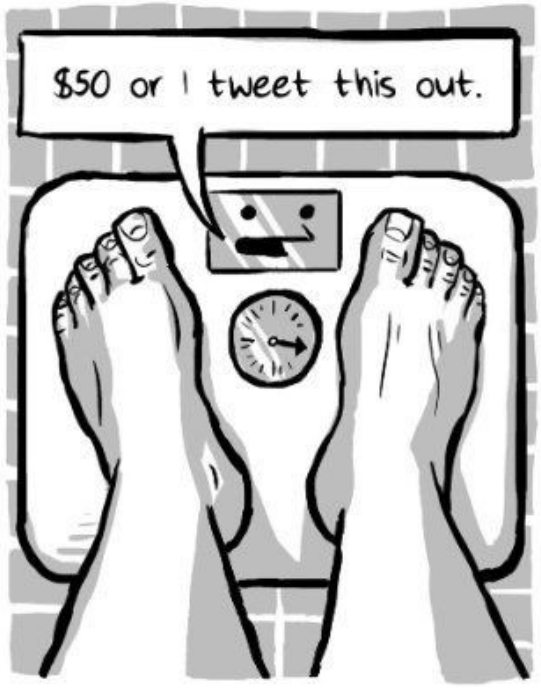
Cybersecurity Management
GCS 2.3 – IoT/ICS

2023-2024
Prof. Marc Ruiz
marc.ruiz-ramirez@upc.edu



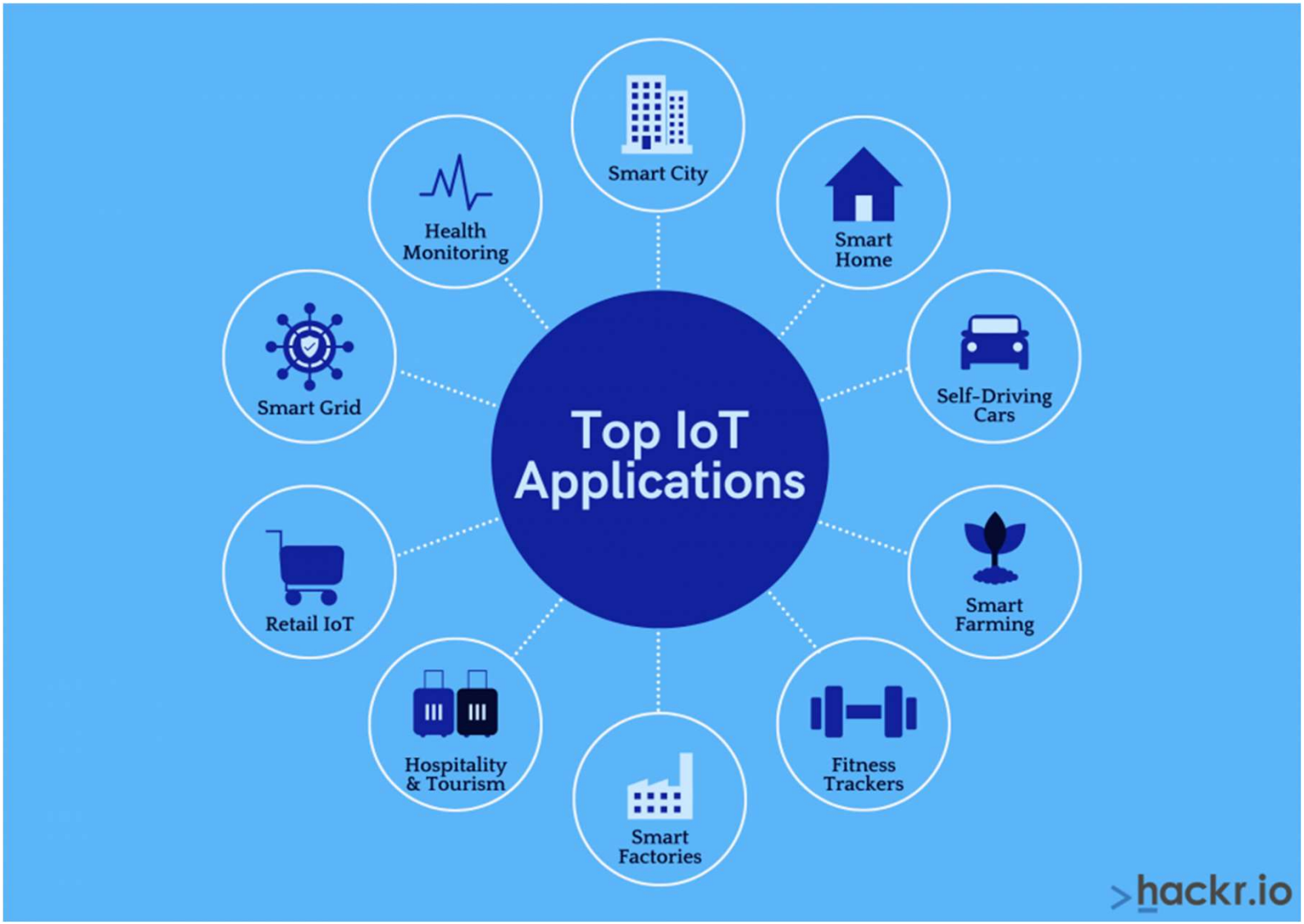
Introduction to Internet of Things (IoT)

Basic definition

- The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
- These devices range from ordinary household objects to sophisticated industrial tools.
- With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and **22 billion by 2025**.

