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

U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

⚒️Team Lead and Lead Architect

KUEHNE+NAGEL

📨jpdias@outlook.com // jpdias@pm.me

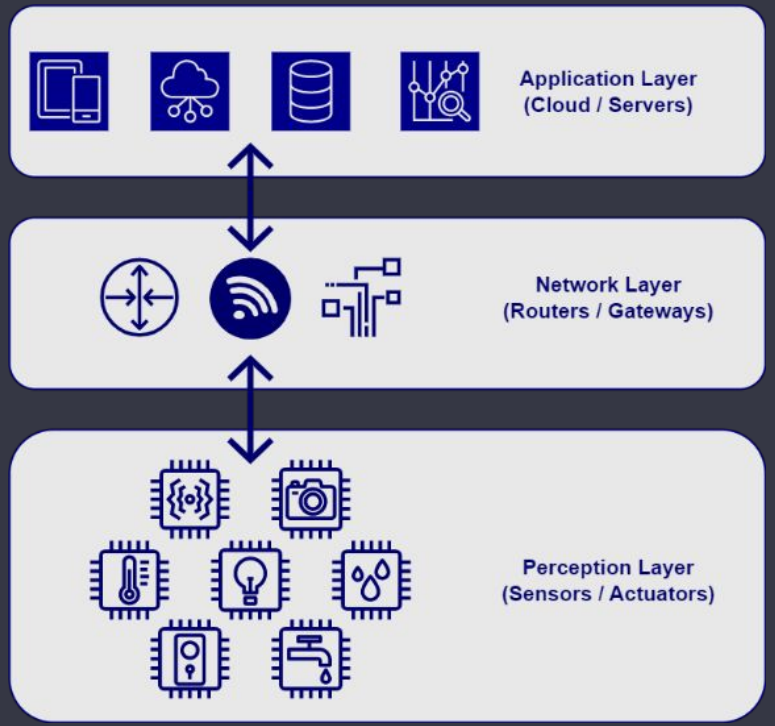
🔗https://jpdias.me

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

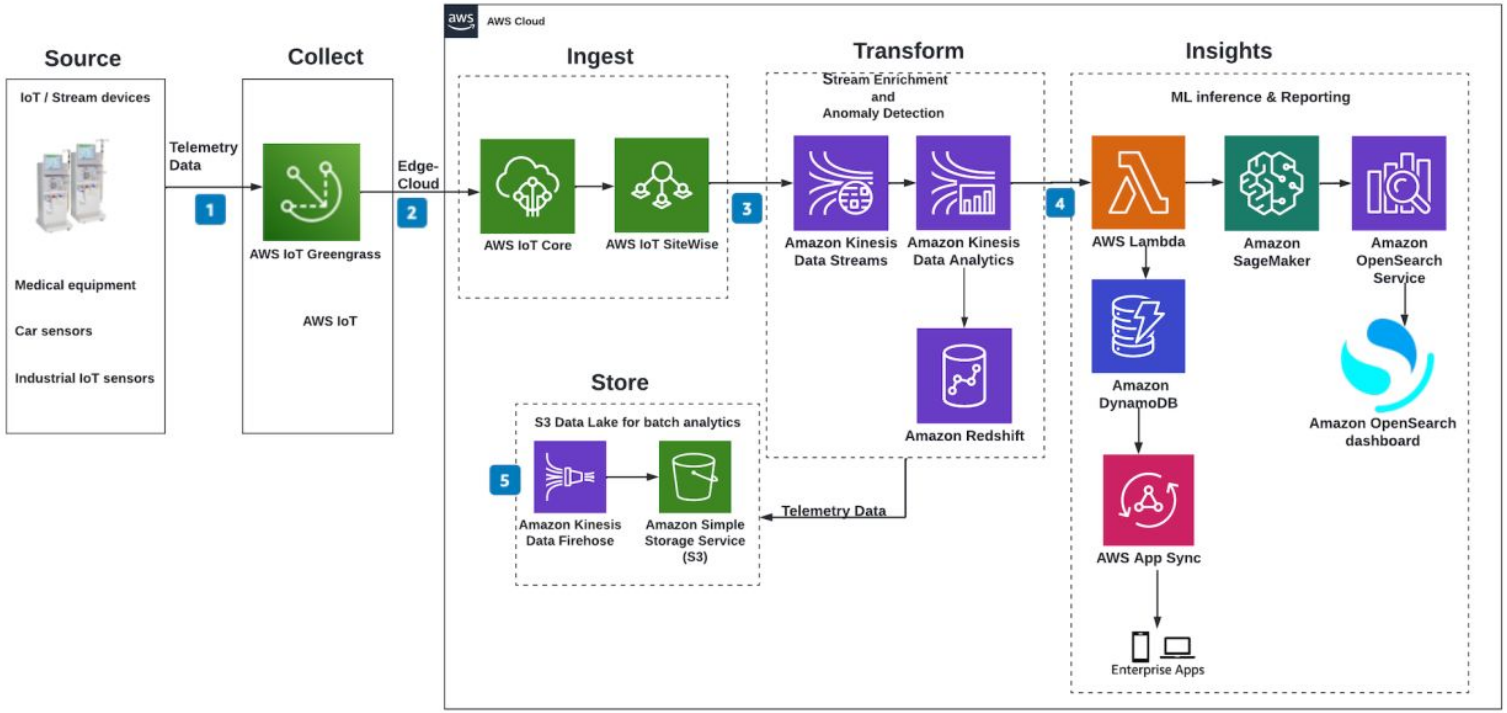
Example: Netatmo

End-user Application

Gateway and Sensors

Sensors

