

Cybersecurity and Internet-of-Things (IoT)



João Pedro Dias

UNIS Digital Seminars
22 Oct 2024

Hello 🙌

📍 João Pedro Dias

📍 Porto, Portugal

✉️ PhD in Informatics Engineering



🛠️ Team Lead and Lead Architect



✉️ jpdias@outlook.com // jpdias@pm.me

🔗 <https://jpdias.me>

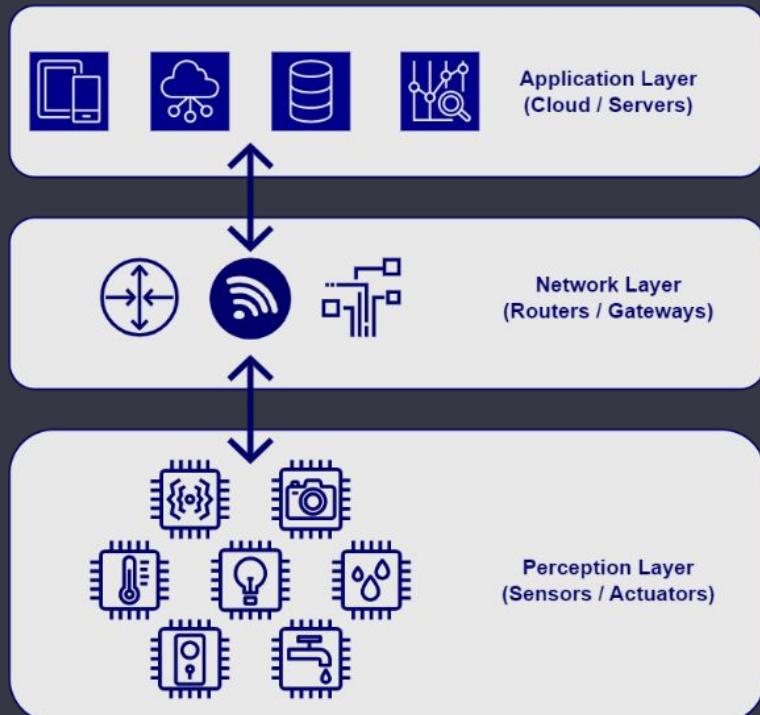


Magic Smoke,
https://en.wikipedia.org/wiki/Magic_smoke

Agenda

- Internet-of-Things
- Protocols
- Encryption
- Common security issues
- Real-world Cases
- Privacy concerns
- What's next?

Internet-of-Things (IoT) / Operational Technology (OT)



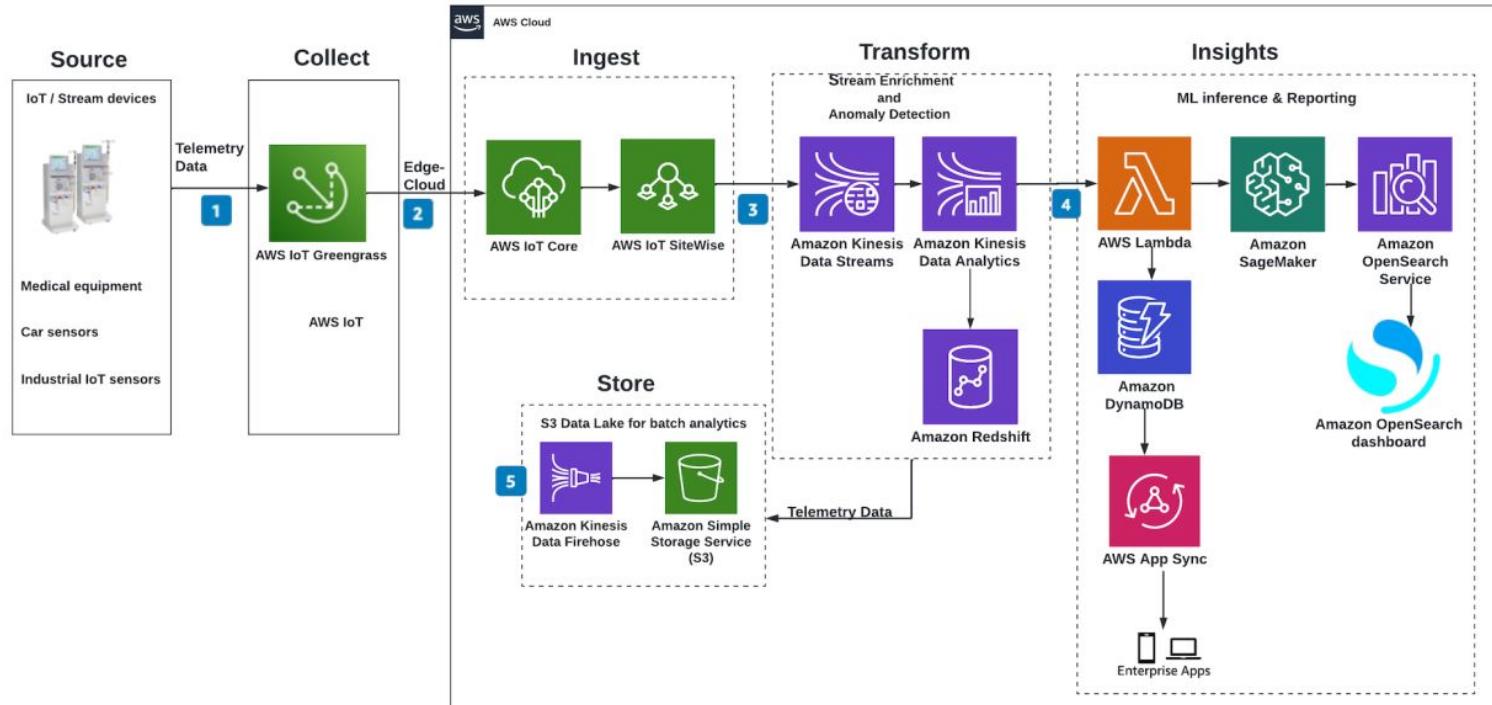
"Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks."