source: ORACLE

IoT use cases

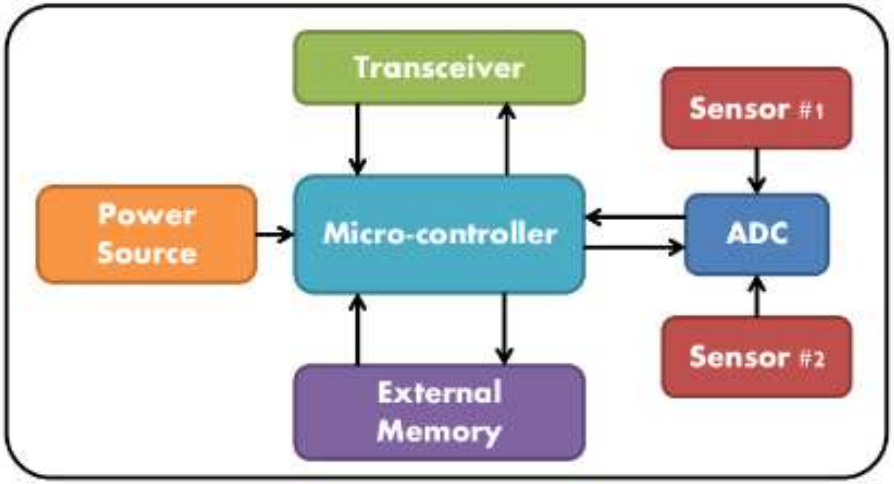


IoT device classification

- Sensors/actuators (constrained IoT devices)
  - They do not communicate with the server
  - Data from these IoT devices can be transmitted to server using gateway
  - Typically they use zigbee, NFC, Bluetooth and RFID standards for communication
  - Battery operated
  - They take care of single sensors, with low data volume
- Intermediate/gateway nodes
  - Directly communicate to central servers for data storage
  - It supports IP protocol and various comm ports: DSL, FTTH, WiFi
  - Powerful processors, not constrained by battery power