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

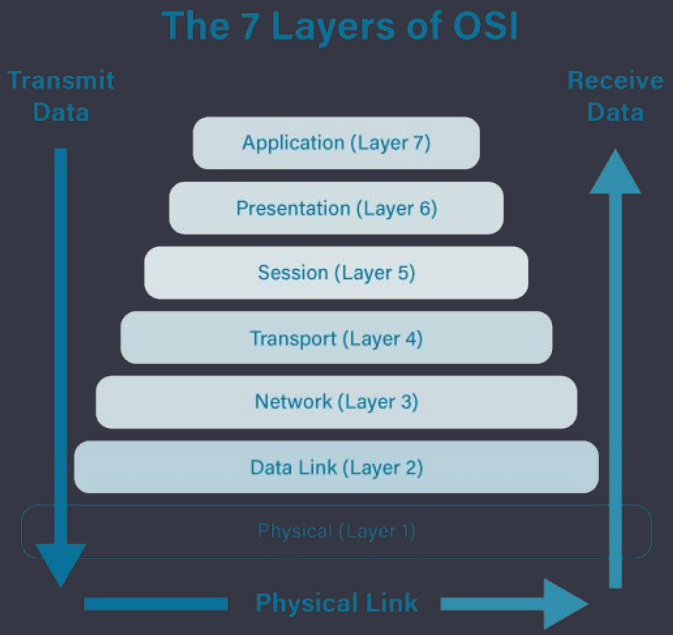


Building event-driven architectures with IoT sensor data,
https://aws.amazon.com/blogs/architecture/building-event-driven-architectures-with-iot-sensor-data/

IoT connects everyday things to the palm of our hands.

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

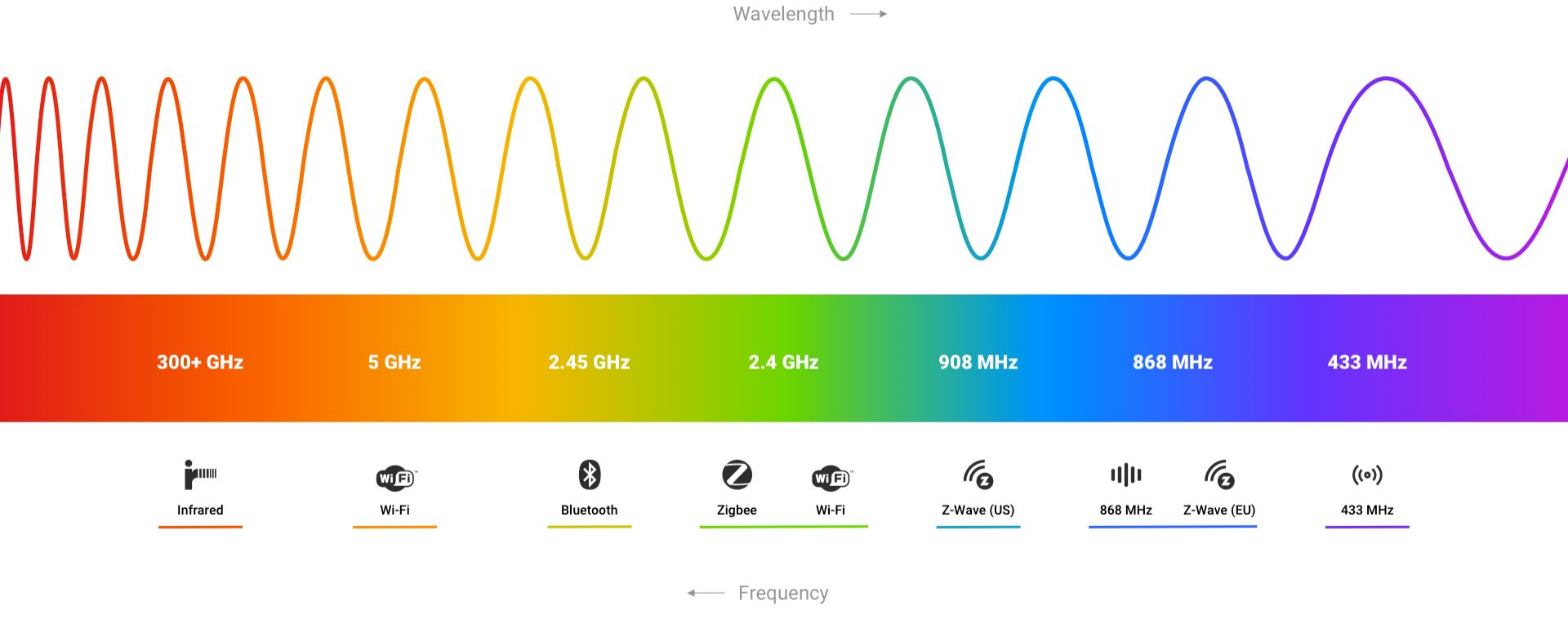
What’s a protocol?



