Internet of Things Security

Saad EL JAOUHARI

2023-2024

isep
École d'ingénieurs du numérique

60 Années d'excellence

Table of contents

Recap module: Lectures

Lecture 1	***Lecture 2***	***Lecture 3***	***Lecture 4***	***Lecture 5***	***Lecture 6***	***Lecture 7***
Introduction to IoT	Mini projects	Intro IoT / B2B / Application	Industrial IoT (IIoT) -Industry 4.0, smart agriculture, robotic, mining, ...	Sensors and actuators	Introduction to IoT Wide area	Introduction
Different visions of the IoT paradigm	Problem Identification	Value Chain and main players	Embedded devices (Hardware) - ESP, Rasp, Arduino, ...	IoT platfroms (Industrial and open source)	LPWAN	Main Security Concepts
Enabling technologies & Reference architecture	Solution Concept / Scenario / Architecture	Standards (IETF, ISO, IEEE, ITU, ETSI, 3GPP, GSMA ...)	Embedded coding (Software) - Arduino IDE	Cloud & Edge	Licenced LPWAN	Security Threats
Application design concepts	Business Model	Typical IoT Architecture Stack	Long Range protocols: 5G LoraWAN, Sigfox, LTE-M and NB-IoT	AIoT = AI + IoT	Unlicensed LPWAN	Security Functionalities
Developing an IoT application by the example (Node-Red, Rasberry Pi, Arduino, IDE, ...)		IoT Networks (PAN To WAN)		Blockchain		
		Communication protocols (Short and long range protocols)		Quick security Introduction		
		Applications (Digital Twins, Smart building, Home Automation, ...)				

Recap module: Project

- Practical project → 6 supervised sessions

01

Introduction

What is computer security ?
IoT issues ?
Well-known IoT attacks

Introduction: what is security ?

- **Security**
  - **Oxford** The state of being free from danger or threat
  - **Collins** Security refers to all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it.
- **Security is not safety**
  - **Security** is highly focused on the deliberate protection actions against malicious actions toward an individual, organization, or assets.
  - **Safety** consists in being sure that nothing goes wrong in absence of malicious person(s)

Introduction: what is information security ?

- **Information Security (Infosec)**:
  - **Definition**: Infosec refers to all the measures that are taken to protect information (data) from unauthorized access, use, disclosure, disruption, modification, or destruction.
  - **Information security** = **Computer security** + **Network security**

What is computer security ?

- Most developers and operators are concerned with **correctness and efficiency**:
  - A working software, website, blog, etc…
- **Security** is concerned with **preventing/protecting against undesired behavior**:
  - Considers an enemy/opponent/hacker/adversary who is actively and maliciously trying to *get around* any *protective measures* in place

What is computer security ?

- Kinds of undesired behaviors:
  - Stealing information: ~~confidentiality~~
    - Corporate secrets (product plans, source code, administrative documents, …)
    - Personal information (credit card numbers, SSN, …)
  - Modifying information or functionality : ~~integrity~~
    - Installing unwanted software (spyware, botnet client, …)
    - Destroying records (accounts, logs, plans, …)
  - Denying access: ~~availability~~
    - Unable to purchase products
    - Unable to access baking information

Defects and vulnerabilities

- Many breaches begin by exploiting a **vulnerability:**
  - This is a security-relevant **software defect** that can be exploited to provoke an undesired behavior
- A software **defect** is present when the software behaves incorrectly, (i.e., it fails to meet its requirements)
- Defect occur in the software's design and its implementation
  - A **flaw** is a defect In the design
  - A **bug** is a defect in the implementation

Considering Correctness

- The Flash vulnerability is an implementation **bug**
  - All software contain bugs. So what ?
- A normal user **never sees most bugs** and **works around them**
  - Most (post-deployment) bugs due to rare feature interaction of failure to handle edge cases
- Assessment: would be **too expensive** to fix every bug before deploying
  - Companies only **fix** the ones **mostly likely to affect** normal users

Considering Security

- Key difference: *an adversary is not a normal user*
- The **adversary will actively attempt to find defects** in rare features interactions and edge cases
  - For a typical user, (accidentally) finding a bug will result in a crash, which he will try to avoid
  - An adversary will work to find a bug that leaded to this crash and exploit it to achieve his goal

Considering Security

The main objective of computer security is to ensure security, by **eliminating bugs and design flows** and/or to make them **harder to exploit**

Introduction: What is IoT in a nutshell ?