Internet of things, https://en.wikipedia.org/wiki/Internet_of_things

Example: Netatmo



Internet-of-Things in the (AWS) real-world



Building event-driven architectures with IoT sensor data,

<https://aws.amazon.com/blogs/architecture/building-event-driven-architectures-with-iot-sensor-data/>

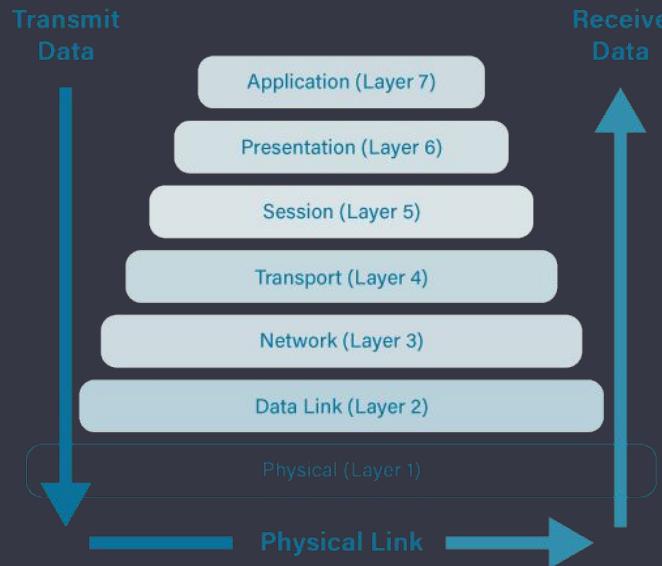
IoT connects everyday things to the palm of our hands.

Protocols ensure that all parts of the system are able to communicate between themselves.



What's a protocol?