“(...) 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/

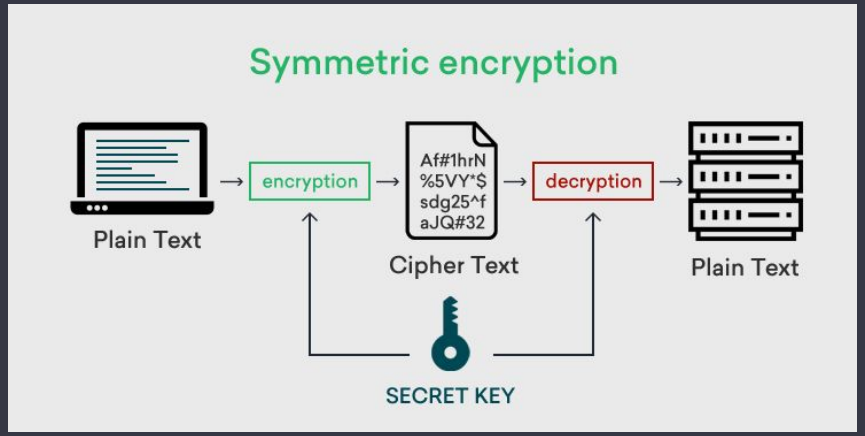
Common IoT Protocols

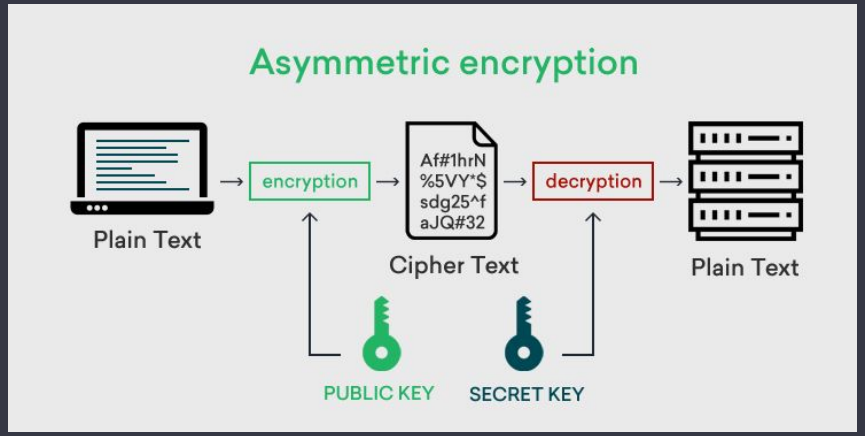


Protocol’s tradeoffs

	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	❌	✅	❌	❌	❌	❌	✅	✅

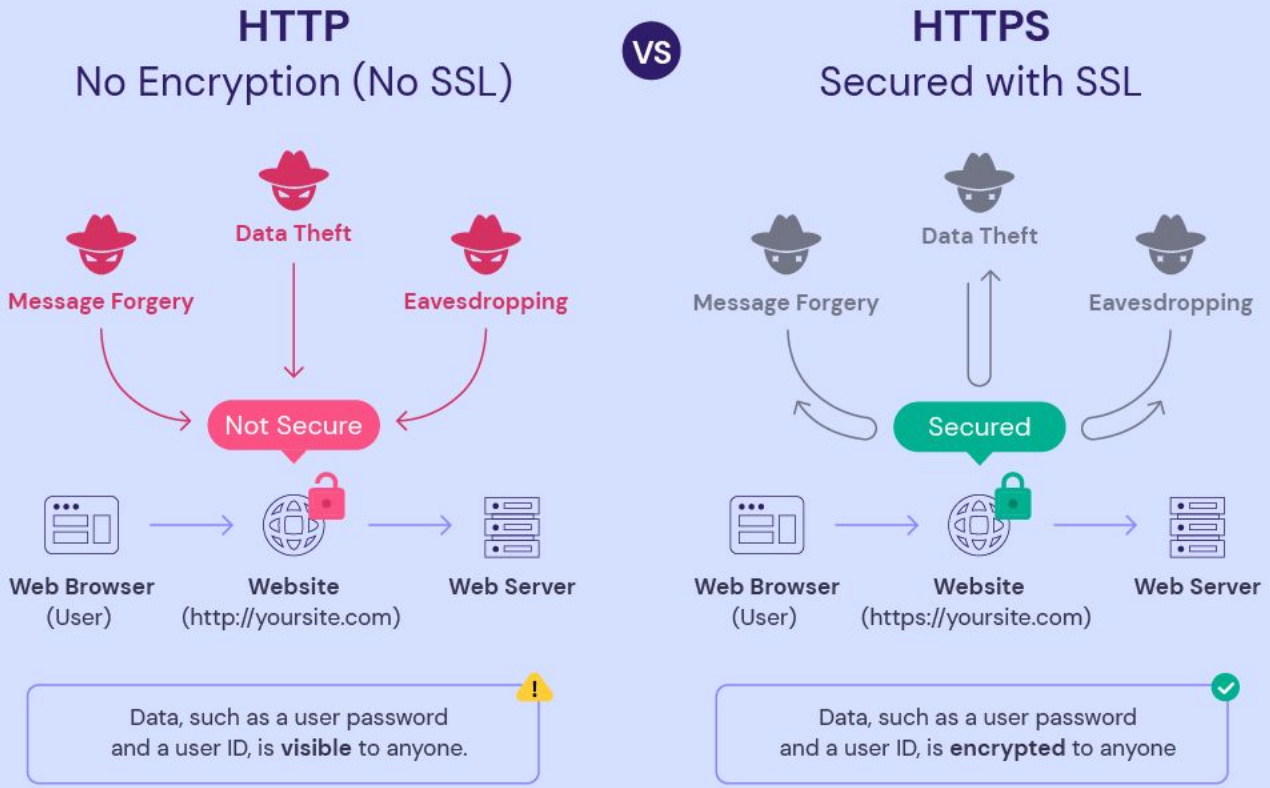
Encryption Types





Symmetric 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?