No precise, consensual definition...

- **Internet of Things (one possible definition):**
  - **Network of devices** that are able to connect, interact and exchange data.

- **Standard devices**: desktops, laptops, smartphones, tablets, …

- But also, any **"traditional" object that contains a digital connectable device**: temperature and humidity sensors, domestic appliance, medical device, security camera, traffic light, ...

IoT is Security Critical

What is the difference between security of IoT and information security ?

Not that much, but…

Security is of critical importance for IoT

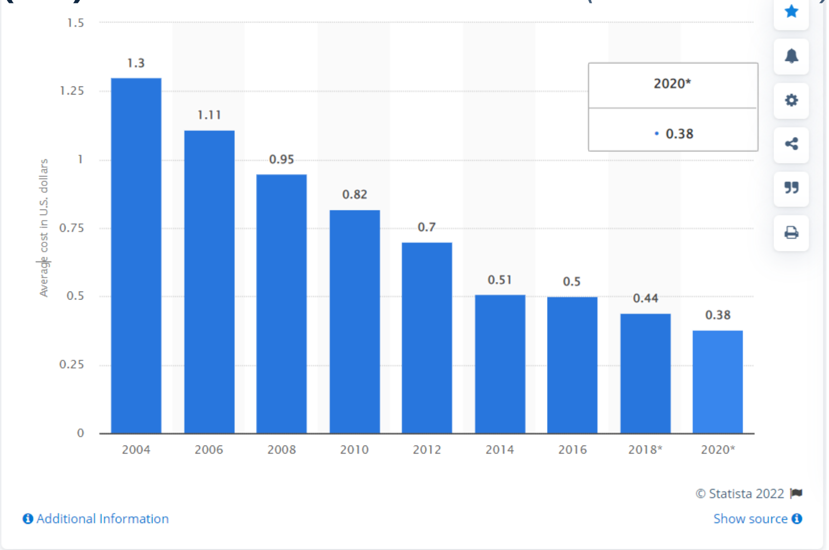
- Importance of communications (many protocols ! → BLE, Zigbee, Z-wave, NB-IoT, Lora, …)
- Huge number of connected devices (Heterogeneity !)
- IoT devices are used in critical systems (healthcare, industries, smart cars, …)
  - Failures may involve human, environmental, economical consequences

IoT is a Constrained System

IoT devices are often low-cost devices: constrained systems (< 1$!)

- Slow processor
- Small amount of RAM
- Low energy consumption
- Low network bandwidth capacity (and short range for some)

Average costs of industrial Internet of Things (IoT) sensors from 2004 to 2020 *(in U.S. dollars)*



Traditional security solutions cannot be (easily) applied to IoT

* https://www.statista.com/statistics/682846/vr-tethered-hmd-average-selling-price/

isep
École d'ingénieurs du numérique

A few Examples of IoT Security Issues

- **2016** possible to open and start a **car** by **hacking its keyless technology** (radio communication)
- **2016 :** DDoS (Distributed Denial of Service) attack (Mirai botnet) against the **DNS provider Dyn** by using **600 000 of connected devices** (mostly cameras) to put it out of order
- **2017**: IoT Goes Nuclear: Creating a **Zigbee** Chain Reaction

A few Examples of IoT Security Issues

- **2016** possible to open and start a **car** by **hacking its keyless technology** (radio communication)

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
https://www.youtube.com/watch?time_continue=1&v=MK0SrxBC1xs&feature=emb_title&ab_channel=WIRED

A few Examples of IoT Security Issues

- **2016** possible to open and start a **car** by **hacking its keyless technology** (radio communication)

