IOT & CYBERSECURITY

CYBERSECURITY OF THE INTERNET OF THINGS

ACADÉMIE MILITAIRE
SAINT-CYR COËTQUIDAN

COURSE OBJECTIVE

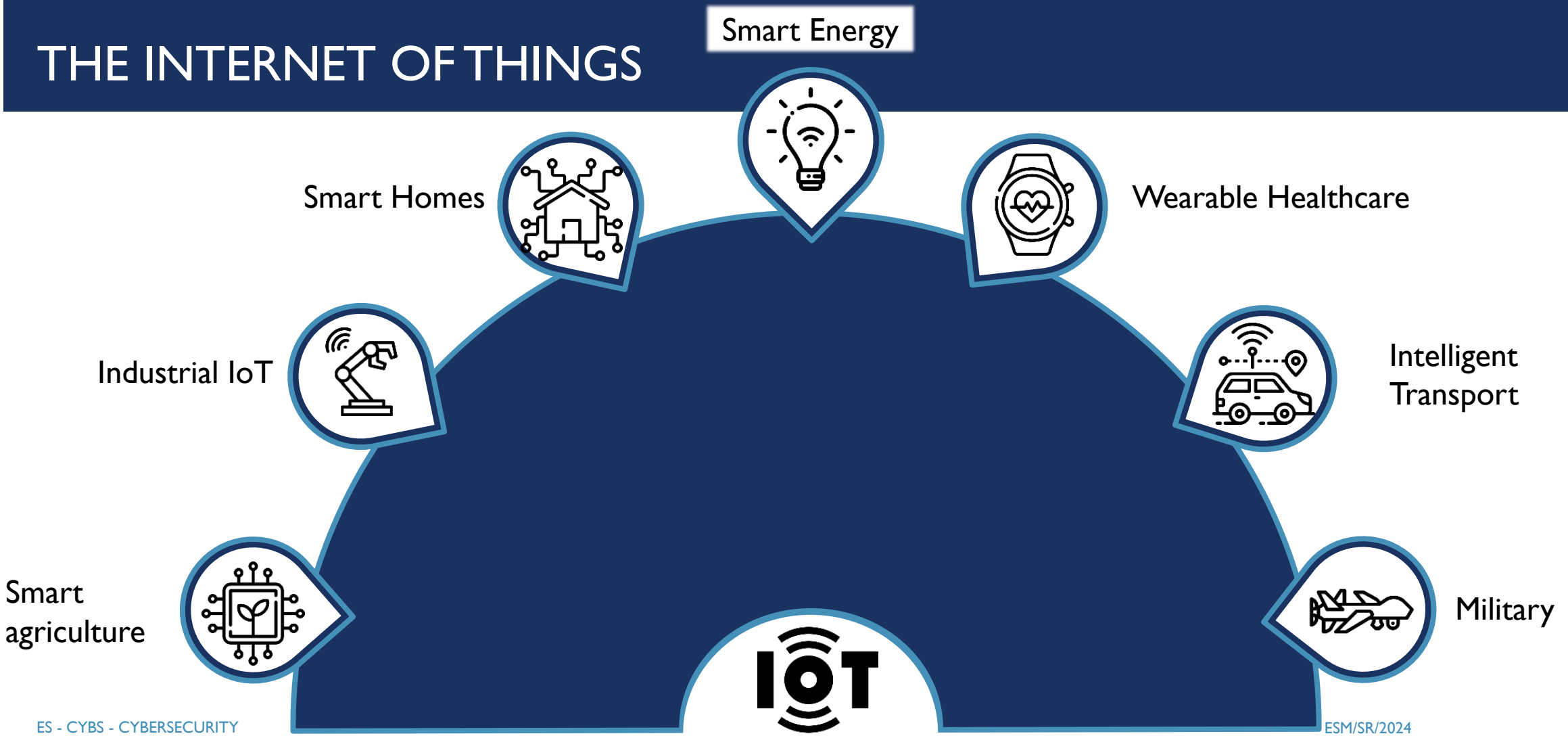
- Associate IoT characteristics with vulnerabilities
- Understand the impact and need of security in the IoT
- Knowledge of security methods