Constrained IoT devices

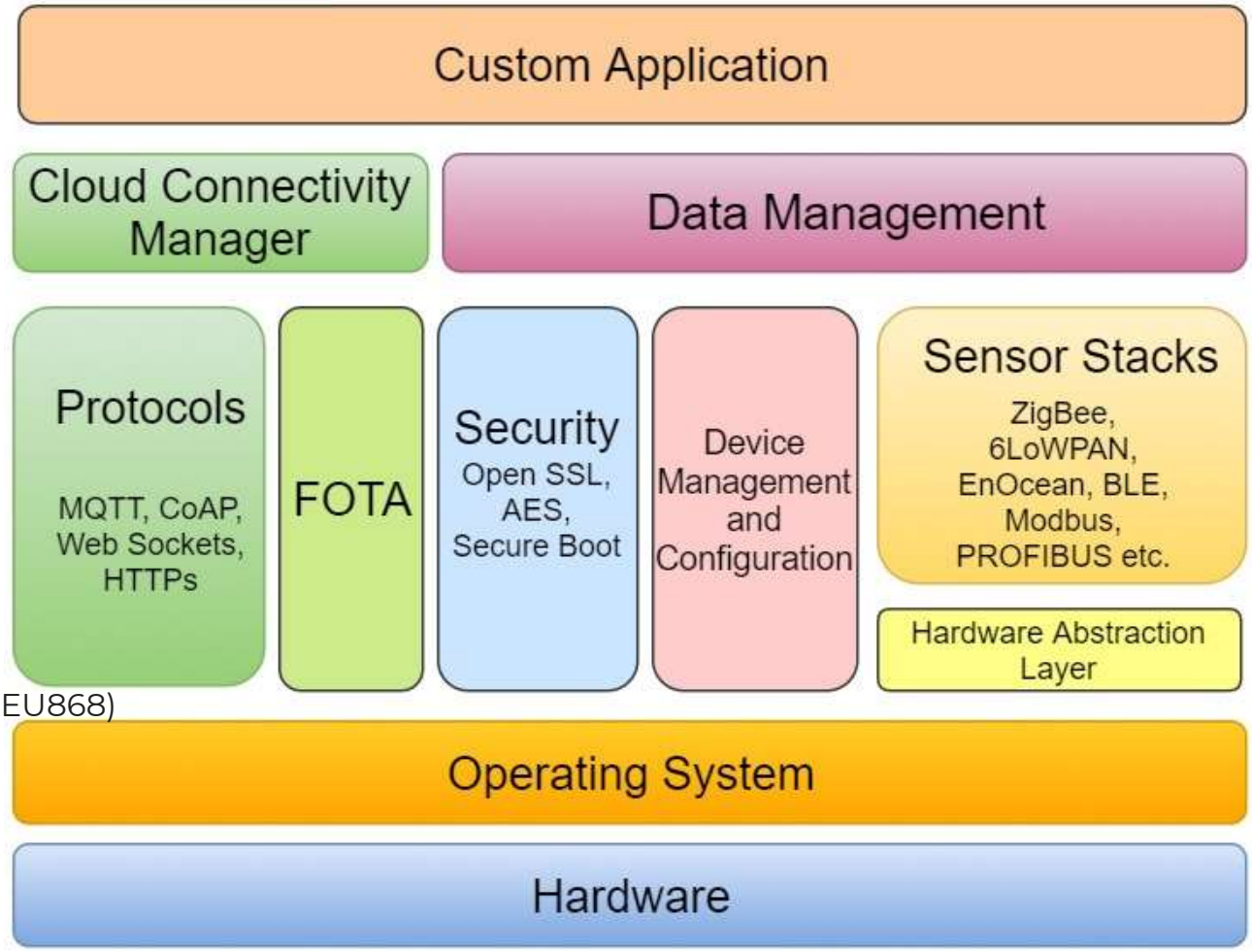
Temperature sensor



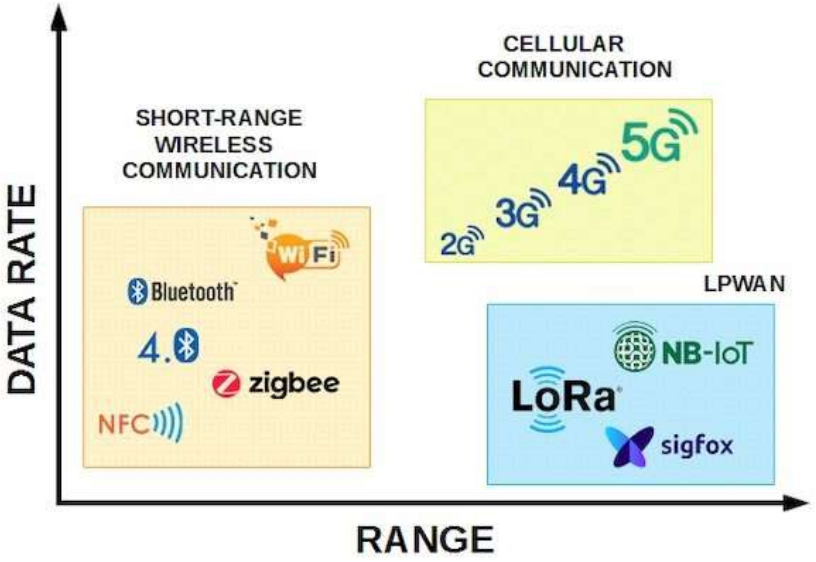
Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

IoT gateway

Dragino LPS8 Indoor LoRaWAN Gateway (EU868)