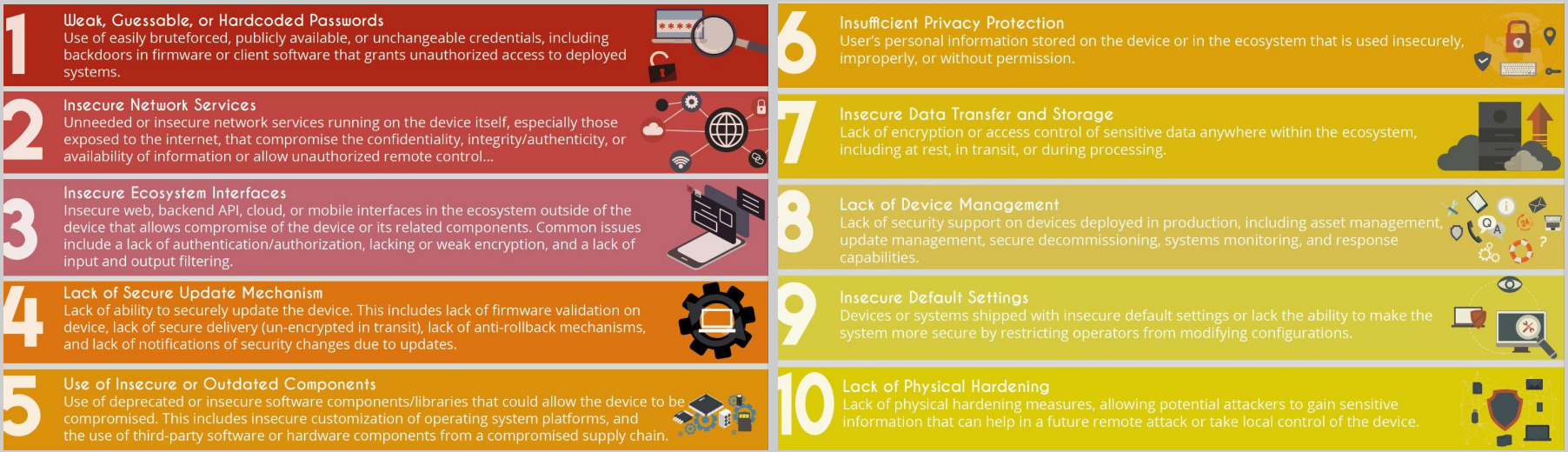
Encryption is a computational heavy task,
and can also increases communication payload size.

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


1
AVAILABILITY
INFORMATION
SECURITY
2
INTEGRITY
3
CONFIDENTIALITY

CIA Triad

IoT Security Issues (OWASP Top 10 IoT)



OWASP Internet of Things Project,
https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