PLAN

1. Context of the IoT
2. Characteristics and challenges
3. Perceived threats and exploitation
4. Defensive methodologies
5. Practical

I. CONTEXT OF THE IOT

THE INTERNET OF THINGS



CRITICAL INFRASTRUCTURES

SITUATIONS

Smart Agriculture

- Devices deployed in fields
  - Limited access to power, network, etc
- Low to high priority tasks
  - Humidity detection, auto irrigation, self-driving tractors, etc.
- Important data sharing and integration
  - GPS positioning for self-driving tractors
  - Irrigation activation upon low humidity

Healthcare

- Devices deployed on people
  - Large mobility probability, strong but infrequent network
- Generally high priority tasks
  - Glucose regulation, heart observation and alert, etc.
- Confidential data sharing
  - Patient medical feedback
  - Integration with hospital systems

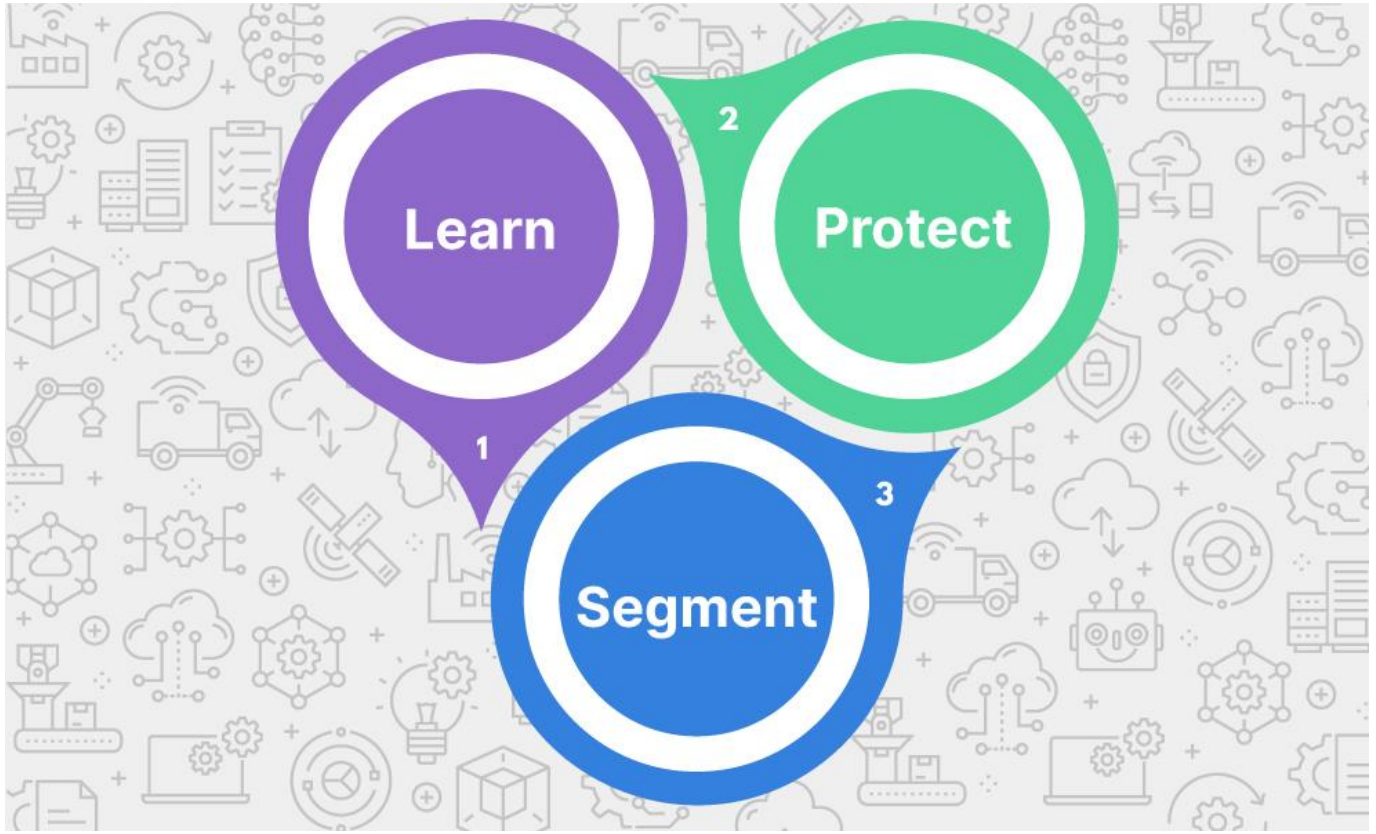
MULTI AREA IMPACT

- Consequences not limited to device
  - Repercussions on other systems
- More and more use in Critical Infrastructures
  - Consequences impacting human life!

IOT SECURITY REQUIREMENTS

- Three key abilities

- Learn
  - Overview and observation
- Segment
  - Segregate devices based upon risks
- Protect
  - Monitoring, inspection and actions



Source: Fortinet, "*What Is IoT Security? Challenges and Requirements*", 7th October 2021

II. CHARACTERISTICS AND CHALLENGES

SITUATION

- Living room with various equipment
  - Smart TV, laptop, tablets, smart phones etc.
- Home Wi-Fi network with password for all devices
- Window at the back with smart opening feature for fresh air
- Electric radiator on smart plug
- Smart thermometer
  - Heating regulated via thermometer and user input