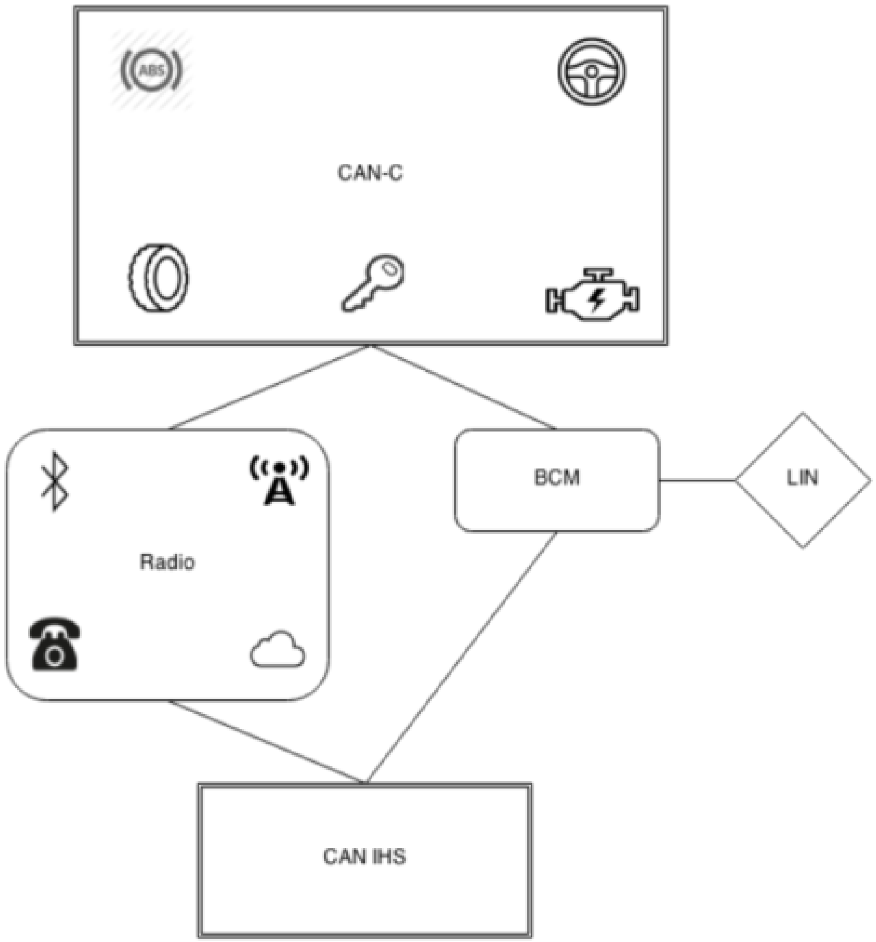


Figure: 2014 Jeep Cherokee architecture diagram

- CAN-C is the high-speed bus that connects the engine, brakes, airbags etc.
- CAN-IHS is a low-speed bus that connects the comfort systems like radio and climate controls.

* Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* 2015.S 91 (2015).

A few Examples of IoT Security Issues

- **2016 :** DDoS (Distributed Denial of Service) attack (Mirai botnet) against the **DNS provider Dyn** by using **600 000 of connected devices** (mostly cameras) to put it out of order

A few Examples of IoT Security Issues

- DDoS Attack in October 2016 → **Main Target**: DNS provider **Dyn**
  - Temporarily crippled several high-profile services such as **OVH, Dyn,** and **Krebs on Security** via massive distributed Denial of service attacks (DDoS)
  - DDoS attack was staged and launched from IoT devices using the Mirai malware
  - OVH reported that these attacks exceeded **1 Tbps** - the largest on public record
  - Mirai infected over **600,000** vulnerable IoT devices

- Mirai was designed for **two** main purposes:
  - Find and infect IoT devices to grow the botnet
  - Participate in DDoS attacks based on commands received by remote Command and Control (C&C) infrastructure

- Mirai operates in three stages:
  1. Infect the devices
  2. Protect itself
  3. Launch attack