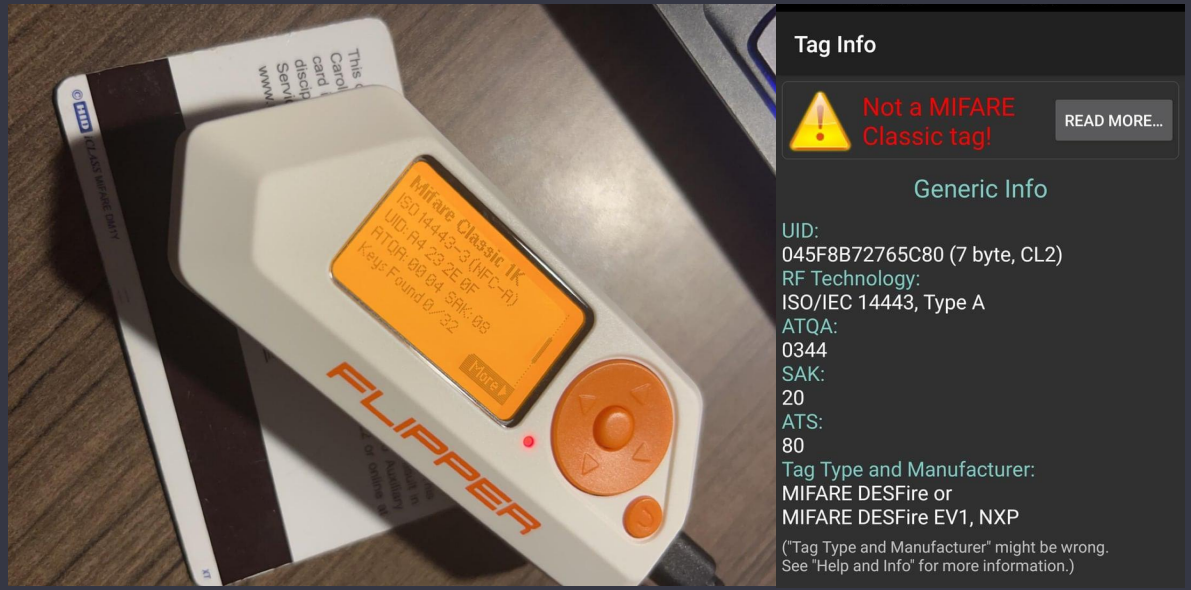
Real-world cases

WiFi networks

- Unauthorized Access
- Spoofing
- Interference / Flooding

WEP - Wikipedia, https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
Wigle.net, https://wigle.net/

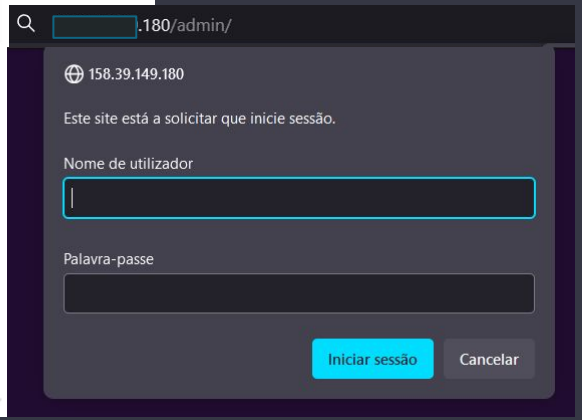
MIFARE Access Cards



	Cloning
	Bruteforce

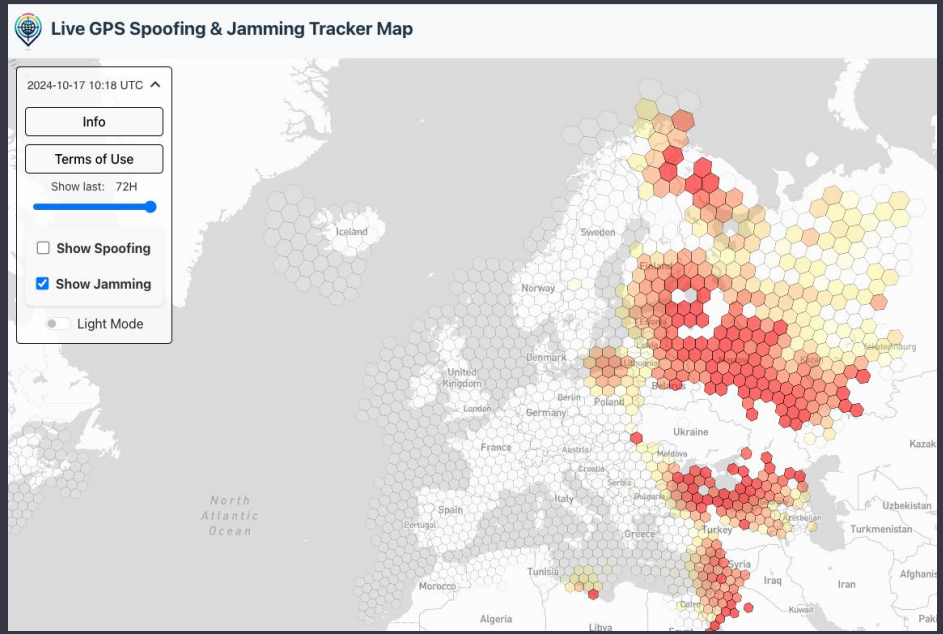
MIFARE Classic: exposing the static encrypted nonce variant... and a few hardware backdoors, https://blog.quarkslab.com/mifare-classic-static-encrypted-nonce-and-backdoors.html

Exposed Video Streams



- Information Leak
- Bruteforce

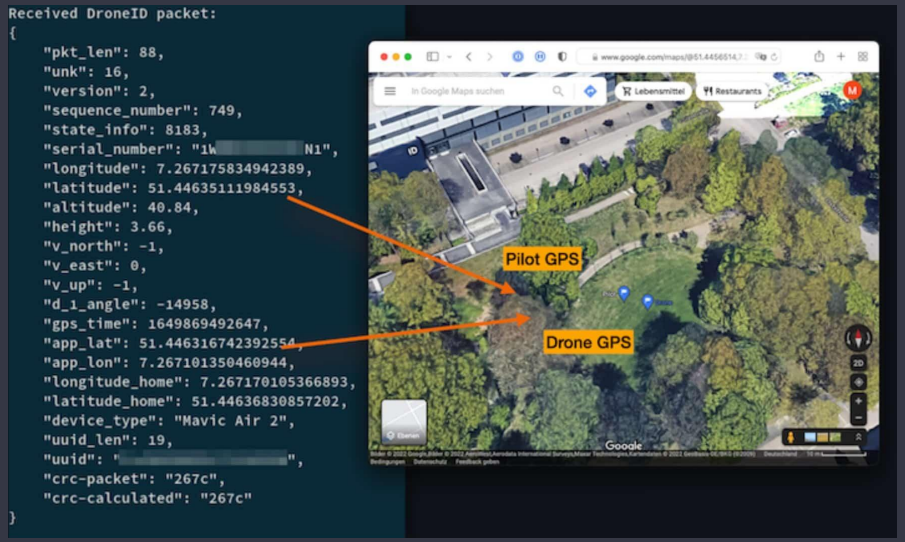
GPS Jamming



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

Jamming

DJI Drones (2023)