The 7 Layers of OSI

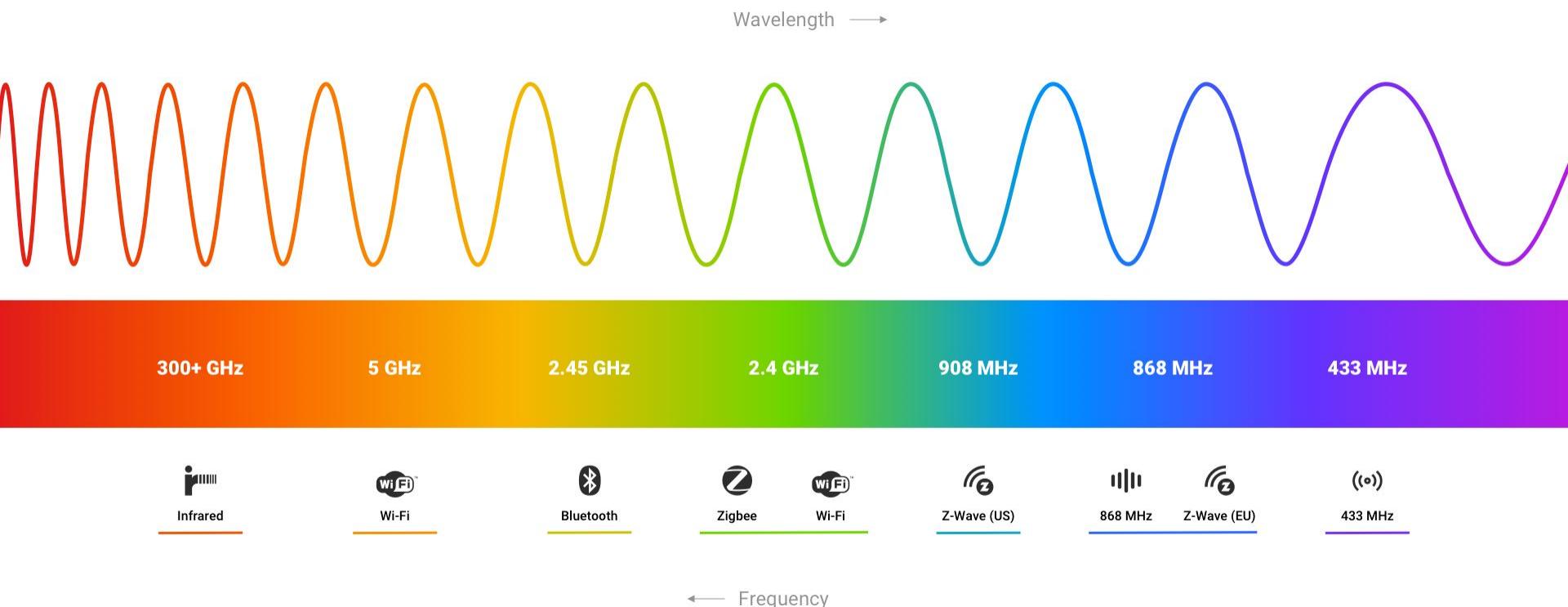


"(...) a set of established rules that specify how to format, send and receive data (...)"

What is a network protocol?,

<https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/>

Common IoT Protocols

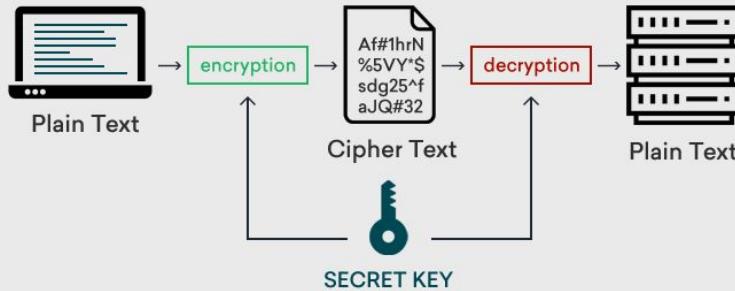


Protocol's tradeoffs

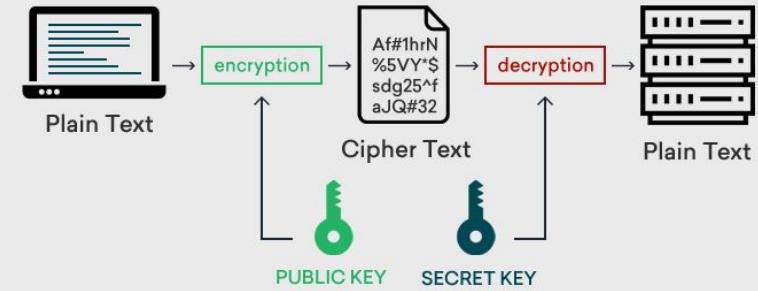
	Infrared	Wi-Fi	Zigbee/ Matter	Bluetooth	Z-Wave	433 MHz	4G	5G
Frequency	300 GHz	5 GHz / 2.4 GHz	2.4 GHz	2.4 GHz	865 – 926 MHz	433 MHz	700-800 MHz 1800MHz 2.6 GHz	700 MHz 3.5 GHz
Useful Range	5m	30m	15m	15m	40m	100m	6.5km	5km
Power Usage	low	high	low	low	low	low	high	high
Affordability	✓	✓	✓	✓	✗	✓	✗	✗
Encryption	✗	✓	✓	✗	✓	✗	⚠	✓
Low Interference	✓	✗	✗	✗	✓	✓	✓	✗
Gateway Not Required	✗	✓	✗	✗	✗	✗	✓	✓