- ➔ Where is the vulnerability?

SITUATION

- Living room with various equipment
  - Smart TV, laptop, tablets, smart phones etc.
- Home Wi-Fi network with password for all devices
- Window at the back with smart opening feature for fresh air
- Electric radiator on smart plug
- Smart thermometer
  - Heating regulated via thermometer and user input

- ➔ Where is the vulnerability?

… BUT WHY?

- Lopsided security interest
  - More attention on more "important" systems than others
- Evident weaknesses → reinforced protection
  - Doors, windows on ground floor, etc.
- Smaller devices generally forgotten
  - Very common → not changing passwords

1. Smart plug turned on by hacker → room heats up
2. Thermometer detects heat and tries to turn of plug
3. Plug ignores commands and keeps heating
4. Heat reaches extreme levels → thermometer opens window for fresh air and to cool down room
5. House is now accessible

SECURITY CHALLENGES

- Attack surface constantly expanding
  - More devices online → more targets
- More importance to security aspects
  - Availability, integrity and confidentiality
- IoT taking critical positions in companies
  - Not only weaknesses but also potential threats

Normal security methods not always possible

➔ Device limitations

DEVICE SPECIFICATIONS

- IoT devices possess limitations
  - Energy
  - Storage
  - Computation
  - Network capabilities

- "Normal" security methods not always applicable
  - Ex: Anti-virus not possible

Chipset	ESP32-Wroom-32
CPU	240Mhz dual-core
RAM	512kb SRAM
Storage	4MB external flash
Power	Battery
Networking	802.11 b/g/n Wi-Fi® Bluetooth 4.2 / Bluetooth Low Energy (BLE)