A few Examples of IoT Security Issues

- **Stage 1: Infect the devices**
  - **Scan** for IoT devices that are accessible over the Internet
    - Primarily scans for ports **22, 23, 5747,** etc., that are open
    - Can be configured to scan for others
  - Once connected → **brute-forces** usernames and passwords to **login to the device**
  - Use the device to **scan networks** looking for more IoT devices

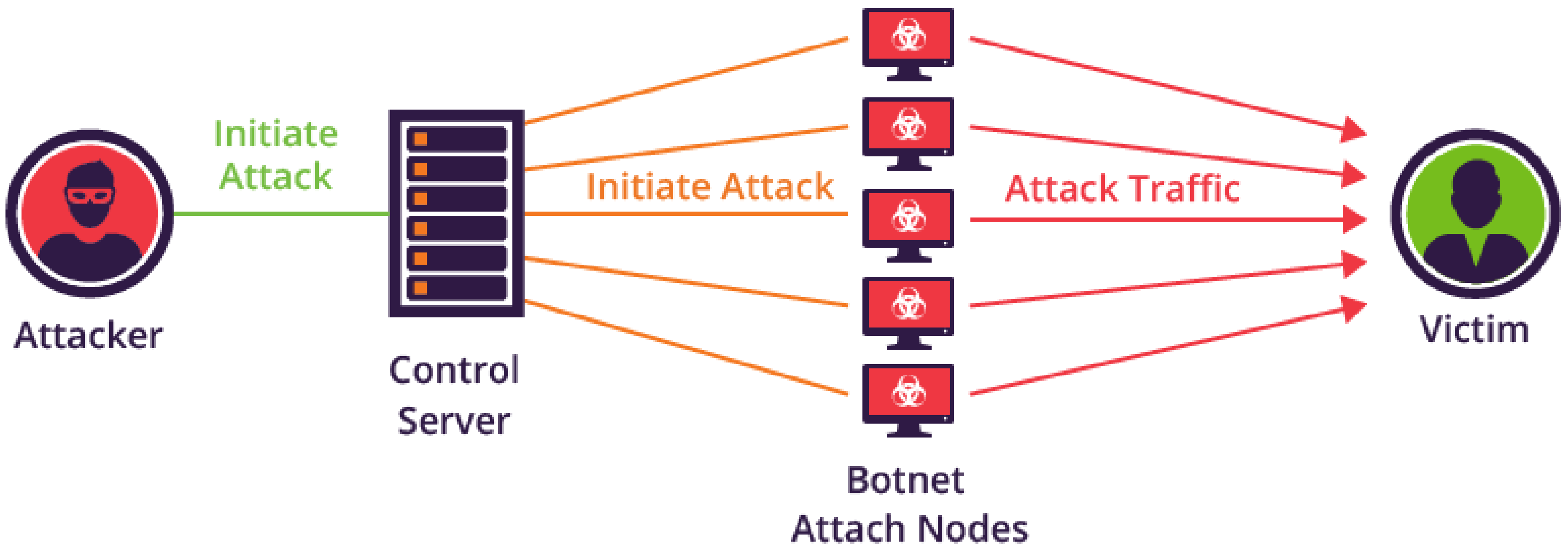
A few Examples of IoT Security Issues

- **Stage 2: Protect itself**
  - **Kill other process** running on infected device (SSH, Telnet, HTTP) to prevent owner from gaining remote access to device while infected
  - **Note:** Rebooting the device can <u>remove</u> the malware, but it can <u>become infected again</u>

- **Stage 3: Launch attack**
  - Infected device launches different types of attacks
  - HTTP floods, SYN floods, etc. → DDoS-based attacks

- ****Note**: Mirai contained a list of known networks in the U.S. to avoid attacking → U.S. Postal Service, Department of Defense

A few Examples of IoT Security Issues



https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

A few Examples of IoT Security Issues

https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

A few Examples of IoT Security Issues

- **2017**: IoT Goes Nuclear: Creating a **Zigbee** Chain Reaction

- Connected Zigbee lightbulbs → Attack steps:
  1. **Target**: Philips Hue lamps using ZigBee wireless connectivity.
  2. Recover the AES-CCM Encryption keys using a side channel attack (Correlation Power Analysis (CPA))
  3. Create a malicious firmware update (a worm)
  4. Load it to a Philips Hue light.
  5. The worm spreads by jumping directly from one lamp to its neighbours, using their built-in ZigBee wireless connectivity and their physical proximity
  - Range 400m outdoor and 70m indoor