Encryption Types

Symmetric encryption

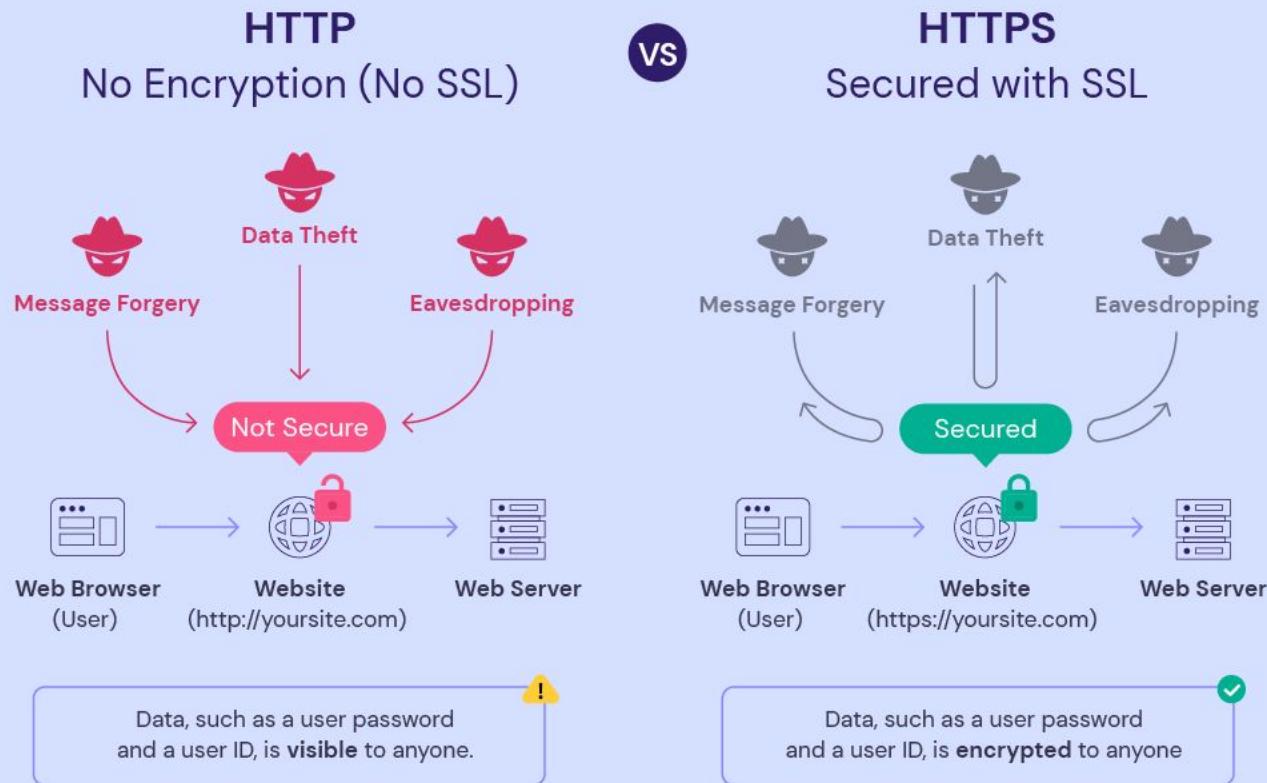


Asymmetric encryption



Symmetric vs Asymmetric Encryption – What Are the Difference?,
<https://www.clickssl.net/blog/symmetric-encryption-vs-asymmetric-encryption>

Example: HTTP versus HTTPS



Why is not everything encrypted by default?

Why is not everything encrypted by default?

Encryption is a computational heavy task,
and can also increases communication payload size.

Encryption also does not solve all problems in communication security nor
in IoT, it is just a piece of the puzzle



CIA Triad

IoT Security Issues (OWASP Top 10 IoT)

1	Weak, Guessable, or Hardcoded Passwords Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.	
2	Insecure Network Services Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...	
3	Insecure Ecosystem Interfaces Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.	
4	Lack of Secure Update Mechanism Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.	
5	Use of Insecure or Outdated Components Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.	
6	Insufficient Privacy Protection User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.	
7	Insecure Data Transfer and Storage Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.	
8	Lack of Device Management Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.	
9	Insecure Default Settings Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.	
10	Lack of Physical Hardening Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.	



