Things that go **bump** in the night

Miranda Mowbray

Assistant: Amine Ballalou

PhD Student: Abia Amin

designed by freepik.com

From Ghoulies and Ghosties
And long-leggedy Beasties
And **Things that go Bump in the night**
Good Lord preserve us

“I'm probably the person who does least with the Internet of Things.”

“I'm probably the person who does least with the Internet of Things.

As I walk home, my phone knows it because of the cell tower signals, and turns on my WiFi. As I get closer, it turns on the smart bulb in my room. When I connect to the WiFi it turns on my fan to cool down the room a little. Finally, if it can, it'll try and get Alexa to play my favourite music as well. That’s all.”

Sunny Miglani

The 1st toothbrush with Artificial Intelligence
La 1re brosse à dents avec Intelligence Artificielle

Rest of the talk

- Some attacks/vulnerabilities
- Historical interlude 1: Talos
- Weather stations going bump
- Motion sensor going bump
- How to hear the bump
- Historical interlude 2: Defending the castle
- State of IoT security

Some Attacks/ Vulns

designed by freepik.com

Casino hacked through fishtank thermometer

Fishtank photo (cc) BY Tristan Ferne/tristanf on Flickr https://www.flickr.com/photos/tristanf/4398720453/

https://thehackernews.com/2018/04/iot-hacking-thermometer.html

10 GB of data was moved through the thermometer in the Casino’s lobby aquarium to an external IP address

DarkTrace, April 2018

https://www.businessinsider.in/Hackers-stole-a-casinos-high-roller-database-through-a-thermometer-in-the-lobby-fish-tank/articleshow/63769685.cms

Unbreakable smart lock devastated to discover screwdrivers exist

- Broadcast its MAC address, used it to calculate key
- Only checked if token is a valid token
- Screwdrivers exist

(Patched since then)

Andrew Tierney (cybergibbons), Pen Test Partners ; Vangelis Stykas; JerryRigEverything, June 2018.

https://www.theregister.co.uk/2018/06/15/taplock_broken_screwdriver

Belkin Wemo vulnerabilities

Stack-based Buffer Overflow vulnerability in WeMo Insight Smart Plug
McAfee, Aug 2018
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/iot-zero-days-is-belkin-wemo-smart-plug-the-next-malware-target/

Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices
Trend Micro, Apr 2019
https://www.zdnet.com/article/bashlite-iot-malware-upgrade-lets-it-target-wemo-home-automation-devices/

Keyless car theft

5 of the 11 new cars launched this year have no protection against keyless relay attack

Thatcham, Mar 2019

http://news.thatcham.org/pressreleases/six-of-the-11-new-cars-launched-in-2019-rated-poor-for-security-2850271

UK car theft claims Q1 2019 highest since 2012

92% of recovered cars in Essex were keyless relay thefts

Motoring Research, Mar 2019

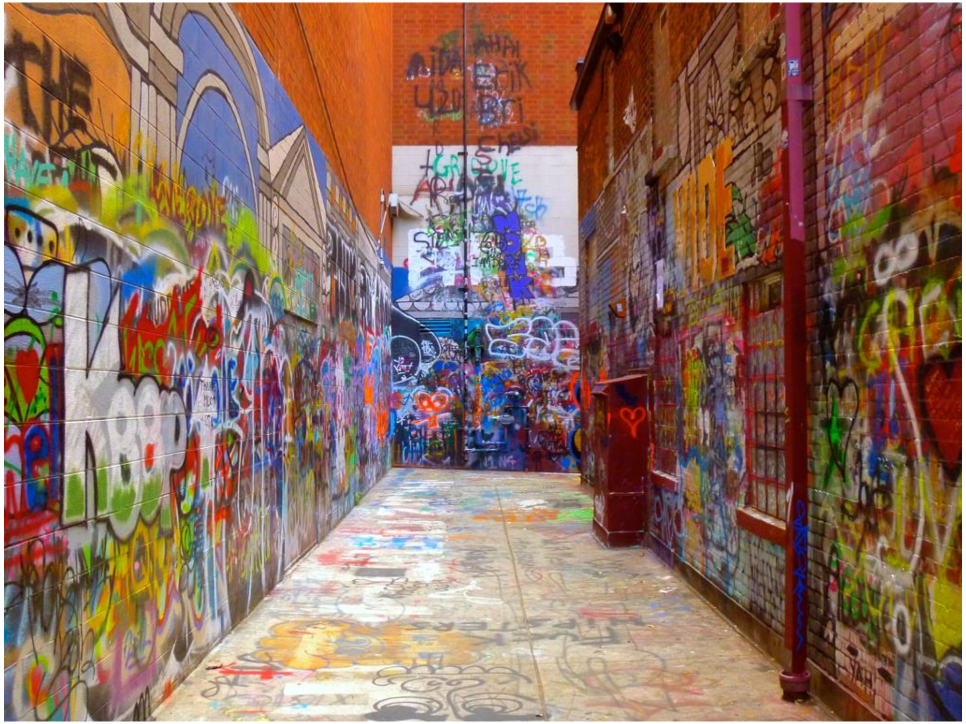
https://www.zdnet.com/article/bashlite-iot-malware-upgrade-lets-it-target-wemo-home-automation-devices/

Monsieur Cuisine

Cooking “robot”
Android 6.0 – no longer patched
Undocumented microphone

Alexis Viguié & Adrien Albisetti, June 2019

Photo: still from "Monsieur Cuisine Connect Hack Android"
cc BY Sinuso Yote
https://www.youtube.com/watch?v=WeTAwJisF3c