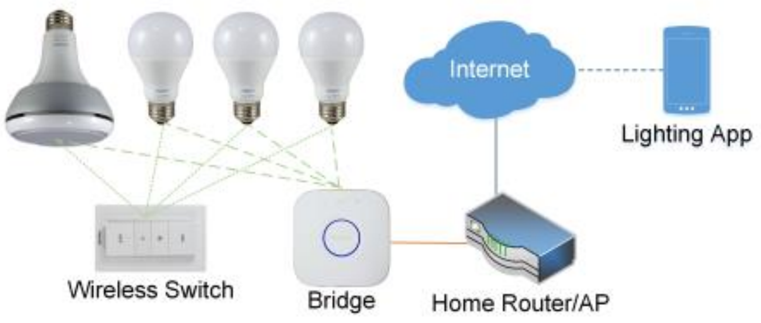


Figure 2. The ZLL architecture.


Figure 3. Philips Hue bridge (gateway), lamps, and wireless switch.

* Source image: [13]

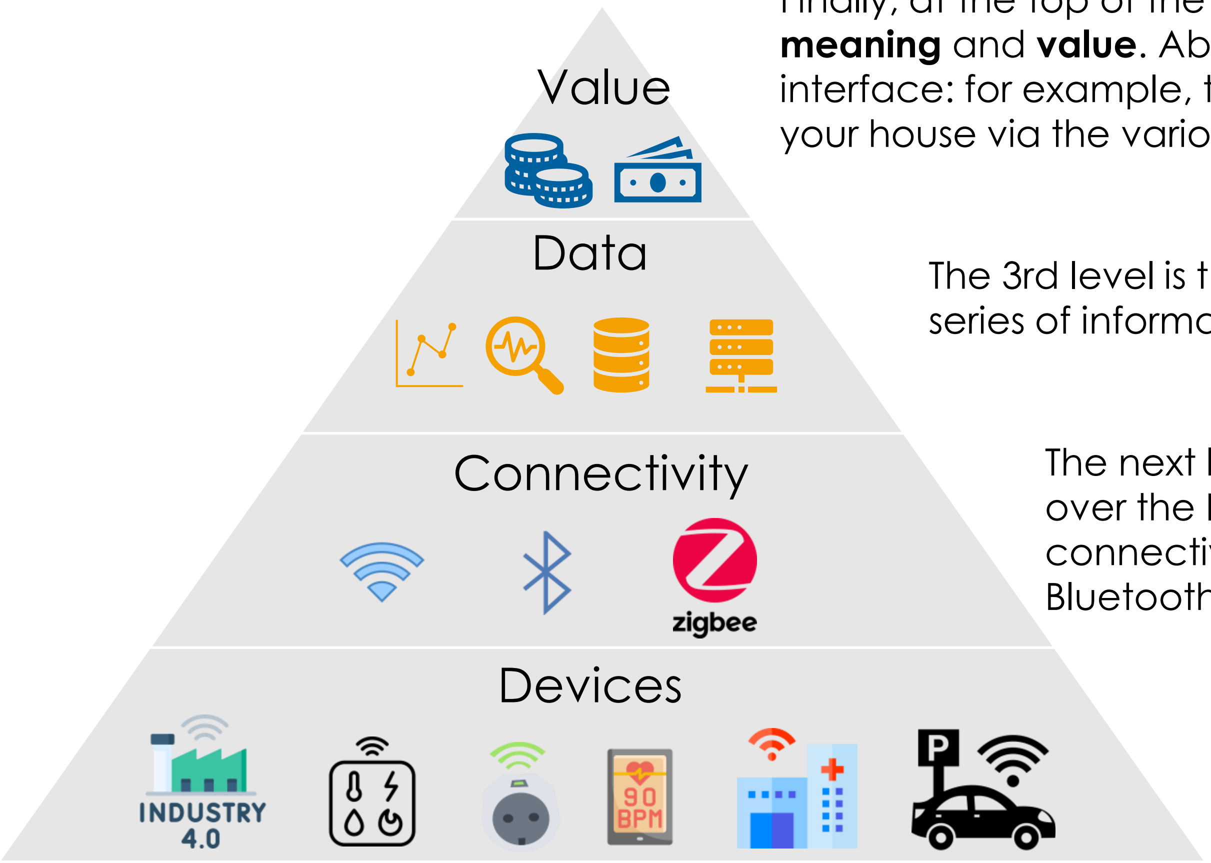
A few Examples of IoT Security Issues

Zigbee War Flying

Zigbee War Driving

https://www.youtube.com/watch?v=Ed1OjAuRARU&feature=emb_title&ab_channel=seyalr
https://www.youtube.com/watch?v=zcwz-lQtCwM&ab_channel=seyalr