- Information leak
- Spoofing
- Jamming

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

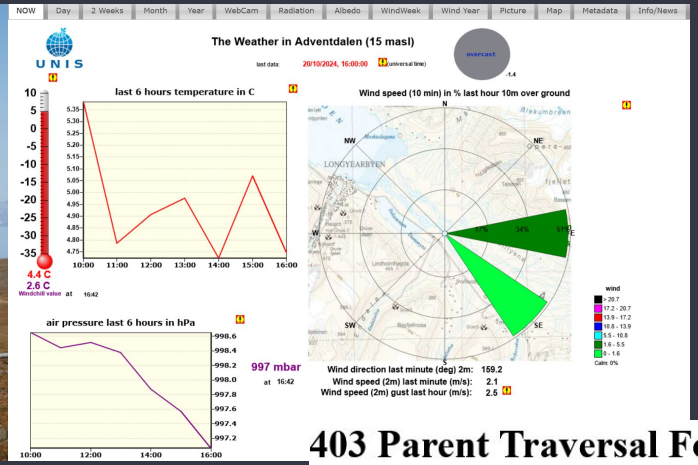
Bresser Weather Station

```
rtl_433 version 18.05-361-g22cc97a branch master at 201812161306
Registered 95 out of 119 device decoding protocols [ 1-4 8 11-12 15-21 23 25-26 29-36 38-60 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          Temperature: 3.11 C     Humidity  : 71 %        Integrity : CHECKSUM
Modulation: ASK               Freq        : 433.9 MHz
RSSI      : -4.7 dB           SNR         : 16.9 dB     Noise     : -21.6 dB

time      : 2018-12-16 13:13:47.911839
model     : Bresser 3CH sensor          Id          : 9
Channel   : 2               Battery     : LOW         Temperature: 17.33 C    Humidity  : 44 %        Integrity : CHECKSUM
Modulation: ASK               Freq        : 433.9 MHz
RSSI      : -0.1 dB           SNR         : 22.1 dB     Noise     : -22.2 dB
```

- 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)



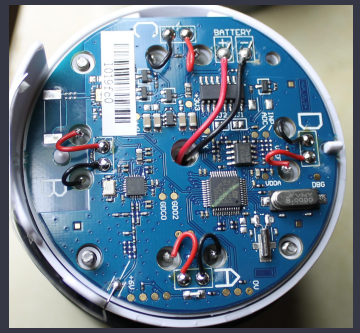
403 Parent Traversal Forbidden

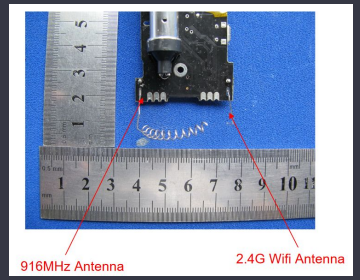
Parent traversal paths are forbidden.

- Weak Encryption
- Path Traversal

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)

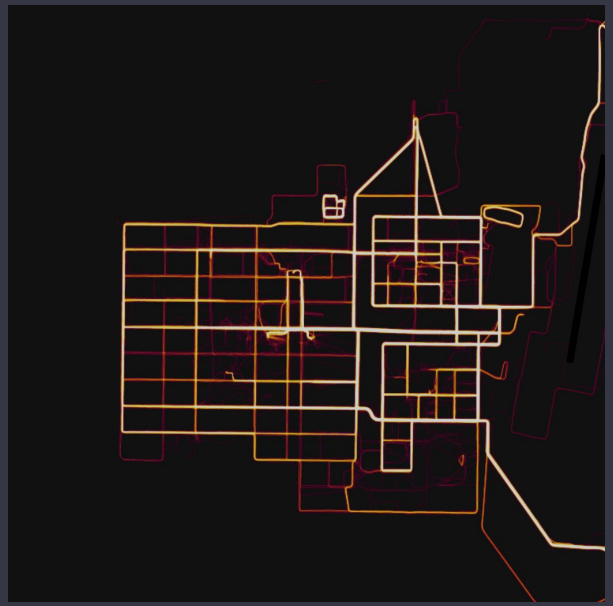
What about privacy?