96 top-selling Wifi/Bluetooth Things on Amazon:
32 companion apps

Communication channel app ↔ device

- 31% no encryption
- 19% use hardcoded keys

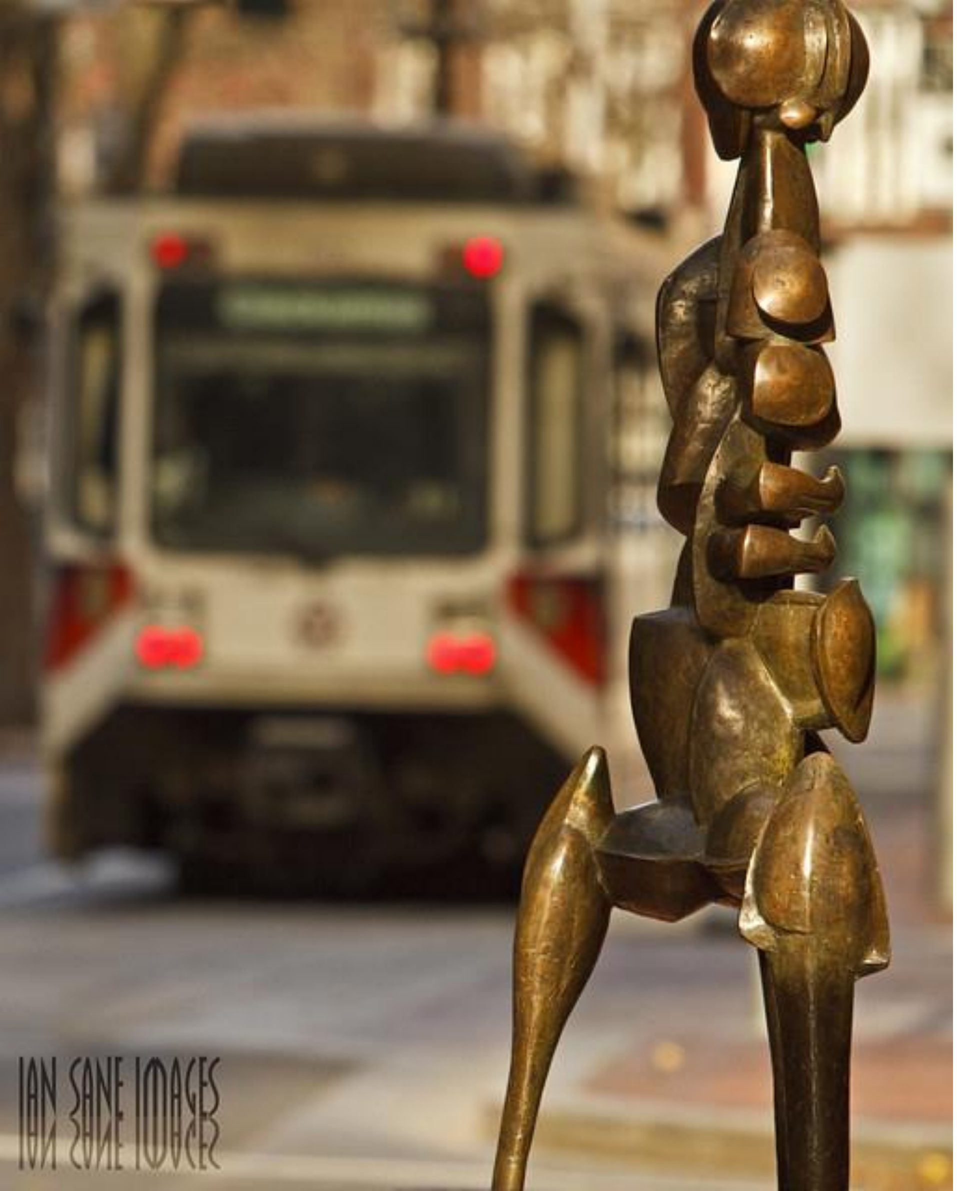
total 50% of apps, or 38% of Things

Universities of Pernambuco & Michigan, Jan 2019

https://arxiv.org/pdf/1901.10062.pdf

Historical interlude 1: Talos

designed by freepik.com



Talos

Photo cc BY Ian Sane
of sculpture by James Lee Hanson,
https://www.flickr.com/photos/
31246066@N04/11441760524/

Medea and Talos

SYBIL TAWSE
MEDEIA AND TALVS

Illustration by Sybil Tawse
in "Stories of gods and heroes" (1920) by Thomas Bulfinch
https://commons.wikimedia.org/wiki/File:Medeia_and_Talus.png

Vulnerabilities in CUJO smart firewall

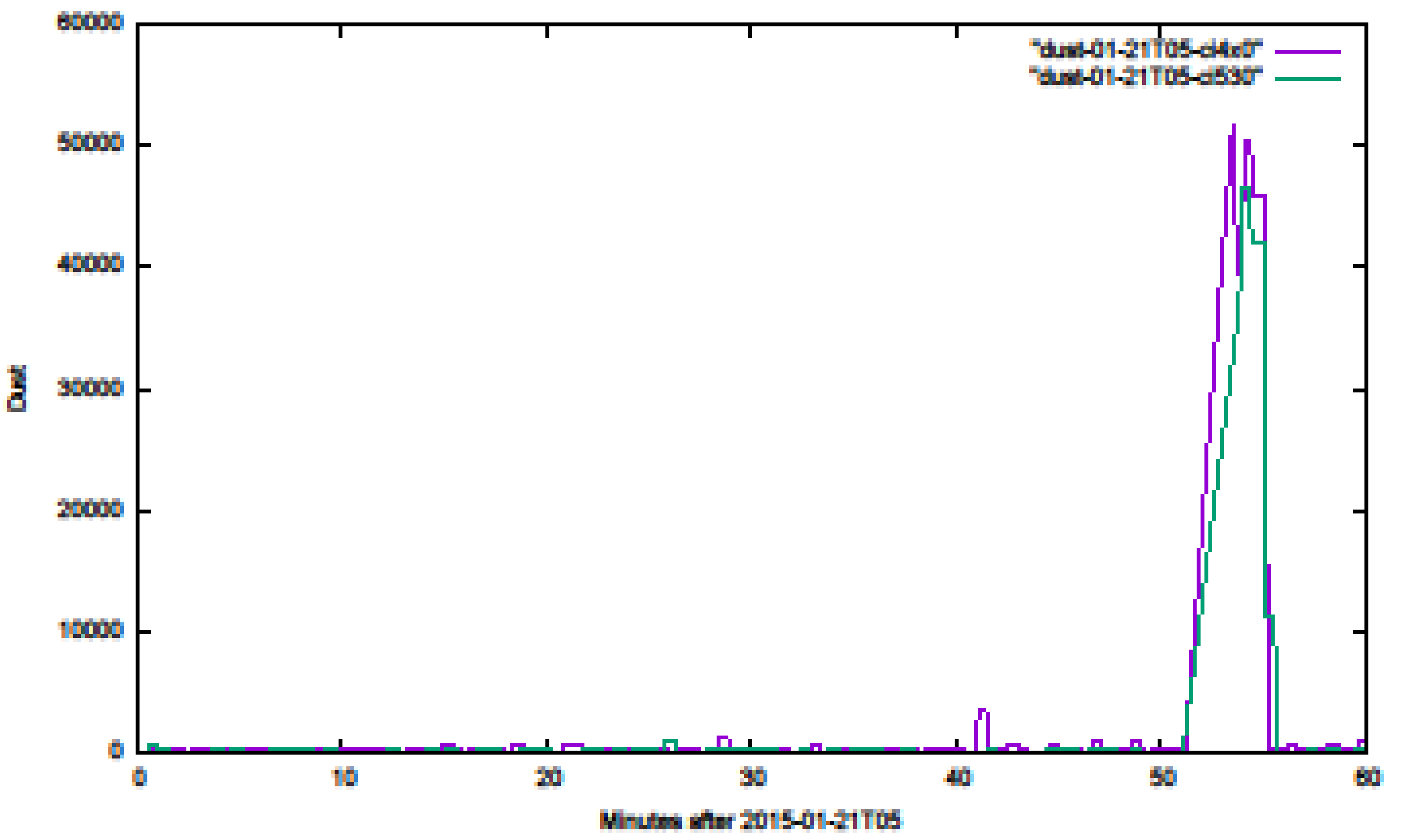
Talos Intelligence, March 2019
https://blog.talosintelligence.com/2019/03/vuln-spotlight-cujo.html