IoT Architecture: global view



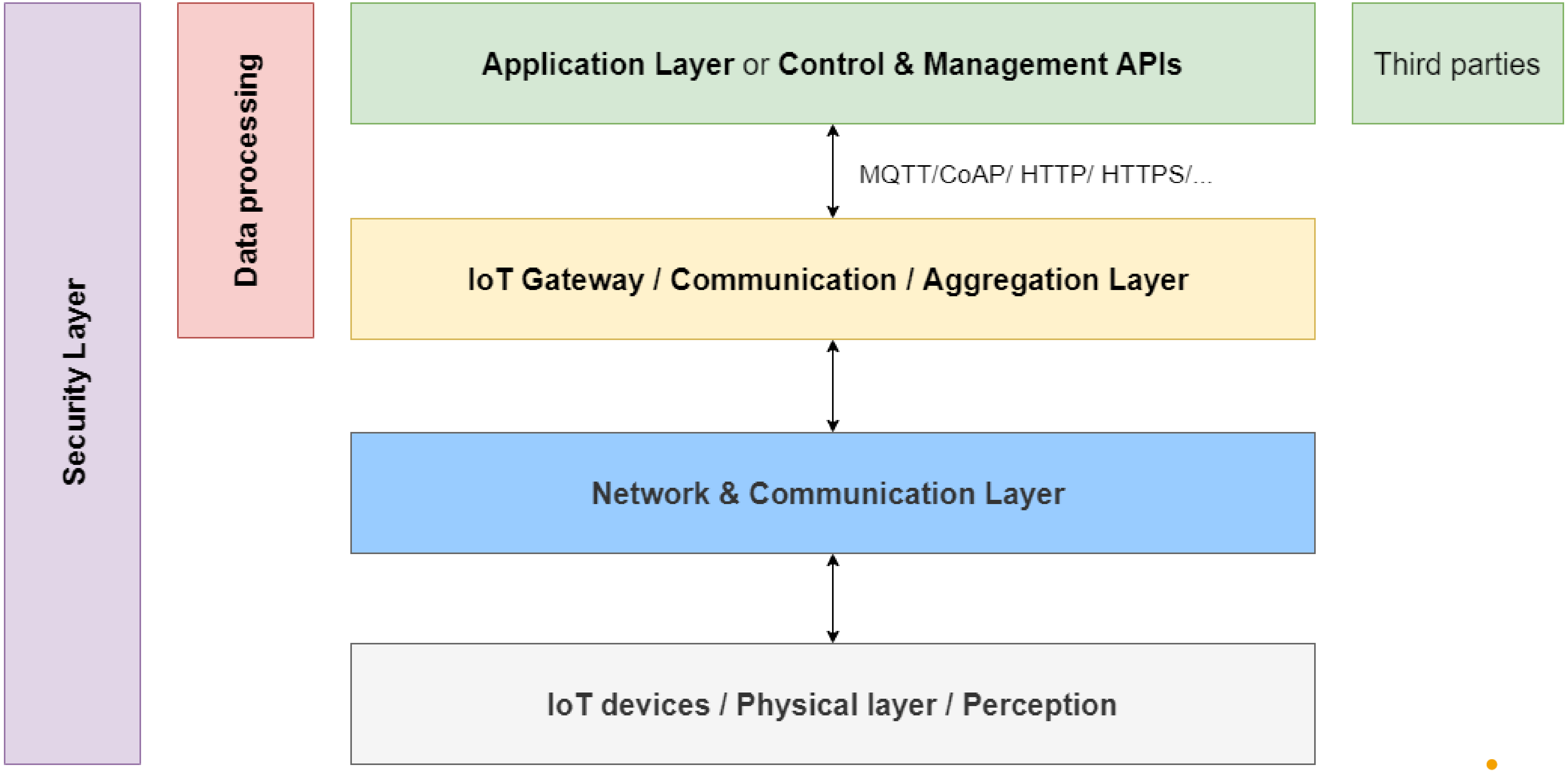
Finally, at the top of the pyramid, it is a matter of transforming this processed data to give it **meaning** and **value**. Above all, to be able to present it in an understandable and usable interface: for example, the application on your phone that communicates the temperature of your house via the various thermostats.