Real-world cases

WiFi networks



Unauthorized Access

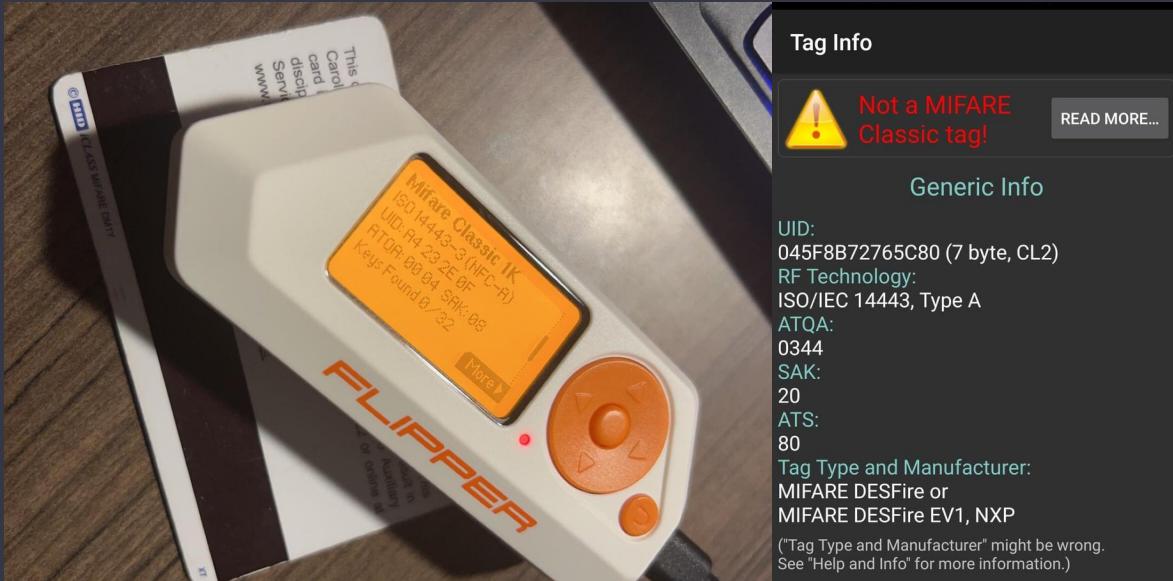
Spoofing

Interference / Flooding

Esri, TomTom, Garmin, Foursquare, METI/NASA, USGS

Wigle.net, <https://wigle.net/>

MIFARE Access Cards



MIFARE Classic: exposing the static encrypted nonce variant... and a few hardware backdoors,
<https://blog.quarkslab.com/mifare-classic-static-encrypted-nonce-and-backdoors.html>

Cloning

Bruteforce

Exposed Video Streams



Information Leak

Bruteforce

Q [REDACTED].180/admin/

158.39.149.180

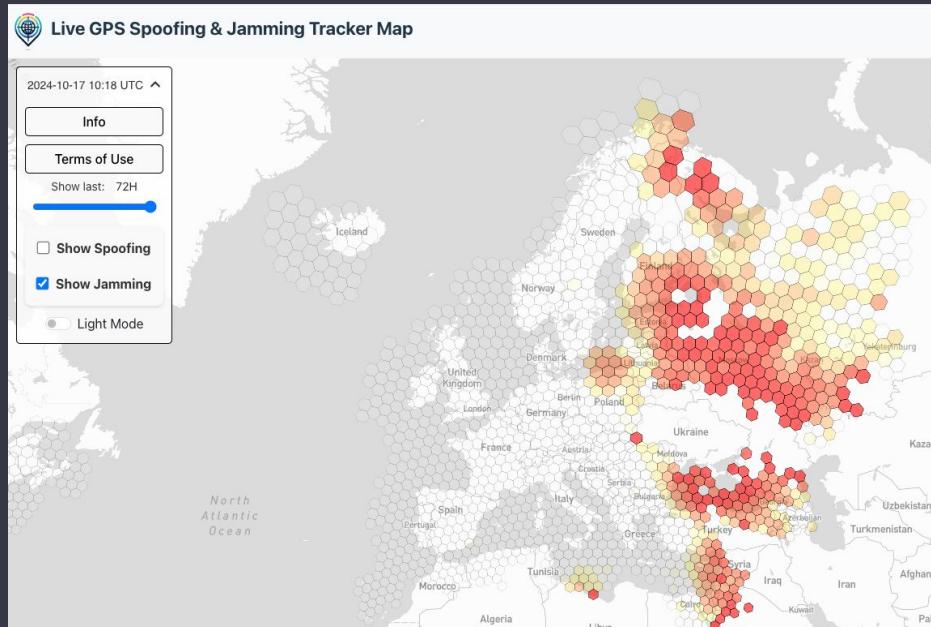
Este site está a solicitar que inicie sessão.

Nome de utilizador

Palavra-passe

Iniciar sessão Cancelar

GPS Jamming



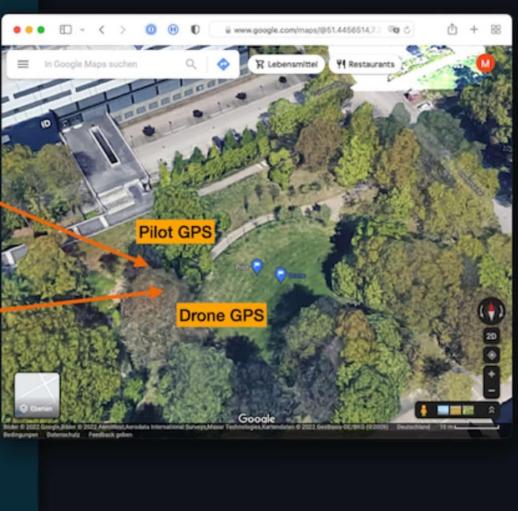
Jamming

GPS Jamming Is Screwing With Norwegian Planes,
<https://www.wired.com/story/gps-jamming-is-screwing-with-norwegian-planes/>

DJI Drones (2023)