Weather Stations Going Bump

designed by freepik.com

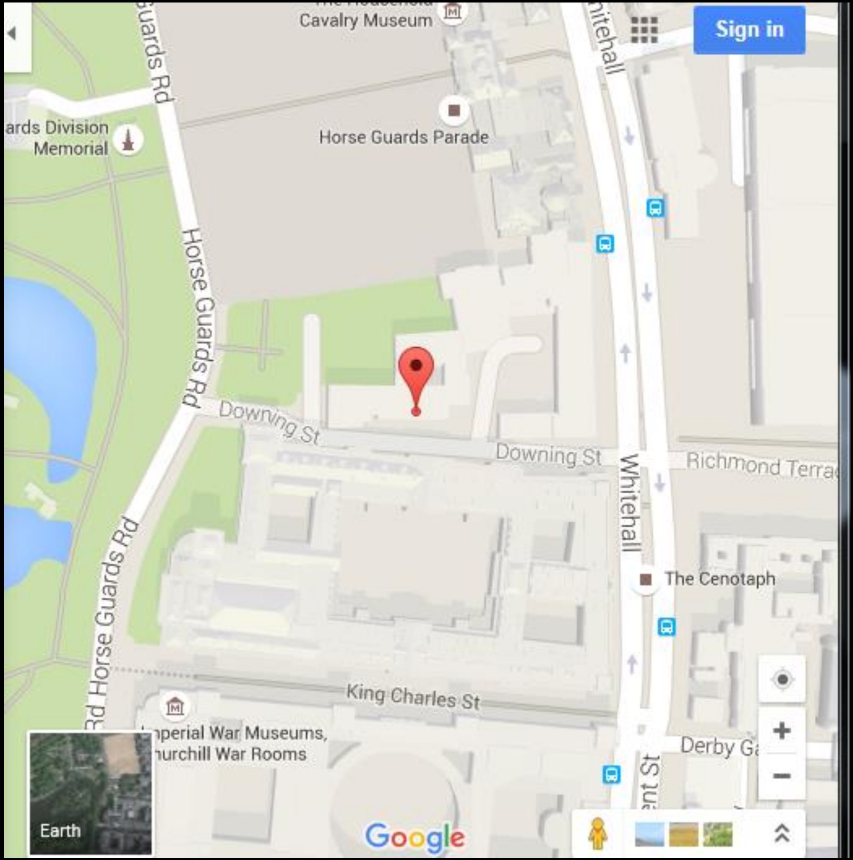
A tale of two dust sensors

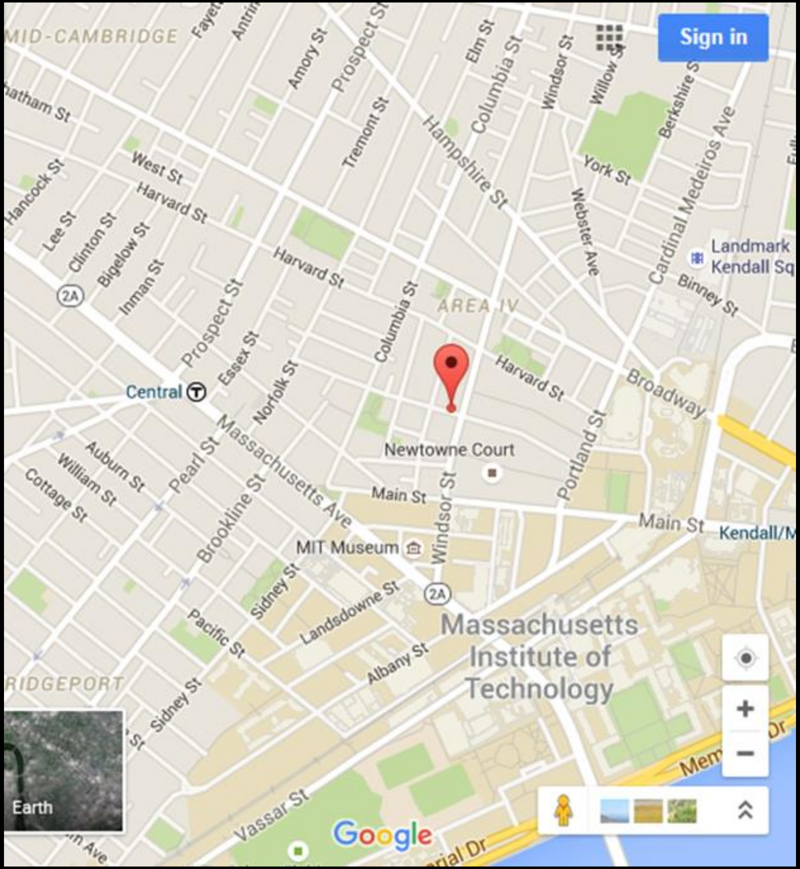
Data from 85 dust sensors in 7 cities,
via datacanvas.org



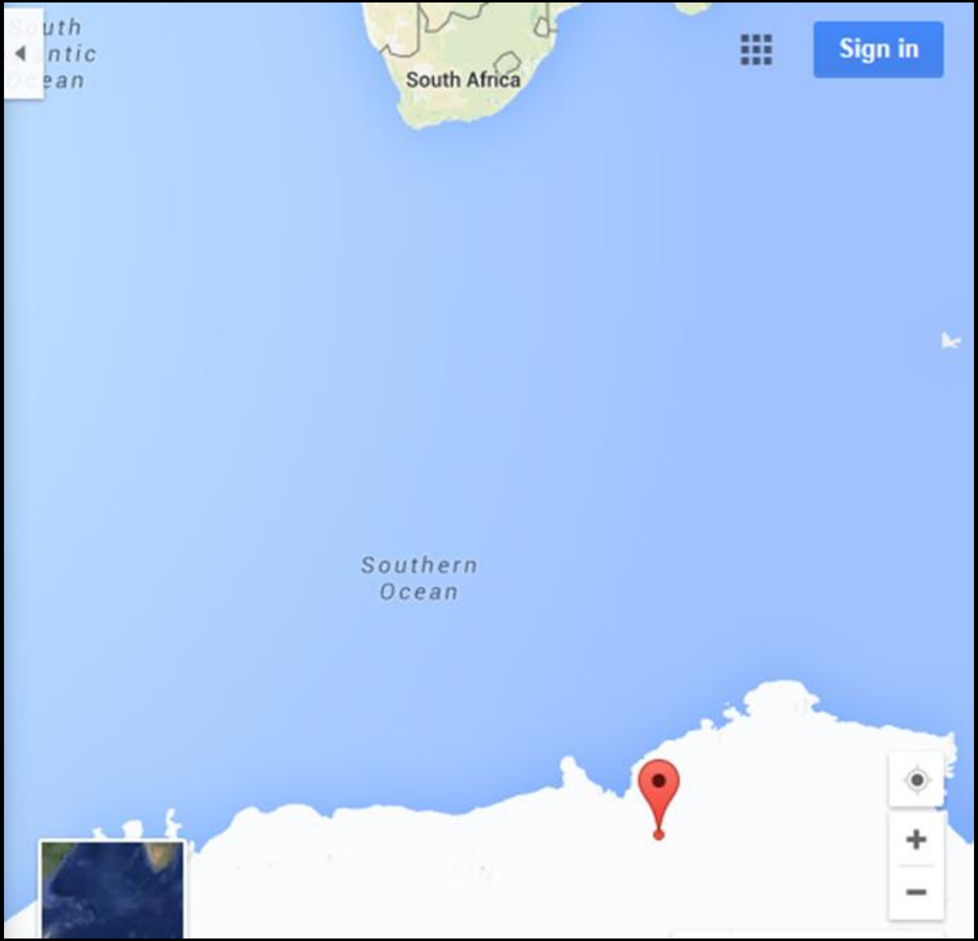
These two have similar, and unusual, dust readings.