The 3rd level is the **data** level. The data arrives in its raw state. It is a series of information that must be sorted, analyzed and stored.

The next level is **connectivity**, i.e., how this captured data will be communicated over the Internet. You are probably already familiar with most of the different connectivity options: your home's WiFi, your phone's cellular network, your car's Bluetooth, etc.

The base of the pyramid is made up of **sensors** (**devices**), which capture and collect physical data from the environment. This can be humidity, temperature, presence, pressure...

IoT Architecture: global technical view



isep École d'ingénieurs du numérique

Security: outline

Broad topic:

we will see most important features,

but we will not cover them in (too much) depth

- **Security Properties**
- **Security Threats**
- **Security Functionalities**

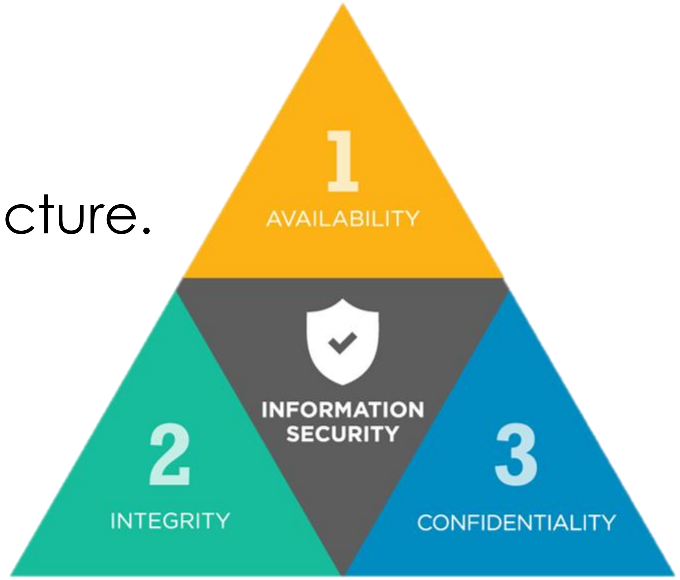
02

Main security concepts/properties

CIA

Main concepts
CIA

- **CIA** → Confidentiality Integrity and Availability
- Why ?
  - They are the **primary goals and objectives** of a security infrastructure.
  - Security **essentials**
  - Most important security **principles**
  - They are **interdependent**



Main concepts
CIA

- **Security controls** are typically evaluated based on the **respect of these principles**.
- A **complete security** solution should **adequately address each of these principles**
- **Vulnerabilities and risks** are also evaluated based on the **threat they pose against one or more of the CIA Triad principles**

Main concepts
Confidentiality

- Definition:
  - **The insurance of the protection of the secrecy of data, objects and resources.**
- Its main objectives:
  - **Prevent** or **minimize unauthorized access to data**
    - No one other than the legitimate recipient of a message receives it or is able to read it.
  - Provides means for **authorized users** to **access** and **interact with resources**

Main concepts
Confidentiality

- Some **attacks** that aim at violating this principle:
  - Capturing the network traffic
  - Stealing passwords
  - Social engineering
  - Port scanning
  - Shoulder surfing
  - Eavesdropping
  - Sniffing
  - Escalation of privileges
  - Etc.