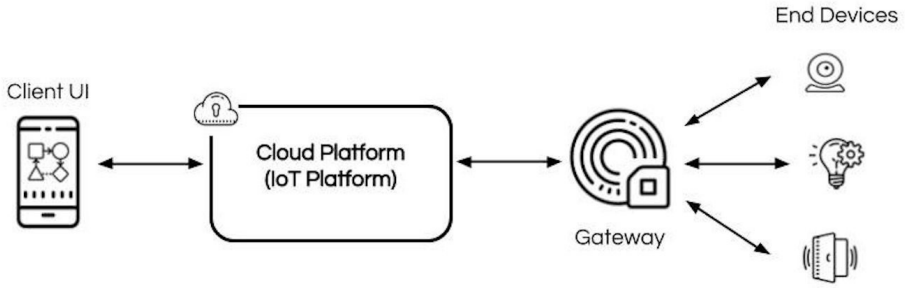


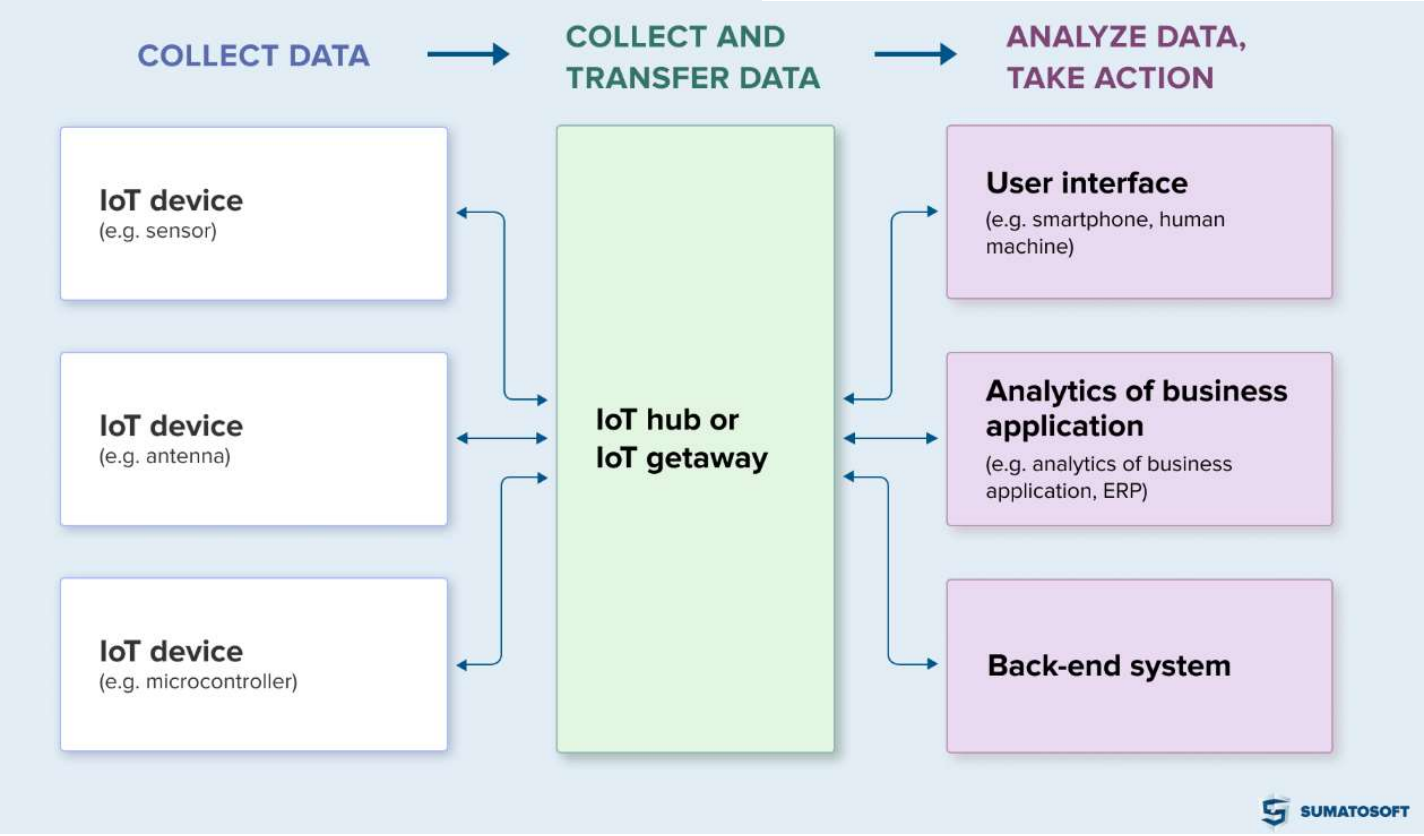
IoT comms



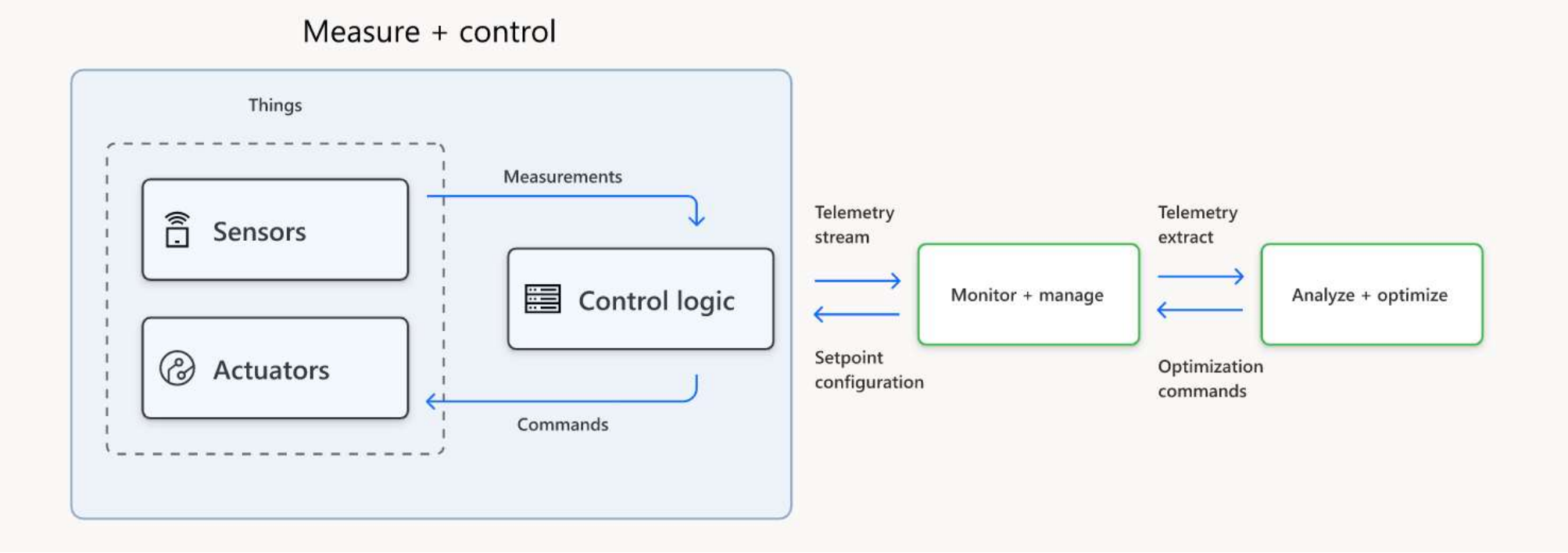
Protocol	Frequency	Range	Data Rates
Bluetooth	2.4 GHz	100 m	125 Kbps–Mbps
Wi-Fi	2.4 GHz, 5 GHz	50 m	150–600 Mbps
NFC	13.56 MHz	4 cm	100–420 Kbps
LoraWAN	867–869 MHz (Europe) 902–928 MHz (North America)	15 Km	0.3–50 Kbps
Cellular	900/1800/1900/2100 MHz	30 m (Between node and base station)	21 Mbps (3G+) 600 Mbps (4G)
Z-wave	865–926 MHz (ISM)	100 m	100 Kbps
Zigbee	2.4 GHz (ISM)	100 m	20 Kbps–250 Kbps
Sigfox	900 MHz	3–50 Km	10–1000 bps

End-to-end IoT architecture





IoT control loops



IoT platforms

- Node-RED
  - Low-code programming for event-driven applications
  - https://nodered.org/
- OpenRemote
  - 100% Open Source IoT Platform for OEMs
  - https://openremote.io/
- ThingsBoard
  - Device management, data collection, processing and visualization
  - https://thingsboard.io/

IoT Congress Barcelona

IOT SOLUTIONS WORLD CONGRESS

31 JANUARY - 2 FEBRUARY 2023
BARCELONA - GRAN VIA VENUE HALL 4

TECHNOLOGY STAGES

This is it! **The new era of industry has arrived. IOT and disruptive technologies are changing the game**, with new business models emerging and technological innovation rapidly changing our world. The content of the **IOT Solutions World Congress** is divided into **6 technology stages:**

INDUSTRY IOT

AI

DIGITAL TWIN

EDGE COMPUTING

AUGMENTED REALITY

5G

IoT Congress Barcelona

IOT SOLUTIONS WORLD CONGRESS

31 JANUARY - 2 FEBRUARY 2023
BARCELONA - GRAN VIA VENUE HALL 4

INDUSTRY JOURNEYS

For targeted audience groups across multiple industry sectors and markets. Learn how these technologies are transforming industries and how they can be foundational to your business.