However:

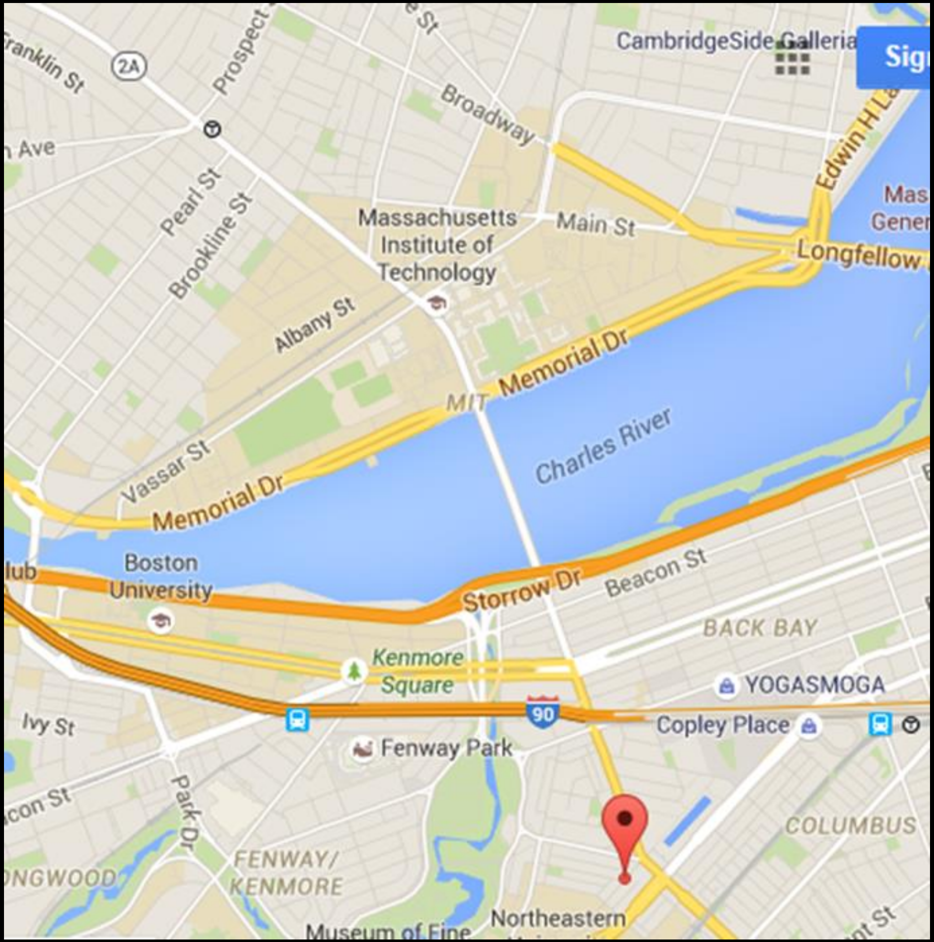




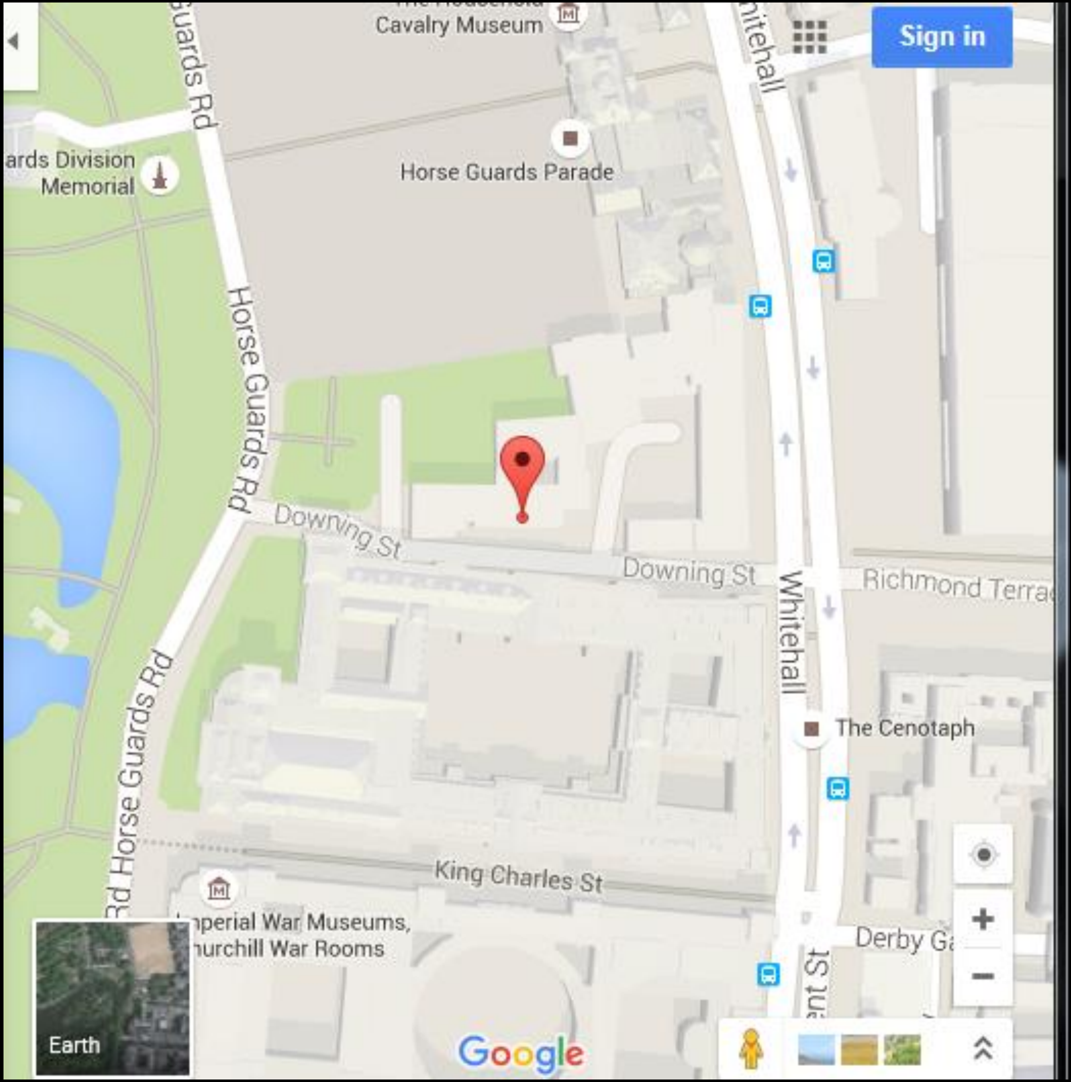
According to their latitude & longitude readings, one is in London and the other in Boston