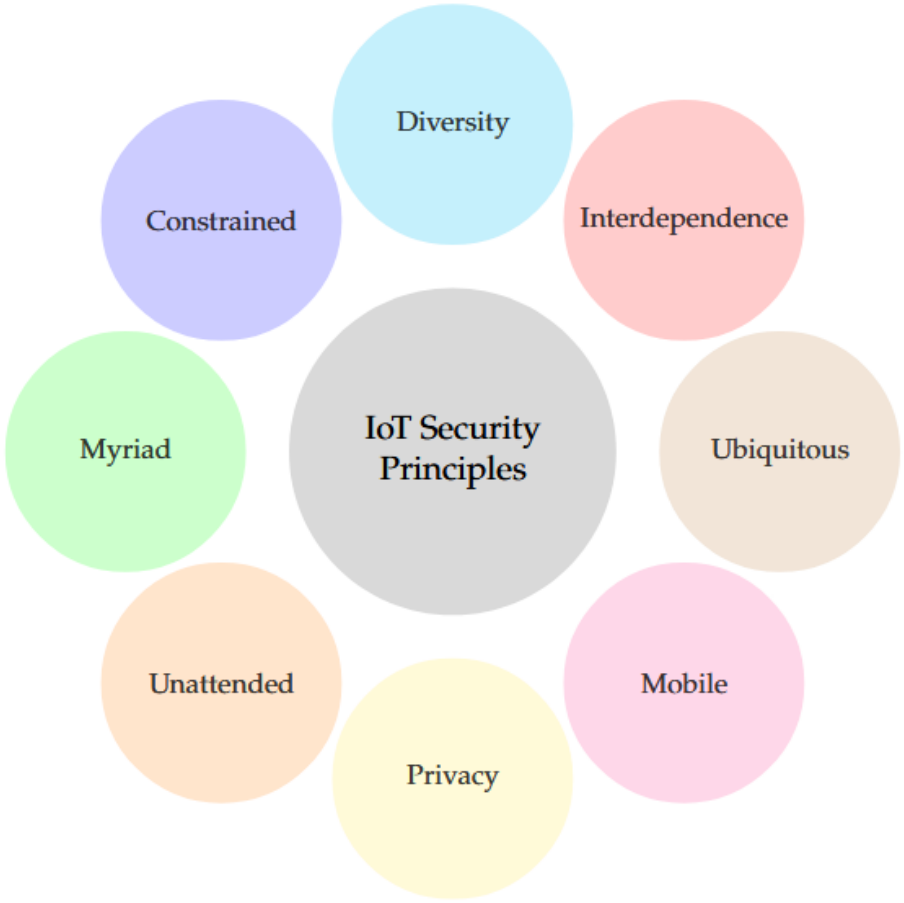
Source: Juniper Research

IoT Characteristics	Potential Security Weakness & Targets
Closed / open platforms Variable policies High data volume handling	Code Lack of penetration testing Weak User / Third Party Authentication
Public / private / hybrid cloud deployment	Code Policy management
2G, 3G, LTE, 5G DSL, Fibre, LPWAN Wi-Fi, Bluetooth MQTT, IP, ZigBee, Mesh RF, Wi-Fi etc	Insecure communications
Variable communications protocols Time-sensitive data analysis	Policy management Denial-of-service No / insecure updates Poor hardware design
Limited power Low bandwidth Constrained capabilities	Design faults Software / firmware implementation faults Inability to update
Sensitive data: video, audio, location, personal information Technical data: environmental measurement, uptime reports	Users Policy management Data storage

Source: Thales, "*What is IoT security?*", 7th October 2021

III. PERCEIVED THREATS AND EXPLOITATION

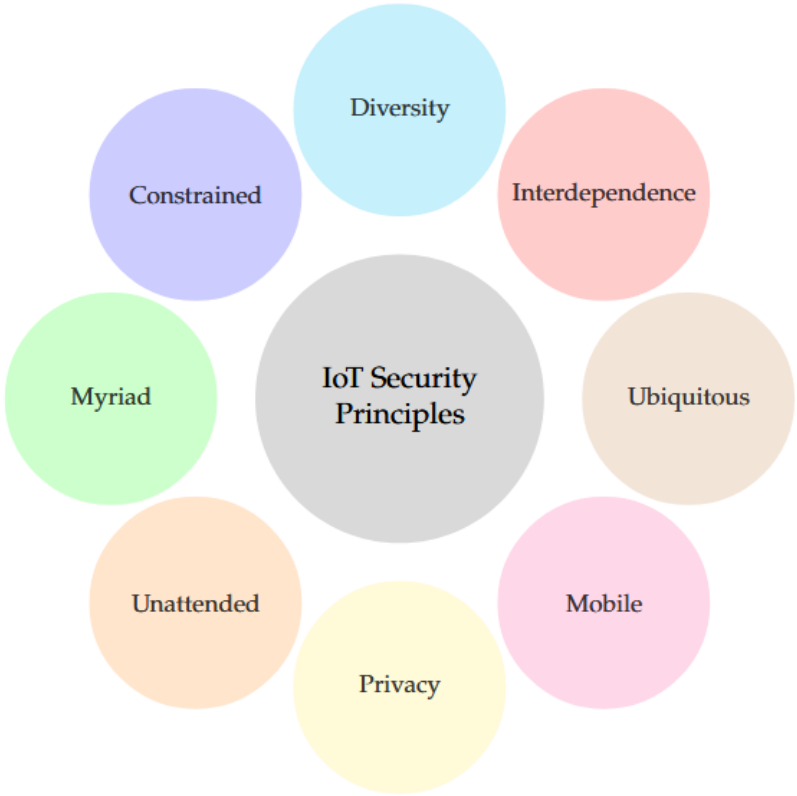
TARGETING SECURITY PRINCIPALS OF THE IOT