MANUFACTURING / SUPPLY CHAIN

HEALTHCARE

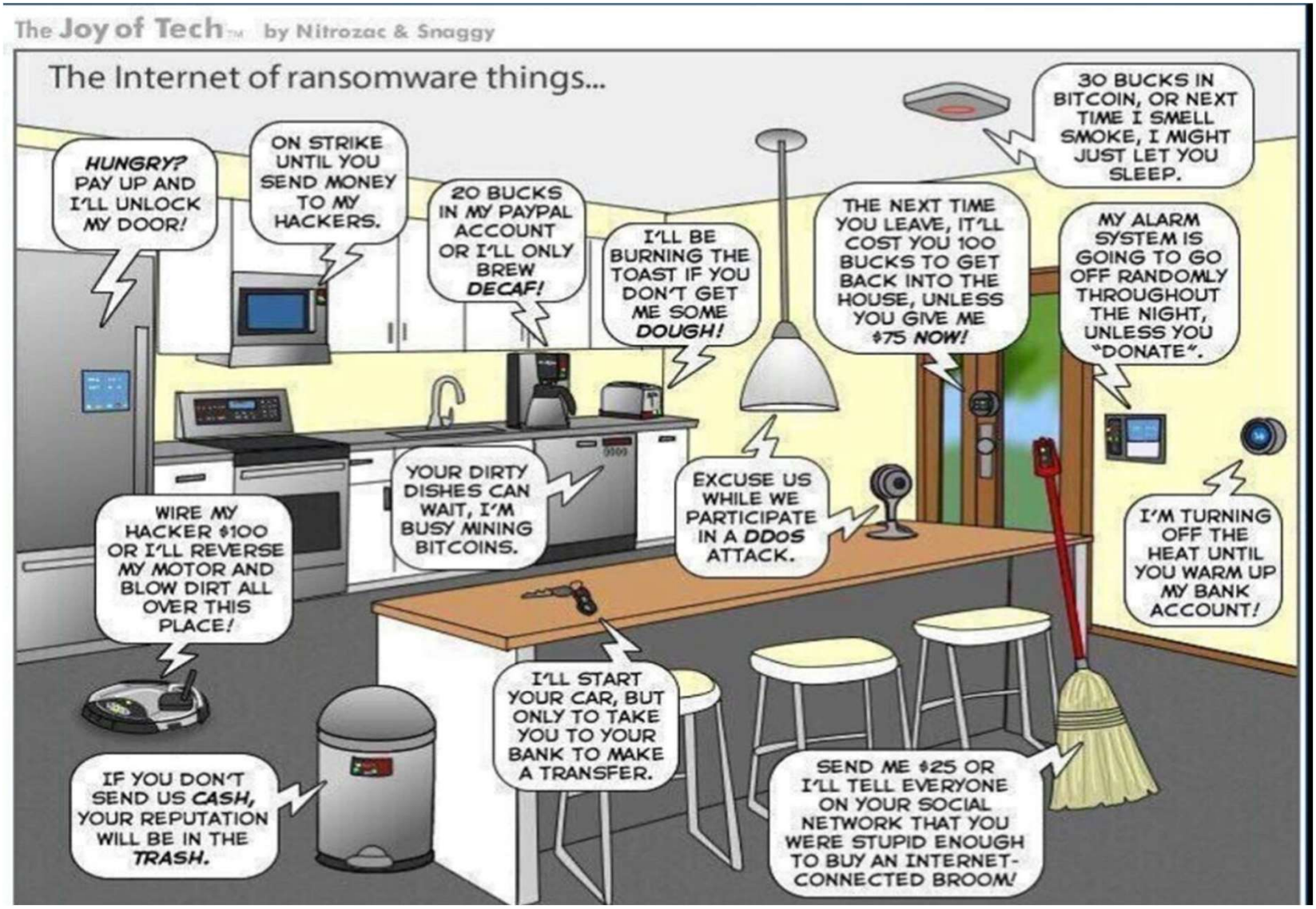
ENERGY / UTILITIES

SMART BUILDINGS / CITIES

CONNECTED TRANSPORTATION

IoT Security

The joke…


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

Concept

- Methods of protection used to secure internet-connected or network-based devices.
- Not only internet-based devices e.g., Bluetooth technology also count as IoT
- Family of techniques, strategies and tools used to protect these devices from becoming compromised.
- The more ways for devices to be able to connect to each other, the more ways threat actors can intercept them.

IoT attacks examples

- Disable the brakes of a connected car
- Hack a connected health device (insulin pump) to administer too much medication to a patient
- Disconnect a refrigeration system housing medicine
- Disable (or unlock) smart door locks
- Etc, etc, etc