Later, the first sensor hops from London to Antarctica



Antarctica:	Lat -71.086502,	Long 42.342751
Above:	Lat 42.342751,	Long -71.086502


The Household Cavalry Museum
Sign in
Guards Rd
Whitehall
Guards Division Memorial
Horse Guards Parade
Horse Guards Rd
Downing St
Downing St
Richmond Terrac
Whitehall
Horse Guards Rd
The Cenotaph
King Charles St
Imperial War Museums, Churchill War Rooms
Derby Ga
Earth
Google

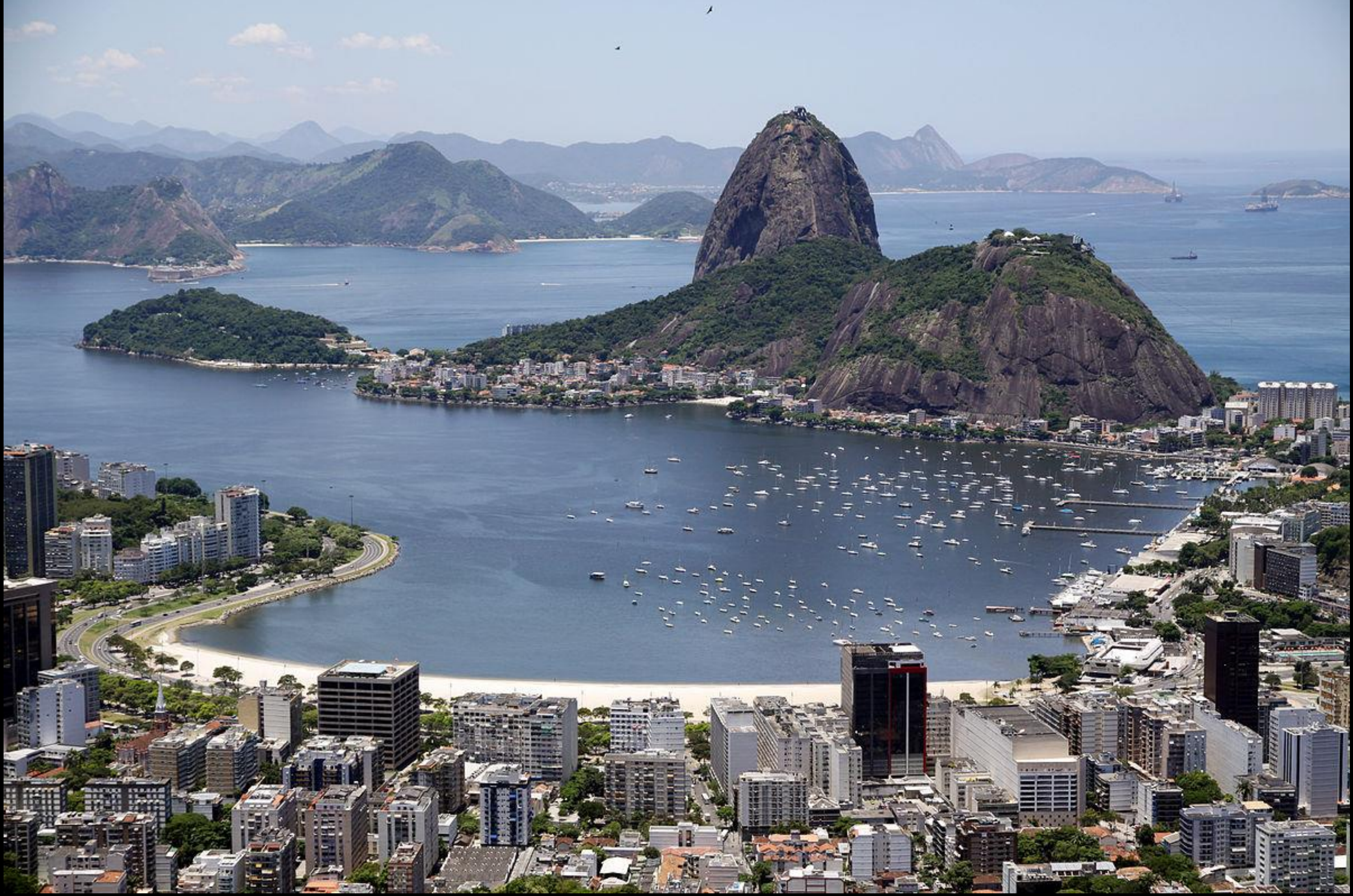
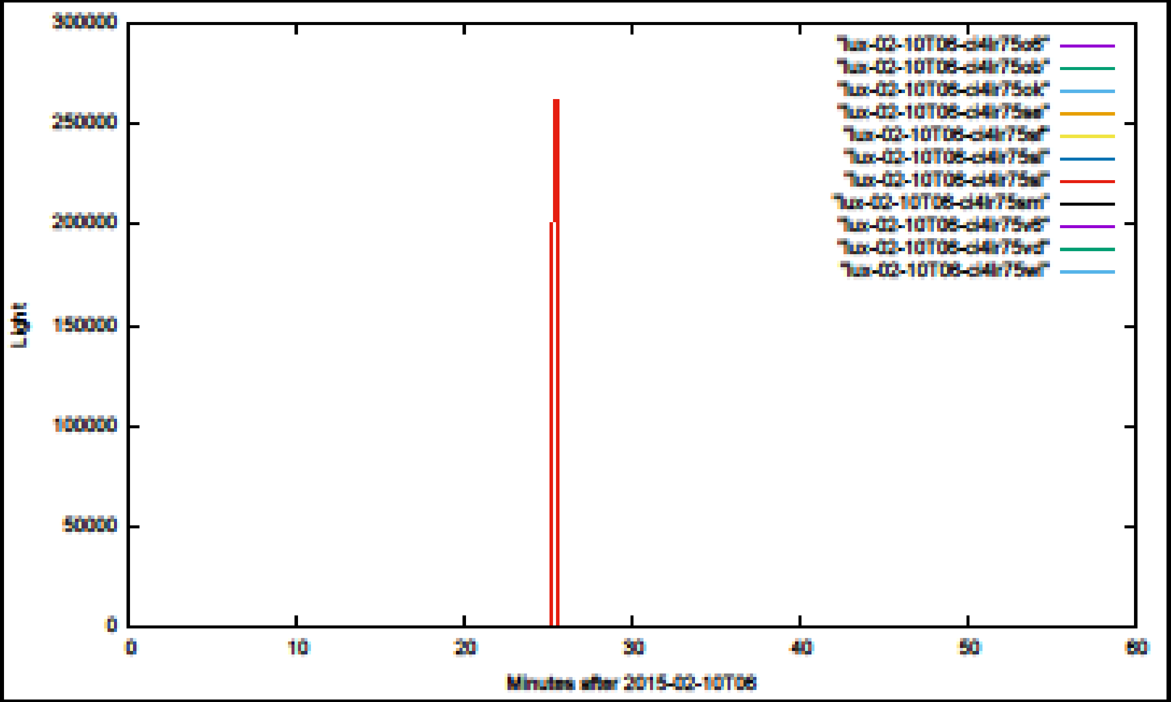