Received DroneID packet:

```
{  
    "pkt_len": 88,  
    "unk": 16,  
    "version": 2,  
    "sequence_number": 749,  
    "state_info": 8183,  
    "serial_number": "1k [REDACTED] N1",  
    "longitude": 7.267175834942389,  
    "latitude": 51.44635111984553,  
    "altitude": 40.84,  
    "height": 3.66,  
    "v_north": -1,  
    "v_east": 0,  
    "v_up": -1,  
    "rd_1_angle": -14958,  
    "gps_time": 1649869492647,  
    "app_lat": 51.446316742392554,  
    "app_lon": 7.26710135046944,  
    "longitude_home": 7.267170185366893,  
    "latitude_home": 51.44636830857202,  
    "device_type": "Mavic Air 2",  
    "uuid_len": 19,  
    "uuid": "[REDACTED]",  
    "crc-packet": "267c",  
    "crc-calculated": "267c"  
}
```



Information leak

Spoofing

Jamming

Schiller, Nico, et al. "Drone Security and the Mysterious Case of DJI's DroneID." NDSS. 2023.

Bresser Weather Station



```
rtl_433 version 18.05-361-g22cc97a branch master at 281812161306
Registered 95 out of 119 device decoding protocols [ 1-4 8 11-12 15-21 23 25-26 29-36 38-69 62-64 67-71 73-100 102-103 108-116 ]
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
[R82XX] PLL not locked!
Sample rate set to 250000 S/s.
Tuner gain set to Auto.
Tuned to 433.920MHz.

time : 2018-12-16 13:13:27.578144
model : Bresser 3CH sensor          Id : 76
Channel: 3                         Battery : OK
Modulation: ASK                     Freq : 433.9 MHz
RSSI : -4.7 dB                      SNR : 16.9 dB
                                         Noise : -21.6 dB
                                         Integrity : CHECKSUM

time : 2018-12-16 13:13:47.911839
model : Bresser 3CH sensor          Id : 9
Channel: 2                         Battery : LOW
Modulation: ASK                     Freq : 433.9 MHz
RSSI : -0.1 dB                      SNR : 22.1 dB
                                         Noise : -22.2 dB
                                         Integrity : CHECKSUM
```

Information leak

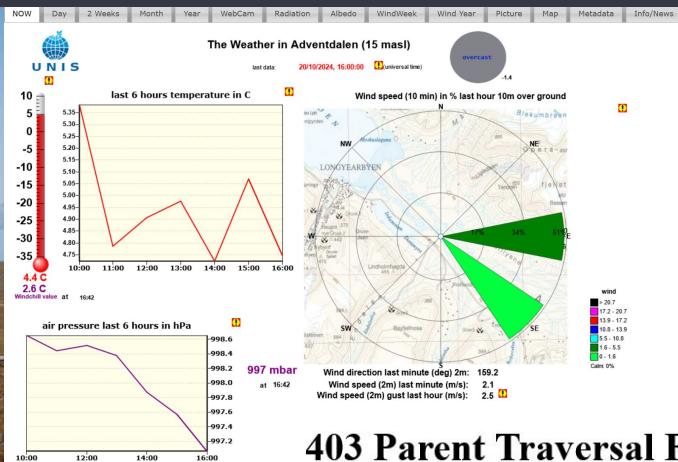
Spoofing

Jamming

Physical Access

rtl_433, https://github.com/merbanan/rtl_433

Campbell Scientific CSI Web Server and RTMC (Real-Time Monitoring and Control) Pro (2024)



Weak Encryption

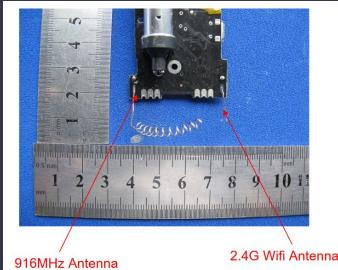
Path Traversal

403 Parent Traversal Forbidden

Parent traversal paths are forbidden.

CISA ICS Advisory, <https://www.cisa.gov/news-events/ics-advisories/icsa-24-149-01>

Netatmo Weather Station



Jamming

Physical Access

Proprietary 916Mhz

Information leak

Did You Remove That Debug Code? Netatmo Weather Station Sending WPA Passphrase in the Clear,

<https://isc.sans.edu/diary/Did+You+Remove+That+Debug+Code+Netatmo+Weather+Station+Sending+WPA+Passphrase+in+the+Clear/19327/> (2015)



What about privacy?

Data Privacy

“(...) individuals can be identified in anonymized datasets and inferences about individuals may be gleaned from aggregated datasets (...)”

Running Apps (Strava)



Using heatmap as a data source, (...) able to ID start and end locations of activities, revealing potential residences. Combined with data from OpenStreetMaps and public records like recent voter registrations, there's a high chance Strava could **reveal your name and home address** to a bad actor.