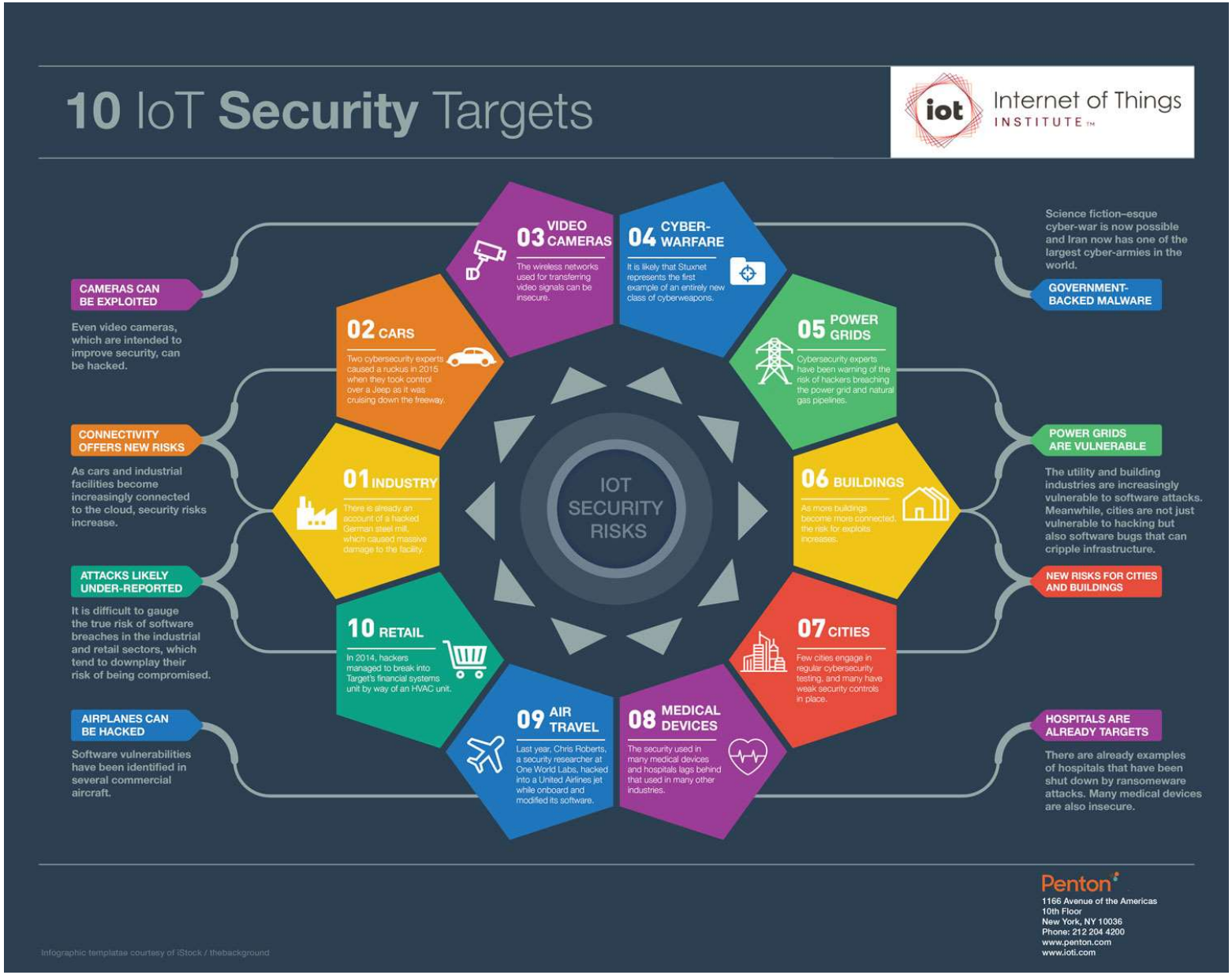
IoT attacks examples

- **Botnets**
  - large collection of devices that has fallen under the control of a centralized attacker
  - DDoS attacks or introduce malware to new victims
  - Many of the security breaches that find their way into the news are the results of botnets!!!