Photo CC BY SA Halley Pacheco de Oliveira, https://en.wikipedia.org/wiki/Sugarloaf_Mountain#/media/File:Enseada_de_Botafogo_e_P%C3%A3o_de_A%C3%A7%C3%BAcar.jpg

Going bump in the night



Peak for one light sensor in the middle of the night

100,000 = full tropical sunlight

Anomaly detection for security

- Anomaly = weirdness: may be unusual but benign
- may be misconfigurations
- Apart from e.g. DDoS, attacks may be stealthy => other weirdness more prominent

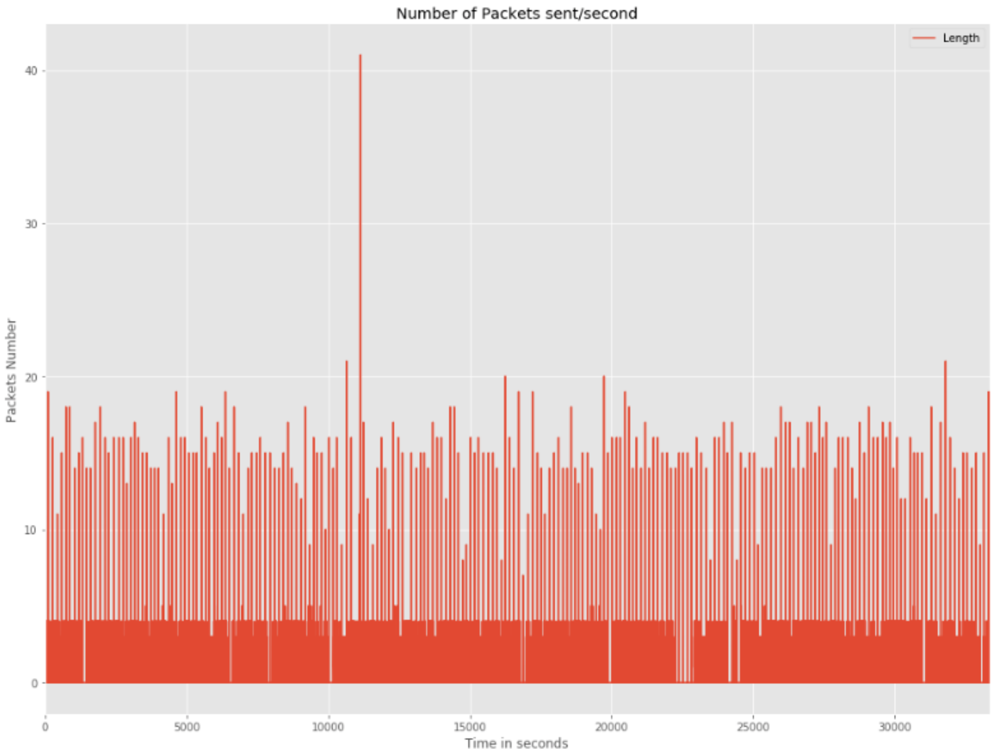
Look for weirdness fitting known attack behaviour, or use weirdness detection just as initial filter