Data Privacy

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

Data privacy and the Internet of Things, https://en.unesco.org/inclusivepolicylab/analytics/data-privacy-and-internet-things

Running Apps (Strava)

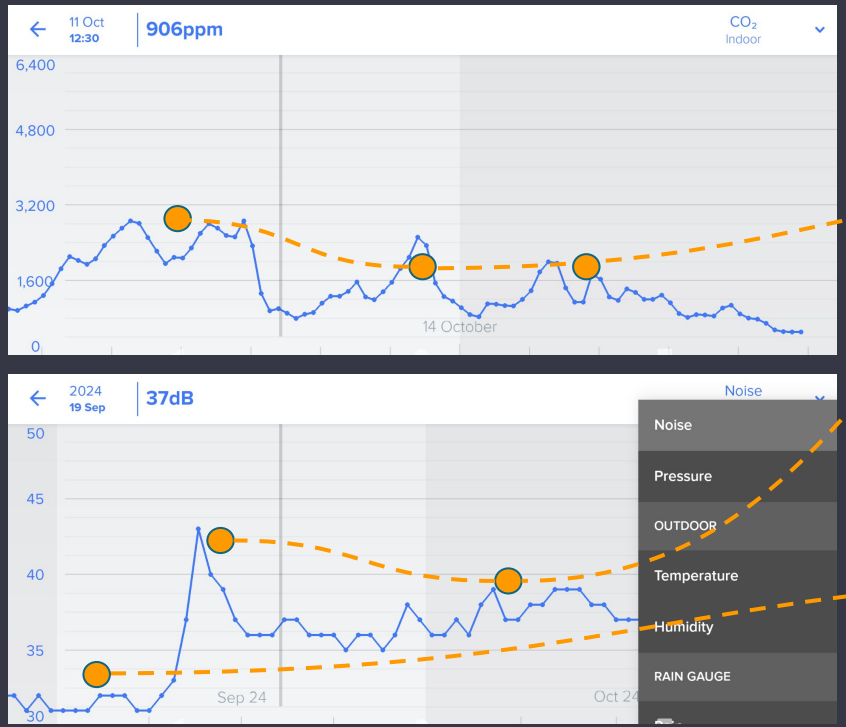


Using heatmap as a data source, (...) able to ID start and end locations of activities, revealing potential residences. Combined with data from OpenStreetMaps and public records like recent voter registrations, there’s a high chance Strava could **reveal your name and home address** to a bad actor.

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-doxxing-problem/

Netatmo Base Station Sensors



People at Home

Empty House

What’s next?

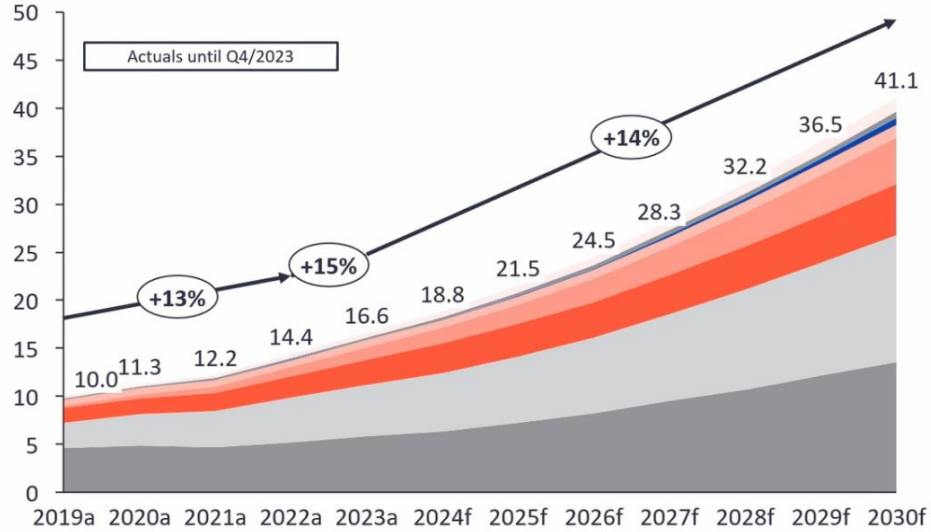
IOT ANALYTICS

September 2024

Your Global IoT Market Research Partner

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

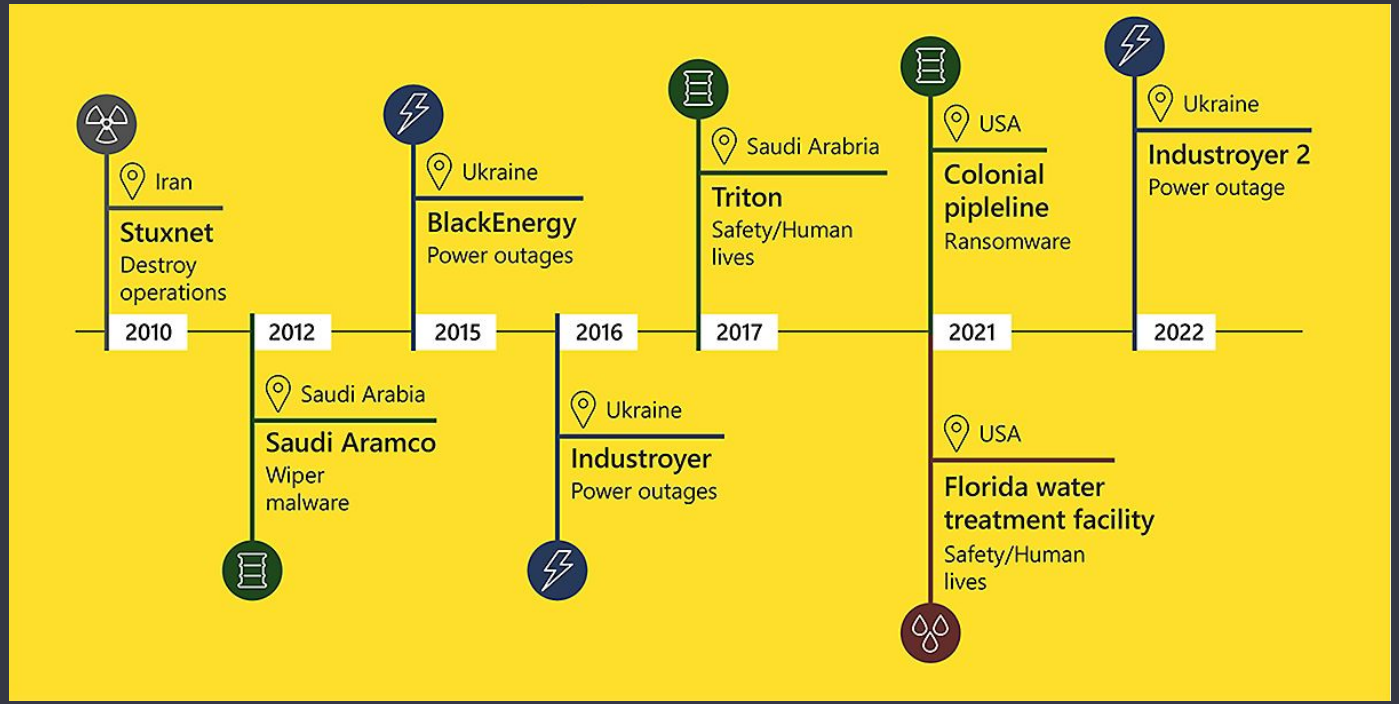
Number of global active IoT connections (installed base) in billions