TARGETING SECURITY PRINCIPALS OF THE IOT

- **Interdependence**
  - Functioning in tandem with other devices (smart home applications)
  - Ex → smart light sensor → turn lights on/off

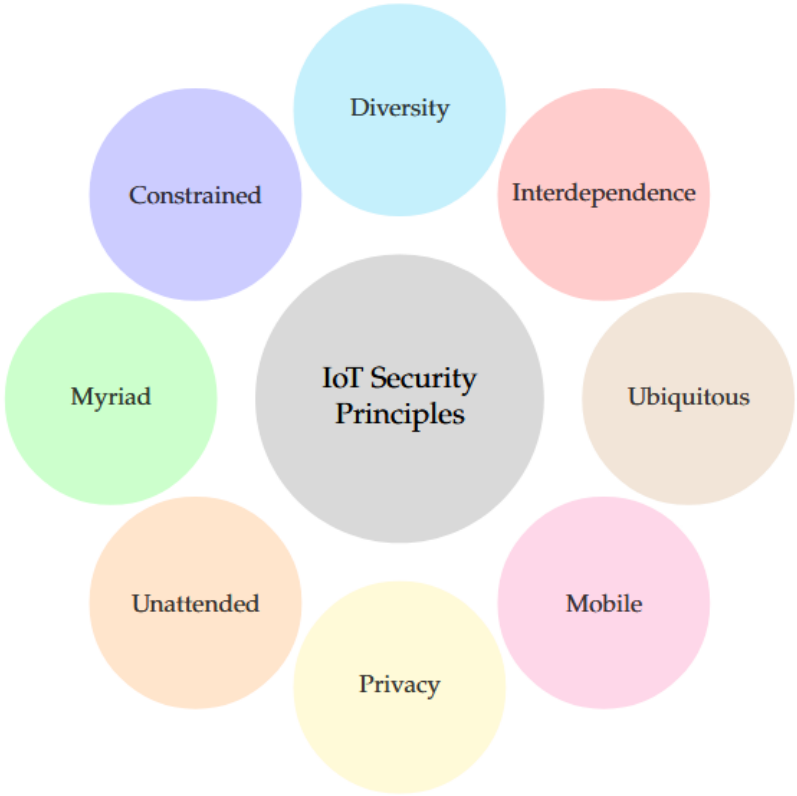
- **Diversity**
  - Difference in hardware (bulbs, plugs, switches, etc)
  - Higher diversity → higher change of vulnerabilities



TARGETING SECURITY PRINCIPALS OF THE IOT

- **Constrained**
  - Hardware limitations (energy, computation, communication, etc.)
  - Dependant on manufacturer / application / use case