Motion sensor going bump

Abia Amin

designed by freepik.com

Wemo motion sensor: normal behaviour

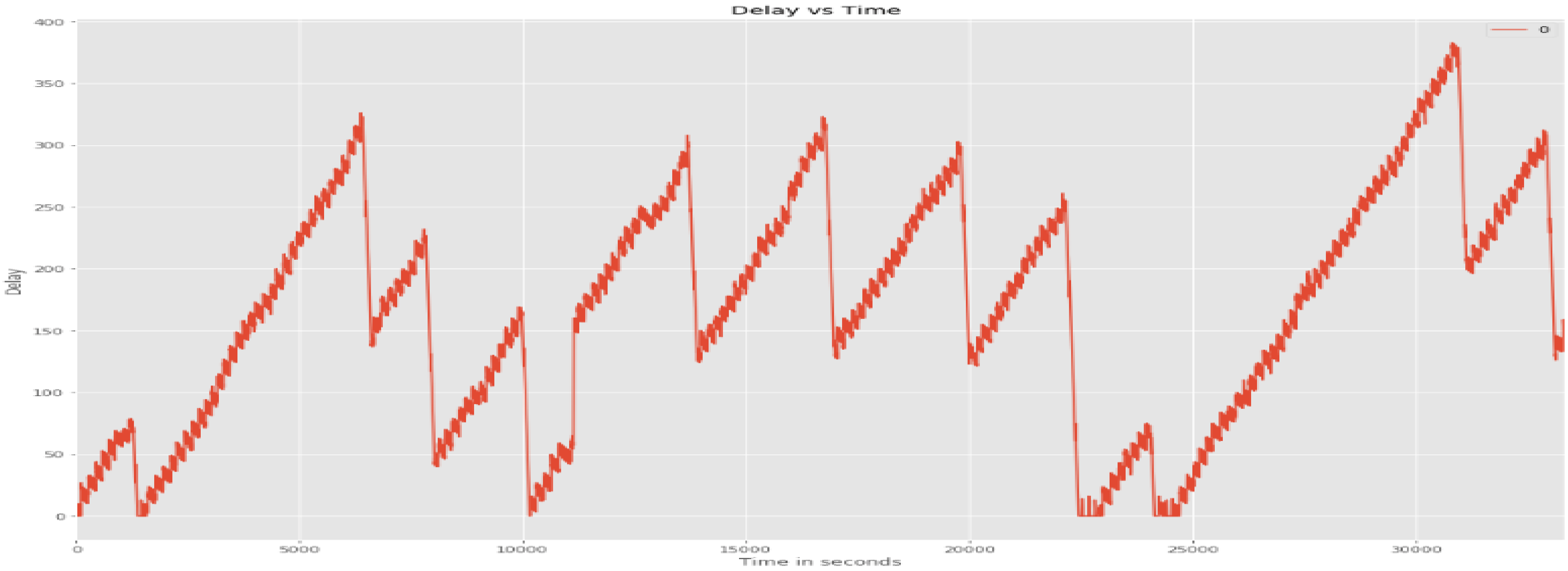


35000 secs of data
Usually below 20 packets/second, peak around 40

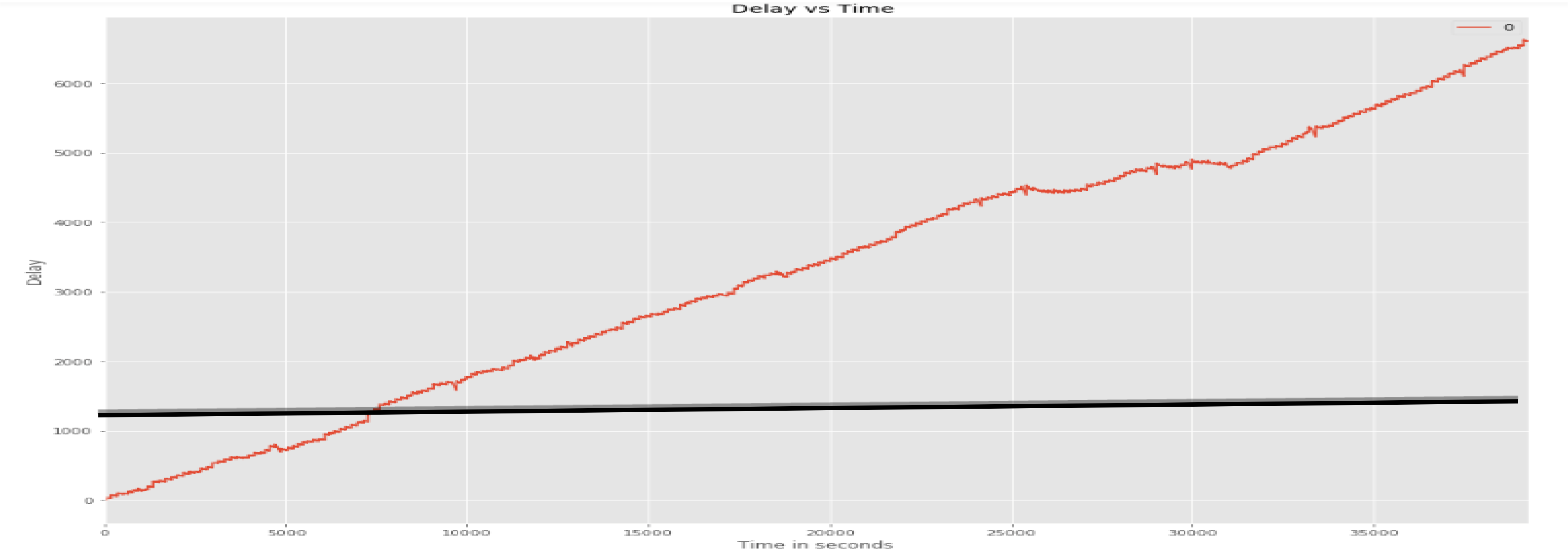
Use CCDF to estimate threshold for queue length at 1 packet/sec

Data Source: A. Hamza, H. Habibi Gharakheili, T. Benson, V. Sivaraman, "Detecting Volumetric Attacks on IoT Devices via SDN-Based Monitoring of MUD Activity", ACM SOSR, San Jose, California, USA, Apr 2019.

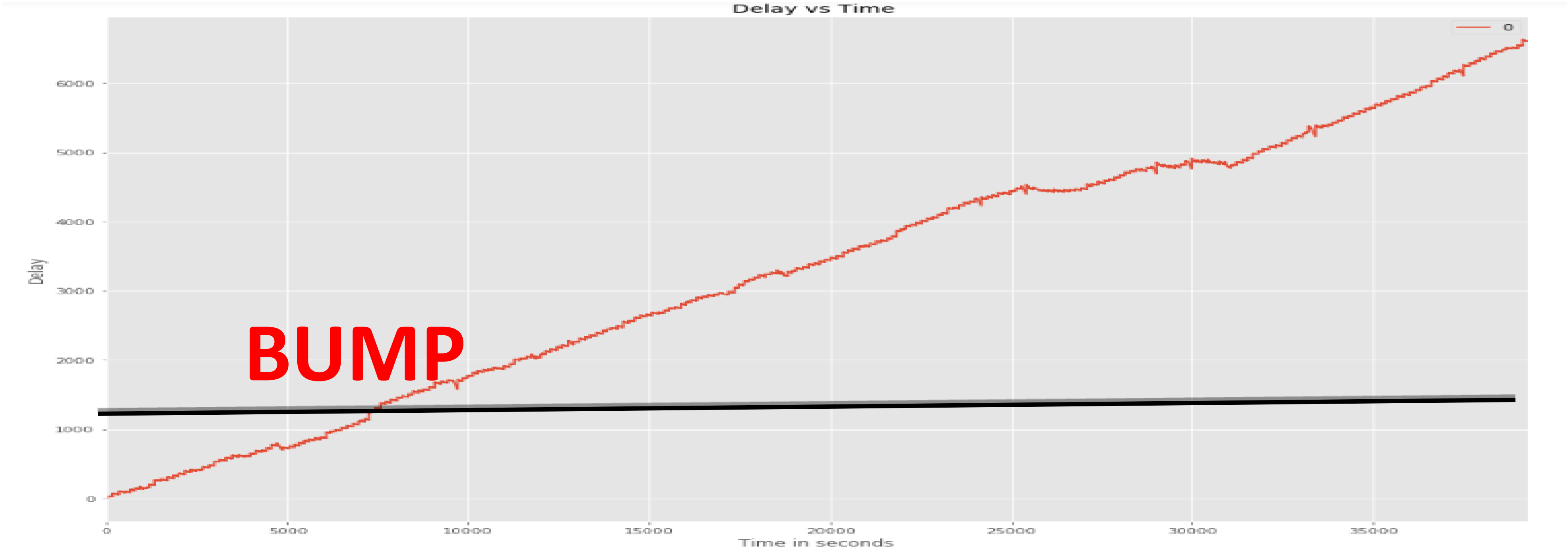
Queue length vs time: normal behavior
max value observed < 400



Queue length vs time: SYN flood attack crosses threshold of 1250



Queue length vs time: SYN flood attack crosses threshold of 1250



How to hear the Bump

designed by freepik.com

Broken rules

- connections to/from forbidden addresses/protocols
- intrusion/malware signature detection rules,
  esp. many rules by one Thing / one rule by many Things
- Thing moves somewhere it shouldn’t
- forbidden control hierarchy zone connections,
  esp. external zone ↔ cell zone
- actions forbidden by policy

Suspicious combinations

- multiple failed logins in short time
- frequent configuration changes or booting attempts
- privilege escalation moving across control hierarchy zones
- Thing often connects to another Thing, followed by attempted privilege escalation by the other Thing
- sequence involving multiple Things known to be used in attacks

Weirdness

- compared to past behaviour of Thing
- compared to other Things of same type / location