Fitness tracking app Strava gives away location of secret US army bases,

<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

Strava doesn't seem to have learned much about user privacy since 2018,

<https://www.androidpolice.com/strava-heatmaps-location-identity-doxing-problem/>

Netatmo Base Station Sensors



People at Home



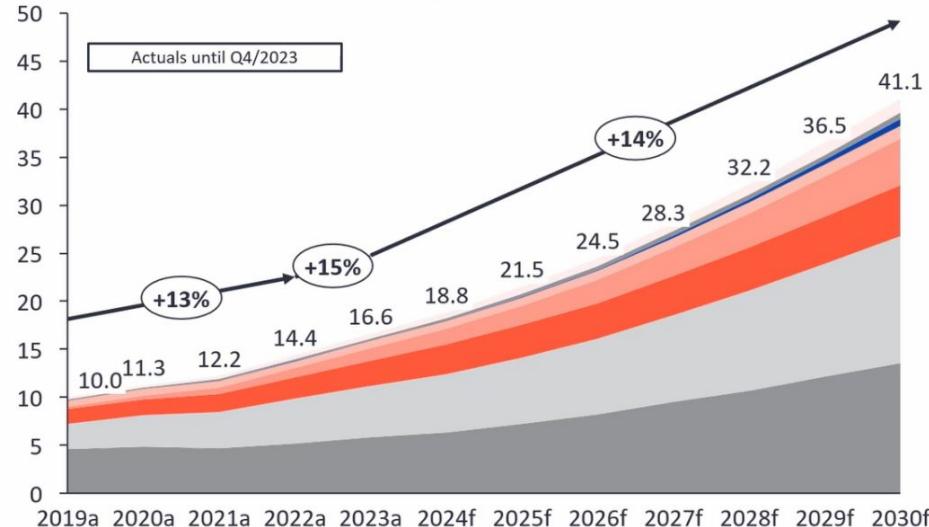
Empty House



What's next?

Global IoT market forecast (in billions of connected IoT devices)

Number of global active IoT connections (installed base) in billions

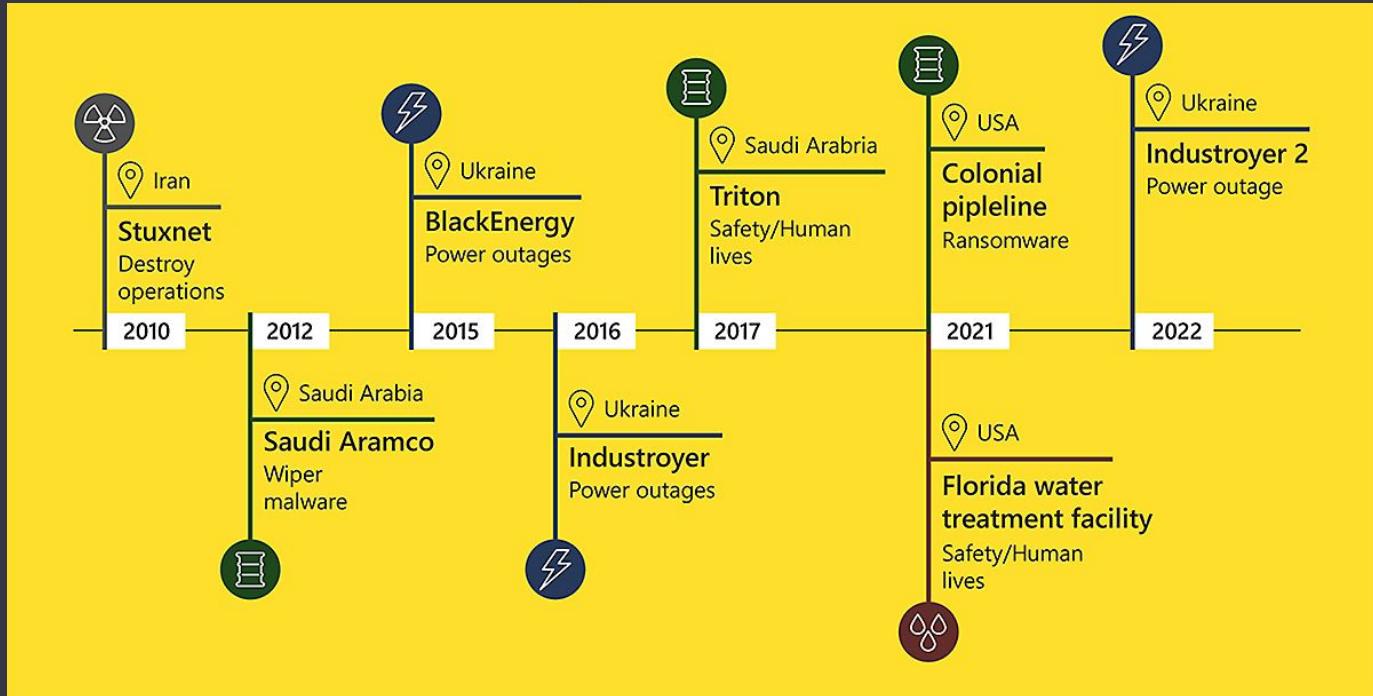


Connectivity type	CAGR 21–23	CAGR 23–30
Other	21%	17%
Wireless neighborhood area networks (WNAN)	15%	14%
Cellular 5G IoT	147%	62%
Wired IoT	4%	9%
LPWA	35%	21%
Cellular IoT (excl. 5G, LPWA)	21%	11%
Wireless local area networks (WLAN)	18%	14%
Wireless personal area networks (WPAN)	12%	13%