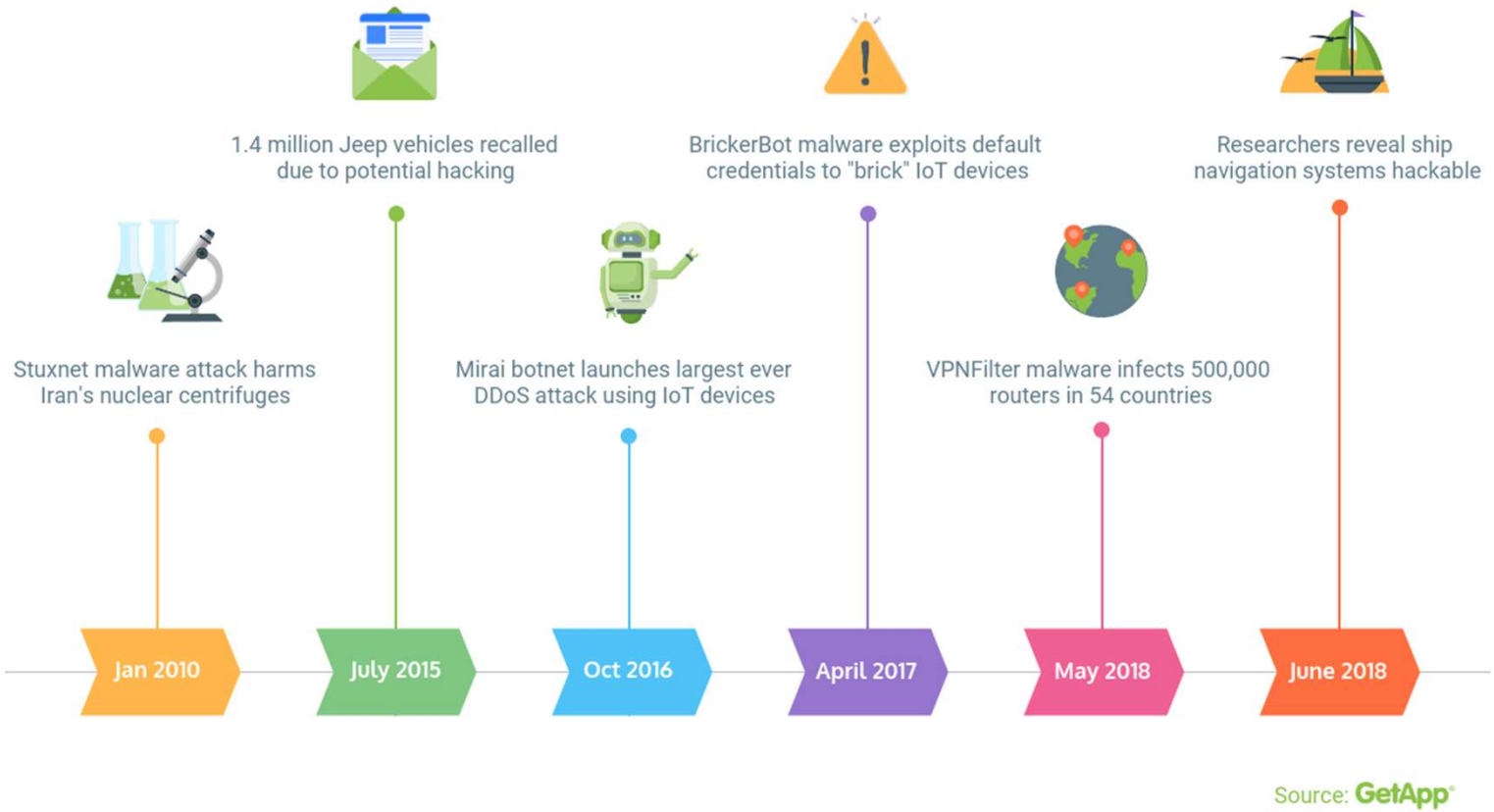
IoT Security targets

Exercise 1: Lightreading "The 10 Most Vulnerable IoT Security Targets"

https://www.iotworldtoday.com/2016/07/27/10-most-vulnerable-iot-security-targets/



Famous IoT attacks



Exercise 2: Lightreading of famous attacks and lessons learned: https://www.getapp.com/resources/internet-of-things-security/

Exercise 3: Watch Video **Hacking TESLA car**: https://www.youtube.com/watch?v=5mdU4ksOc2w

Cybersecurity threats

- **Service disruption**
  - Manipulating IoT devices to make an essential service (e.g., a power generating dam, the water system, a database) completely unavailable
- **Data theft**
  - Gaining improper access to personally identifiable information (PII), such as names, user accounts, social security, national health ID numbers, telephone numbers and residence addresses
- **Data or service manipulation**
  - Where the attacker can make arbitrary changes to the settings of a device, which can cause loss of life, loss of service, damage to the device itself or damage to other devices.
  - Include manipulation of actuators for malicious purposes

Major flaws

- **Inadequate default settings**
  - Default passwords
- **Non-existent upgrade paths**
  - Sometimes, it is impossible to update the firmware or other information itself, making the device permanently toxic to healthy IoT networks.
- **The use of inappropriate technology**
  - Placing powerful software onto an IoT device, even though such computing power is not necessary.
  - Complete Linux operating system makes an IoT device a powerful weapon in the hands of an attacker.

Issues and challenges

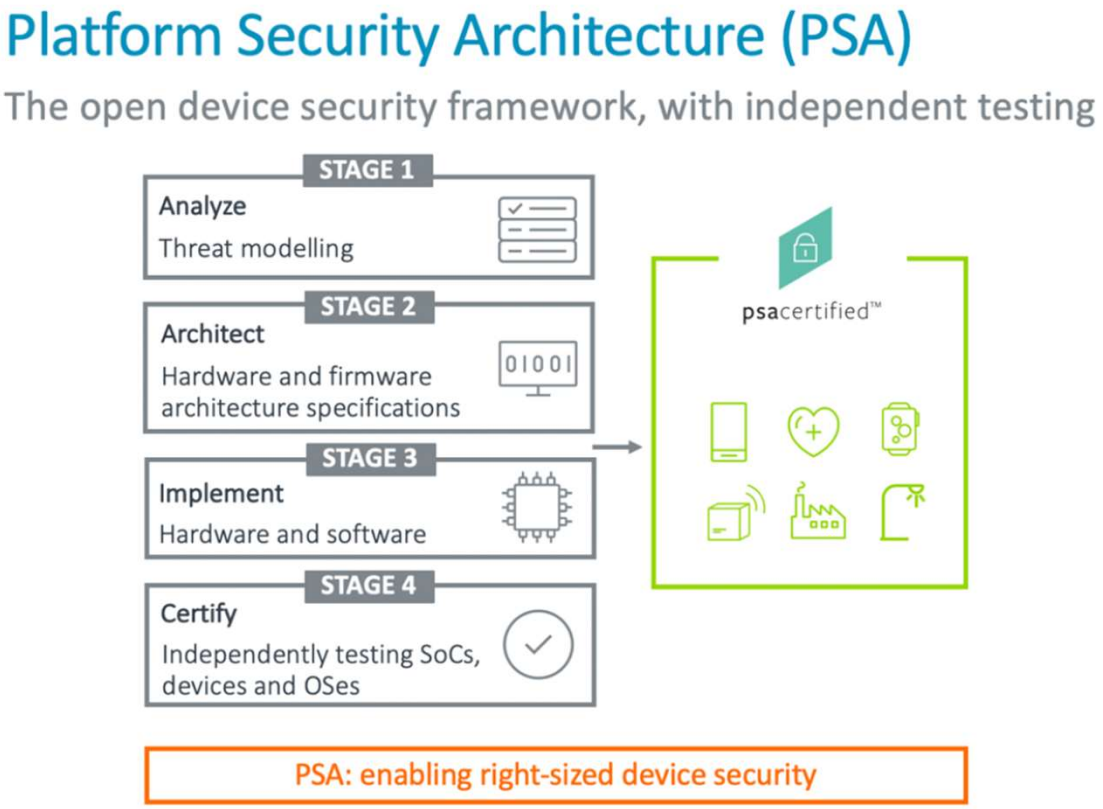
- **Remote exposure is…good…and also bad**
  - accessibility is extremely valuable <-> grants hackers the opportunity to interact with devices remotely
  - IoT security has to account for a large number of entry points!!