- sensor near Thing (eg motion sensor, heat sensor, camera) detects ***weirdness*** or damage, then Thing changes behaviour
- similar ***weirdness*** very close in time by multiple Things
- ***weirdness*** beginning with one Thing, copied by close Things
- ***weird*** items or totals on phone bills
- Thing sending out ***weirdly*** large volume of data

Image from Freepik.com

Going **Bump** in the night

- weird actions by a Thing in the night

- configuration changes in the night
- admin logins in the night
- password changes in the night
- similar actions by multiple Things in the night
- login attempts by multiple Things in the night

Maroochy Shire Sewage Incident, 2000

https://cams.mit.edu/wp-content/uploads/2017-09.pdf

Historical interlude 2: Defending the Castle

designed by freepik.com

Gary Danvers/gcdnz on Flickr
https://www.flickr.com/photos/gcdnz/41473660210/

Niall Watson/niallclairewatson on Flickr
https://www.flickr.com/photos/niallclairewatson/395830408/

Image: cc BY reynermedia on Flickr,
https://www.flickr.com/photos/89228431@N06/11080409645/
Anecdote: David Rogers, “IoT security attack surfaces exposed”,
https://iotsecurityfoundation.org/iot-security-summit-2015/

Jason Staggs on wind farms

No authentication or encryption of control messages
Insecure remote management services
Easily guessable or vendor-default passwords
No network segmentation between turbines
Extremely weak physical security

Quote from ‘17 Def Con talk. More details: Jason Staggs, David Ferlemann, Sujeet Shenoi, “Wind farm security: attack surface, targets, scenarios and mitigation” *IJCIP* 17: 3-14, 2017
https://www.sciencedirect.com/science/article/pii/S1874548217300434

Jason Staggs on wind farms

No authentication or encryption of control messages

Insecure remote management services

Easily guessable or vendor-default passwords

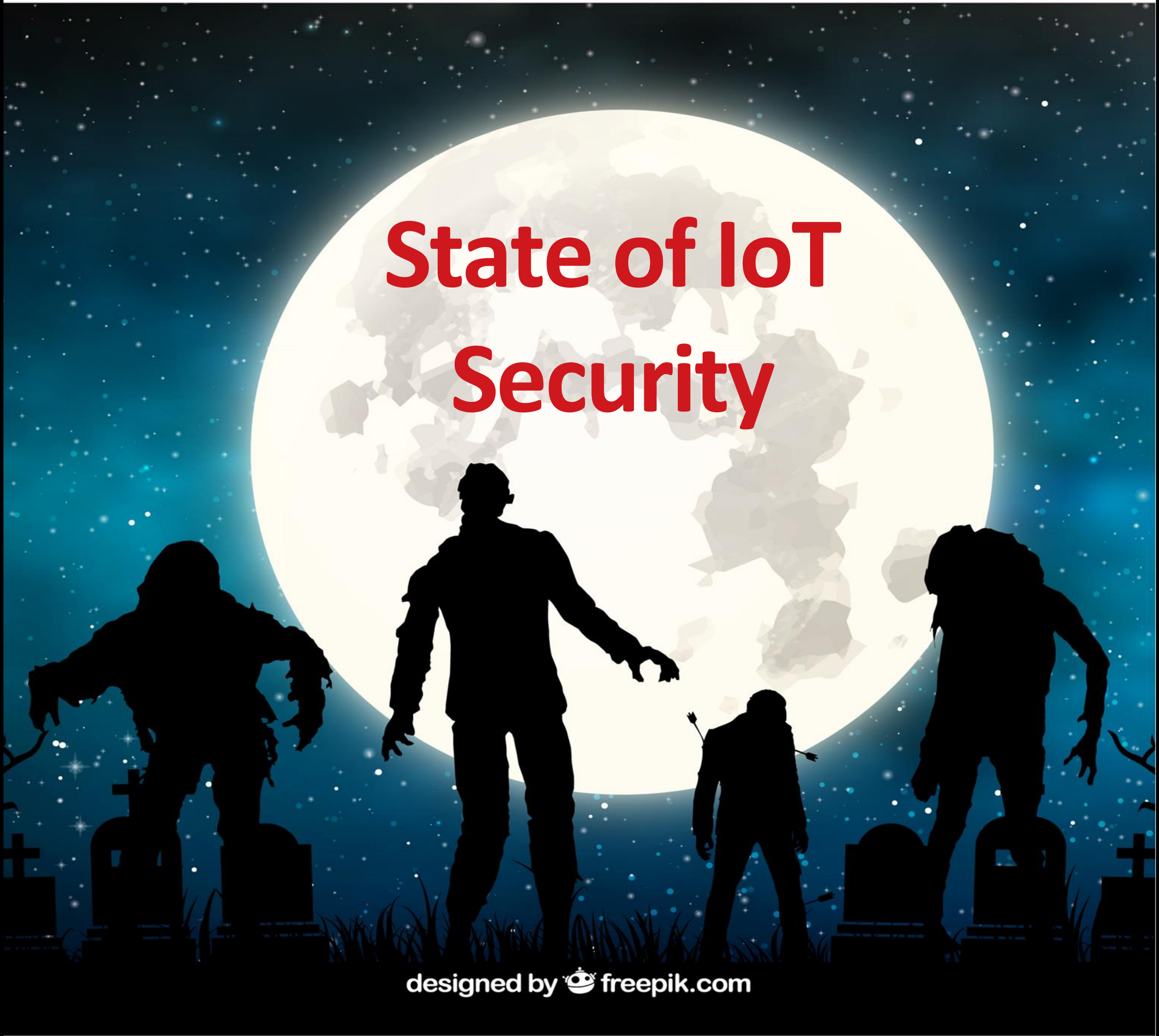
No network segmentation between turbines

Extremely weak physical security

Exactly what we would expect from Industrial Control Systems

Quote from ‘17 Def Con talk. More details: Jason Staggs, David Ferlemann, Sujeet Shenoi, “Wind farm security: attack surface, targets, scenarios and mitigation” *IJCIP* 17: 3-14, 2017 https://www.sciencedirect.com/science/article/pii/S1874548217300434

State of IoT Security



designed by freepik.com

Disco Pants o0mouse0o aka Russell Couper, Coupertronics
http://www.instructables.com/id/Disco-pants/

Why so pants?

- New tech
- Hooking up old tech
- Early Things still in use
- Limited resources on Thing
- Big attack surface
- Long supply chains
- Patch development/distribution difficulties
- Not even trying

Image adapted from Fail stamp (cc) BY Nima Badiey/ ncc_badiey on Flickr, https://www.flickr.com/photos/ncc_badiey/3095099782

Suggestions

- Security development processes / platforms
- Process for responding to vuln report
- Supply chain info
- Business models
- **Detection**
- Don’t fund insecure Things
- Don’t put insecure options in Thing security standards
- Regulation & Lawyers
- Chuck out old Things
- Try not to be part of the problem

Photo of Secret Pizza Party poster in Detroit CC BY CAVE CANEM/bewareofdog, https://www.flickr.com/photos/bewareofdog/284770877/

Things That Go Bump In The Night

Miranda Mowbray

designed by freepik.com