XX% = CAGR

Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WMAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

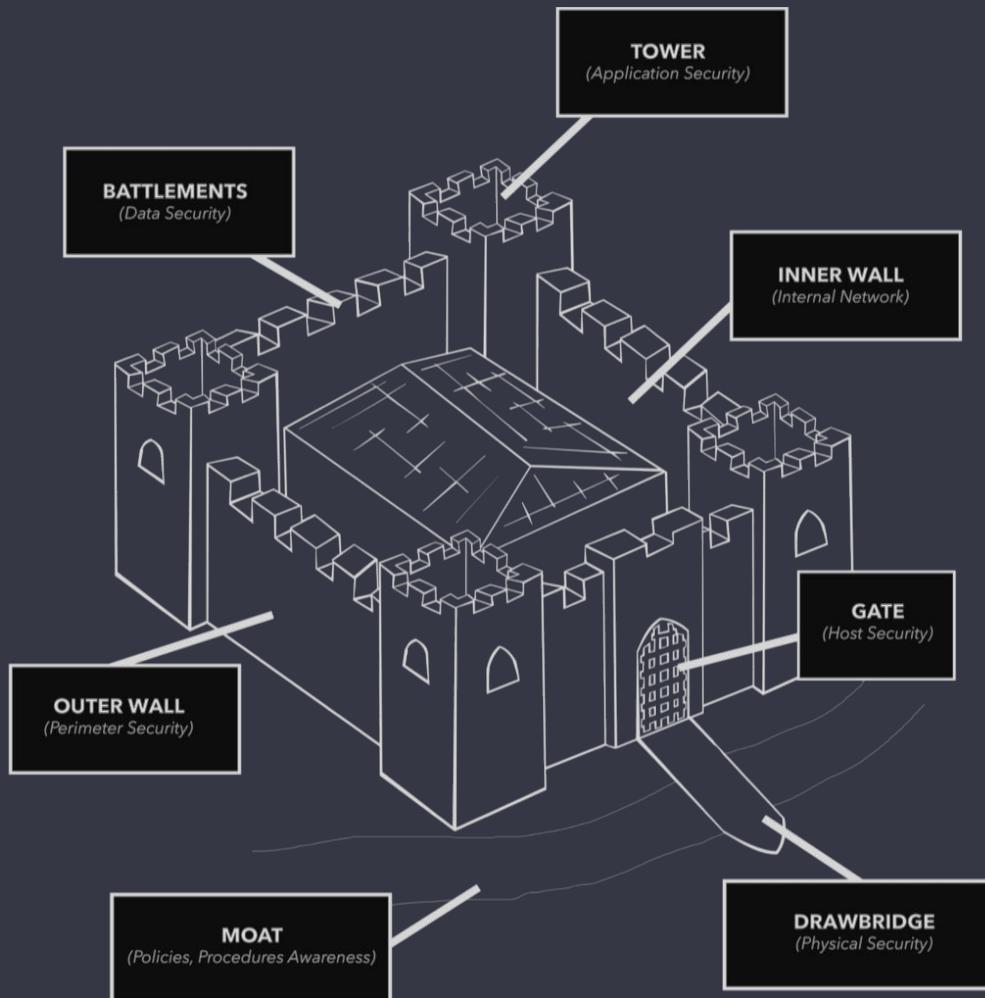
Source: IoT Analytics Research 2024-State of IoT Summer 2024. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.



The convergence of IT and OT,

<https://www.microsoft.com/en-us/security-insider/intelligence-reports/cyber-signals-issue-3-the-convergence-of-it-and-ot>

-
- 1 Secure your smart devices
- 2 Improve networks security
- 3 Ensure data security
- 4 Check your firmware security
- ```
graph TD; 1[1] --- A[Secure your smart devices]; 2[2] --- B[Improve networks security]; 3[3] --- C[Ensure data security]; 4[4] --- D[Check your firmware security]
```



*Thank you!*

João Pedro Dias

✉ [jpdias@outlook.com](mailto:jpdias@outlook.com) // [jpdias@pm.me](mailto:jpdias@pm.me)

🔗 <https://jpdias.me>