- **Maybe digital revolution is going too fast…**
  - More IoT devices -> cost-efficient production ☺
  - More IoT devices -> more vulnerability ☹
  - Lack of investment in securing IoT devices.

- **Resource constraints**
  - Not all IoT devices have the computing power to integrate sophisticated firewalls or antivirus software.
  - Energy can be scarce in those devices with batteries e.g., field sensors

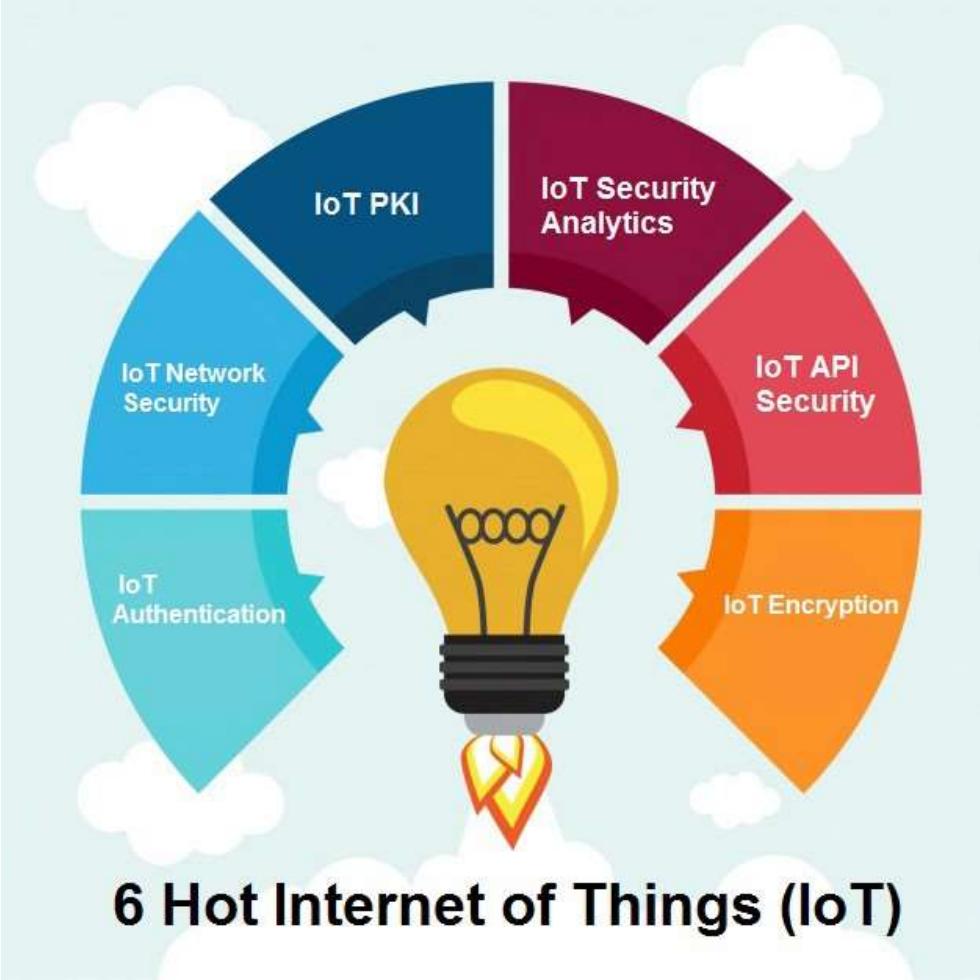
Measures

- Introduce IoT security awareness during the design phase



Measures

- PKI and digital certificates to protect messages and interactions
- Secure connectivity by implementing network security
- API security



Measures

- Network access control for IoT inventoring
- Network segmentation
- Security gateways acting as intermediary between IoT devices and the network
- Patch management/continuous software updates
- Cybersecurity Training and team integration (devops and cybersec experts)
- Consumer education

Exercice 4: Watch this video: https://www.youtube.com/watch?v=iFsCIVH3eS0

ENISA IoT

Online tool:

https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

Exercise 5

Find out which good practices ENISA proposes for baseline security IoT in the area of *cryptography*.

Industrial Control Systems (ICS)
(Self-learning)

Instructions

- Light-reading documents extracted from the extensive information available at Cybersecurity & Infrastructure Security Agency (CISA) website.
  - *Cybersecurity Practices for Industrial Control Systems (2 pages)*
  - *Cyber Threat Source Descriptions (4 pages)*
  - *Overview of Cyber Vulnerabilities (14 pages)*

  All documents available in RACO!!!!! (ics_docs.zip)
- Read them and make yourself questions to try to better understand the concepts of this lesson, as well as find relations with other lessons of the course:
  - Try to identify the similarities and differences between ICS systems and IoT systems. Feed your ICS knowledge with those lessons learned from IoT systems
  - Which threats/vulnerabilities/attacks described in the document are typically observable in other environments and use cases?
    - For instance, man-in-the-middle attack is identified as a potential attack in ICS LANs. Then, is different to other man-in-the-middle attack typically affecting WANs?
  - Conversely, identify any issue/attack/measure inherent or native to ICS systems that is not present (or infrequent) in other use cases.

Cybersecurity Management
GCS 2.3 – IoT/ICS

2023-2024

Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu

Don’t forget the exercises ;)