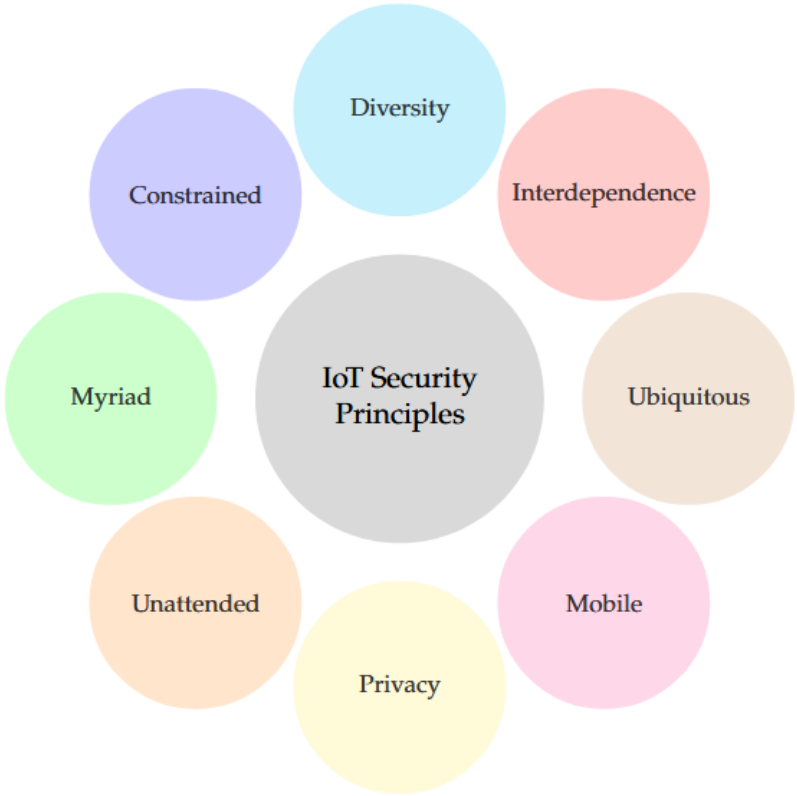
- **Myriad**
  - Easy to create / deploy in large quantities → increased network complexity
  - More devices → higher diversity → higher risk of compromise



TARGETING SECURITY PRINCIPALS OF THE IOT

- **Unattended**
  - Deployment in remote / inaccessible areas
  - Autonomous functionality, intercommunication, no human interaction

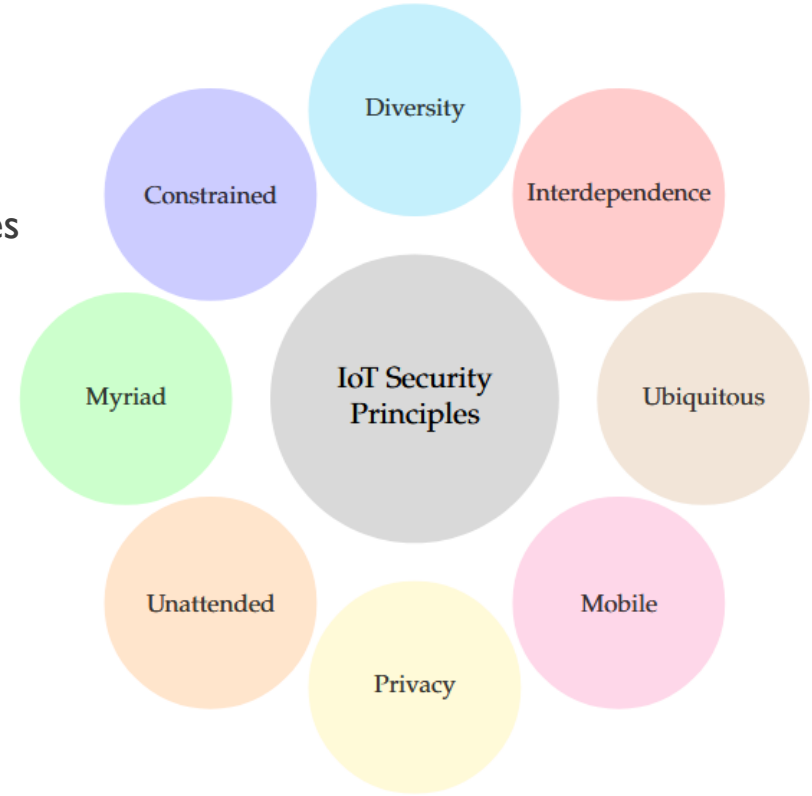
- **Privacy**
  - Capture and process large quantities of personal data (wearable healthcare)
  - Can be exploited → must protect device storage / exchanges