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%

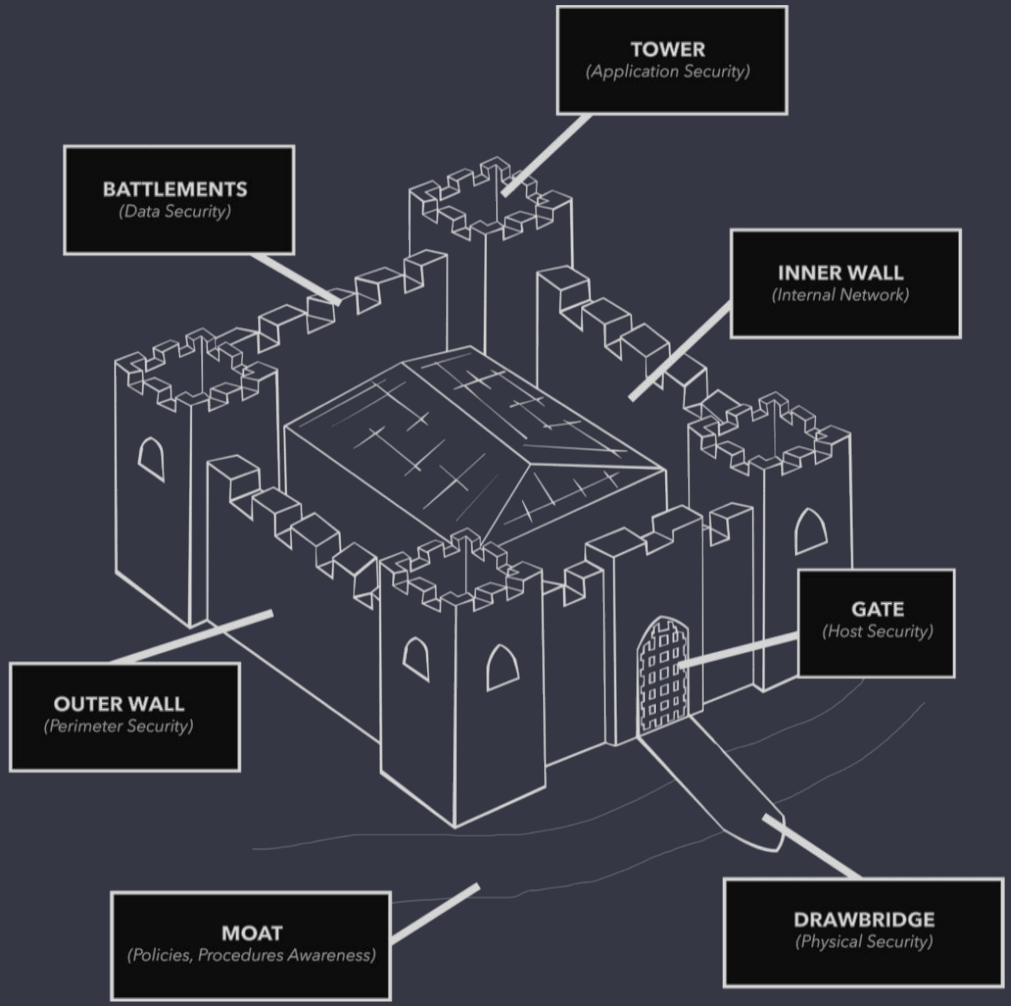
XX% = CAGR

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; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.



The convergence of IT and OT,
https://www.microsoft.com/en-us/security/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



Thank you!

João Pedro Dias

📨jpdias@outlook.com // jpdias@pm.me

🔗https://jpdias.me