booklet

Search docs

Intro

Guide

- What it does
- Clients
- Scenarios
- Apps
- Topics
- Broker
- Bridging
- Waypoints
- Beacons

Features

- Comparison
- iOS
- Android
- Security
- TLS
- TLS client
- Location
- Tracker ID
- Friends
- Card
- Waypoints
- Beacons
- Pedometer
- Copy
- Featured
- Encryption
- Remoteconfig
- Debugging

GitHub Next »

OwnTracks

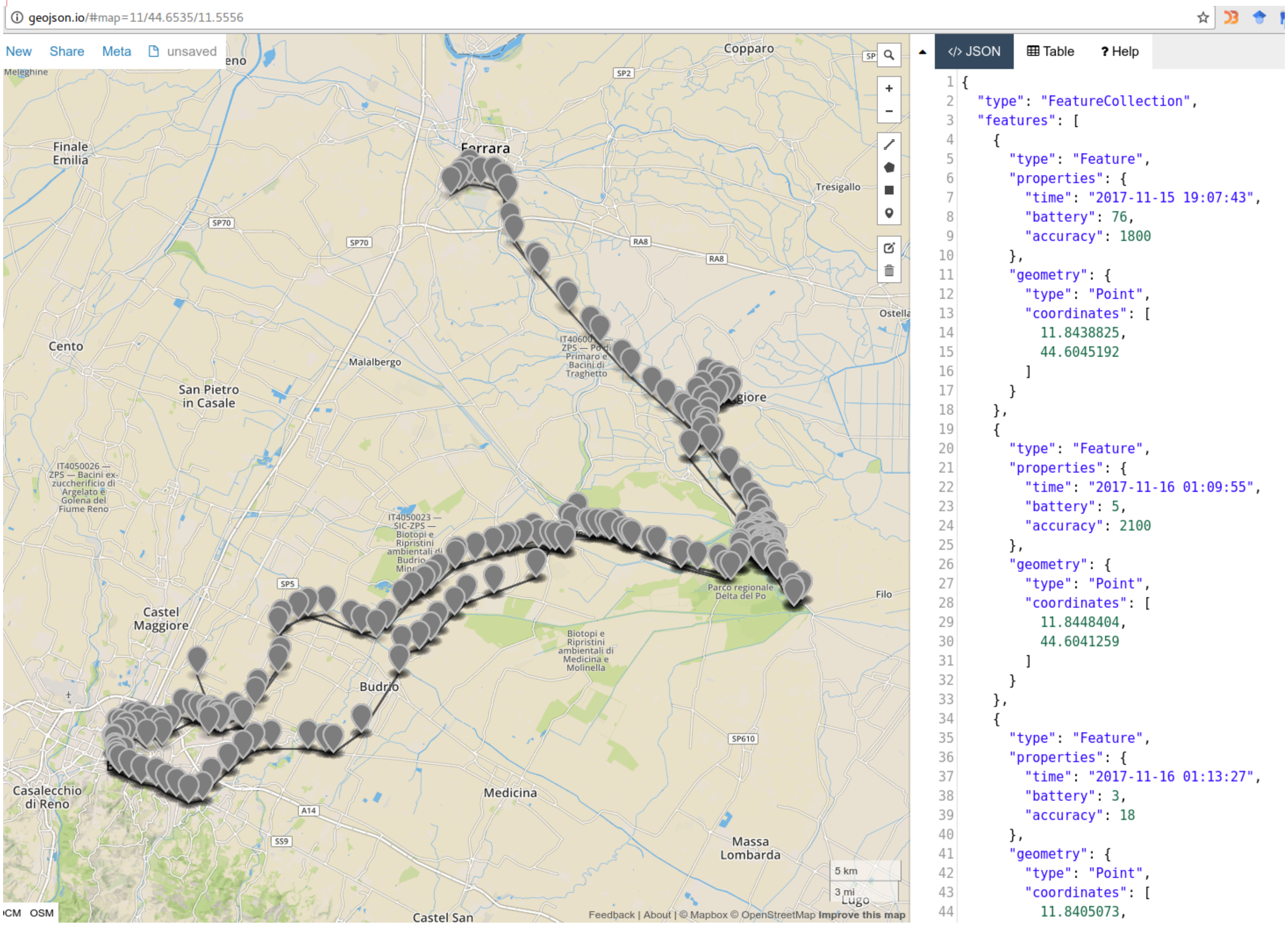
OwnTracks is an Open Source project which provides an iOS and an Android app with which your smartphone records its current location. While there are many smartphone apps available which can do that, we think OwnTracks is special.

Whether you want your young child to know where you currently are, or you want to keep track of where you spent your last vacation, or you and a group of friends want to see each other on a map, OwnTracks does that. It consists of an app which runs on your smart phone, and which periodically, publishes a small chunk of data which other OwnTracks users you authorize may see. The big deal here is *which you authorize*: we are extremely picky about the security features of OwnTracks.

This is the end:

```
{
"_type":"location",
"tid":"g4",
"acc":192,
"batt":88,
"conn":"m",
"lat":44.57761108875275,
"lon":11.493496298789978,
"tst":1511771317
}
```

Real Attack: MQTT on Unibo



```
{
  "type": "FeatureCollection",
  "features": [
    {
      "type": "Feature",
      "properties": {
        "time": "2017-11-15 19:07:43",
        "battery": 76,
        "accuracy": 1800
      },
      "geometry": {
        "type": "Point",
        "coordinates": [
          11.8438825,
          44.6045192
        ]
      }
    },
    {
      "type": "Feature",
      "properties": {
        "time": "2017-11-16 01:09:55",
        "battery": 5,
        "accuracy": 2100
      },
      "geometry": {
        "type": "Point",
        "coordinates": [
          11.8448404,
          44.6041259
        ]
      }
    },
    {
      "type": "Feature",
      "properties": {
        "time": "2017-11-16 01:13:27",
        "battery": 3,
        "accuracy": 18
      },
      "geometry": {
        "type": "Point",
        "coordinates": [
          11.8405073,
```

Tip#4: Do you Really need A tip?

DEMO TIME!

Final Thoughts

Protect your MQTT, you can!

@evilsocket quote “If you wanna build and sell some IoT-smart-whatever crap, and you wanna do it quickly because your competitor is about to go on the market with the same shit, you take Bluetooth, you strip it from the very few close-to-decent things it has and voilà, you have this a***le brother of BT”**

Questions?