TARGETING SECURITY PRINCIPALS OF THE IOT

- **Mobile**
  - Wearable devices → high mobility → adapt to dynamic environmental changes
  - Network jumping / communication with multiple devices

- **Ubiquitous**
  - Increased presence of IoT devices → increased risk of security incidents
  - Human interactions important → "The error is generally found between the chair and the keyboard" → Human error a contributing factor



MULTIPLE ISSUES …

- "Normal" security methods not always applicable
- Limitations in security methods due to device / network characteristics

- Multiple problems to overcome

Weak Authentication & Authorisation
Lack of Encryption
Firmware and Software Vulnerabilities
Insecure communications & channels
Difficulties in patching / updating
Lack of testing
Bad management
Poor hardware design
Users
Storage

VULNERABILITIES WITH DATA SECURITY

Weak authentication and authorisation

- Insufficient authentication / authorisation practices
- Use of default passwords
  - Often forgotten to change …
  - Can be exploited to access network
- Rogue devices can be used to steal data

Lack of encryption

- Network traffic generally left unencrypted
  - Confidential / personal data vulnerable
  - Threats include malware / ransomware
- Even important devices!
  - Medical imaging / patient monitoring / security cameras / printers …

Insecure communication protocols and channels

- Use on generic network
  - Shared with normal devices
  - Attacks can spread much easier
- Data can be intercepted due to lack of segmentation
  - Use of unprotected Bluetooth (automotive industry)
  - Exploitation of HTTP / APIs

VULNERABILITIES WITH SOFT OR HARDWARE

Firmware and software vulnerabilities

- Limited development and testing of secure firmware
- Devices vulnerable to most rudimentary forms of attack
  - Firmware / software / third-party apps
- Network environment comprised by vulnerable web apps / software for IoT devices

Difficulties in patching and updating devices

- Focus not on building security into devices
- Devices not designed for regular updates
- Cannot ensure secure upgrades
  - Firmware update / patches / dynamic testing

Poor hardware design

- No in-depth testing or study of hardware
  - Oversight of design flaws / lack of embedded security systems
  - Insufficient storage
- Use of out of data legacy systems
- Un secured open-source components
  - Easily comprisable

HUMAN RELATED ISSUES

Lack of testing

- IoT system testing overlooked
- Interest generally on "important" servers
  - Web / database / cloud storage
- Generally, forget potential weak points
  - Missed vulnerabilities

Bad management

- Generally overlooking IoT constraints and characteristics
- Considered "low importance"
- Pour money into large scale systems
  - Servers, etc.
- Lack of sufficient finances / manpower

Users

- Insufficient training
- Incorrect use cause of many attacks
  - Miss-configuration / victim of phishing
- Sometimes ego gets in way
  - "I know more than you" …

THREATS

- These vulnerabilities leave way for multiple threats
- Too many to count …

- Important role of security professionals
  - Use of taxonomies / threat models
  - ENISA → https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Firmware exploits
Credentia-based attacks
On-path attacks (mitm)
Physical hardware-based attacks
Network-based attacks (routing)

SOFTWARE AND IMPLEMENTATION

Firmware exploits

- Not many protections in place for device firmware
  - MicroPython on Pi Pico
- Presence of vulnerabilities to exploit

- Can update / replace firmware with compromised version

Credential-based

- Use of default usernames / passwords
  - Generally insecure or shared (shown previously)

- Default credentials known
- Possible, to "guess" or force authentication

On-path – Man-in-the-Middle

- Positioning of attacker between trusted parties
  - IoT camera → attacker → cloud server
- Intercept communications

- No encryption → no problem
- Possible to change data, impact services

DEVICE AND COMMUNICATION BASED

Physcal hardware-based

- Many devices placed in public / accessible areas
  - Security cameras / stop lights / fire alarms …
- Sometimes also in remote on protected areas
  - Fields / military observation zones

- Physical access to hardware → steal data / gain control
- Also possible to extract encryption keys, when used

Network-based

- Devices exchange data using multiple protocols
  - Many open source and unprotected
    - LoRa / Wi-Fi / etc
- No physical access needed to device

- Eavesdropping on communications for information
- Can cause targeted or general communications blackout

POSSIBLE TO EXPLOIT COMPROMISED DEVICES

- Devices compromised can be used for attacks
  - Principal of Bot-Nets
- Collection of infected / compromised devices to perform malicious actions
  - Can be zombies → alive but dead (seemingly normal operations)
- General principal of DDoS

IV. DEFENSIVE METHODOLOGIES

ADAPTABLE DEFENCES

- Defences must correspond to a vulnerability
  - Possibly a principal → secure communications
- Must also take into account device specifications
  - Intrusion Detection System for Windows ……..
  - Not possible on IoT → too heavy

Software and firmware updates
Credential Security
Device authentication
Encryption
Deactivating unneeded features
DNS filtering

DEVICE SYSTEMS AND FUNCTIONALITIES

Software and firmware updates

- Same principal as Windows / Linux
  - Regular software updates
  - Security updates important to perform, whatever the device
- Updates need to be tailored to device
  - Large update over network not recommended
  - Use of Over The Air (OTA)
- If device cannot be updated → removed / taken offline

Deactivating unneeded functionalities

- Devices come with many different features
  - Good for diversity and options
  - Bad when not all needed
- Unused featured must be deactivated
  - Closing unused ports / stopping unused software
- More systems running → more targets
- If not used → won't easily see potential attack

IDENTITY VALIDATION

Credential security

- Devices sometimes possess admin access
  - Used for remote configuration and deployment
- Credentials updated **BEFORE** deployment

- General practice → long complex passwords (as seen previously)
- No reused credentials → unique passwords
  - Use of password manager

Device authentication

- Devices talk to each other to relay information
  - Light sensor → bulb / Thermometer → heating
  - Sensor → cloud server, etc.
- All devices need to confirm their identity

- No device should interact with others UNLESS authorised
- Use of certificates → TSL (Transport Layer Security)

ENCRYPTION AND FILTERING

Encryption

- Data exchanges are vulnerable to attackers
- Protect the data using different Encryption methods :
  - Encoding → simple reversable data translation via algorithm
    - A becomes B : Hello → Ifmmp
  - Symmetric encryption → Single key for encryption and decryption
    - Fast but lacking in security
  - Asymmetric encryption → Dual keys, one for encryption and one for decryption
    - Computationally heavy but stronger

DNS filtering

- Communications on internet utilise IP addresses
  - 192.168.4.1 → server Pi Pco in *practical work 1*
- Difficult to remember
  - IPv4 → 2^{32} addresses / IPv6 → 2^{128} addresses
  - Use of URLs as shorthand
- IP → URL resolution by DNS (Domain Name Server)

- Use DNS to block and filter only needed websites
  - Avoid reaching out to attacker domain

V. PRACTICAL

YOUR TIME TO SHINE … AGAIN

CONTEXT

- Take on the role of security officers
- Maintaining a Chat system

- System functions ➔ possesses weaknesses
- Identify them and propose solutions

- Reinforce 2 pillars of security
  - **Confidentiality | Integrity**
- Study another notion of importance ➔ **Authentication**

- Working on data security

- Studying the differences between four data transformation algorithms
  - Encoding
  - Symmetric Encryption
  - Asymmetric Encryption
  - Hashing

OBJECTIVES

- Information available on Moodle
  - Source code available as well ➔ Pico W
- Collaboration is key

- Propose solutions and study limits
  - Relation to what has been shown during the course

- Evaluation on report ➔ **must be submitted before the end**