Main concepts
Confidentiality

- Some security means to **guarantee confidentiality** includes, but not limited to:
  - Encryption of data
  - Strict access Control
  - Rigorous authentication procedures
  - Personal training
  - …

Main concepts
Confidentiality in IoT

- **In-device:** The data stored (if any) and the security keys need to be **safely stored** in the memory.
- **Device to Device**: **protecting** the **data exchanges** between IoT devices.
- **Device to Gateway**: **protecting** the **data exchanges** between the IoT device and the corresponding gateway.
- **Device to Cloud**: **protecting** the **data exchanges** between the IoT device and the cloud.
- **E.g.,**: via **data** or **traffic encryption**.

Main concepts
Integrity

- Definition:
  - **Is the concept of protecting the reliability and the correctness of the data.**
- Main objectives:
  - **Prevents unauthorized** subjects from **making modifications** on an object
  - **Prevents authorized** subjects from **making unauthorized modifications** (to avoid mistakes)
  - **Ensures** that the object remains **correct**, **unaltered** and **preserved** in most of the states of the object (data)

Main concepts

Integrity

- Some **attacks** that aim at **violating** this principle:
  - Viruses
  - Malwares
  - Errors in coding and applications
  - Man in the Middle
  - …

Main concepts

Integrity

- Some security means to **guarantee integrity** includes, but not limited to:
  - Encryption of data
  - Strict access Control
  - Rigorous authentication procedures
  - Data/Object Encryption
  - Using robust hash functions
  - Personal training
  - …

Main concepts
Integrity for IoT

- **Crowded frequency bands cause missed packets:**
  - Transmitting devices can **interfere** with nearby receiving devices.

- **Corrupted memory can lead to unexpected outcomes:**
  - Both flash and non-volatile memory can occasionally become corrupted.
  - **Unintended** or **intentionally** through malicious hardware hacking or malwares.
  - Regardless of the mechanism, it is imperative that microcontrollers are equipped with the necessary **integrity features** to identify when a device has been corrupted.
  - Once identified, the microcontroller can either **correct** the error or shut the device down, appropriately ensuring that the security of the wider system is not breached.

- **Sensor's data integrity:**
  - How to **guarantee** the integrity of the **data in transit** from the sensor to the end user ?

- In every stage of the IoT data life cycle from sensing and measuring, to interpreting and connecting the data, the quality and integrity of the information needs to be guaranteed. → E.g., via **hash function**

Main concepts
Availability

- Definition:
  - Authorized subject are granted **timely** and **uninterrupted** access to objects

- Its main objectives:
  - High level of **assurance** that the objects are **accessible to authorized subjects** and an acceptable level of performance
  - **Prevention** of Denial of Service (DoS)
  - Quick handling of **interruption** (**fault tolerance**)

Main concepts
Availability

- Some **attacks** that aim at **violating** this principle:
  - These include device failure
  - DoS attacks,
  - Object destruction
  - Communication interruptions or jamming
  - …

Main concepts
Availability

- Some security means to **guarantee availability** includes, but not limited to:
  - Providing redundancy mechanisms for critical systems
  - Maintaining reliable backups
  - Prevent data loss or destruction
  - Monitoring performance and network traffic
  - Using firewalls and IDS/IPS to prevent DoS/DDoS
  - Following a Business Continuity Planning (BCP) (in case of a disaster for instance)
  - Fault tolerance at the various levels of access/storage/security
  - Eliminating single points of failure (SPoF) to maintain availability of critical systems
  - …

Main concepts
Availability in IoT

- Ensuring that critical IoT devices are **always operational**
  - E.g., IoT monitoring sensors in healthcare or Industrial sensors
  - Quick detection and correction
  - Fault tolerance (redundant sensors !)

03

Security Threats

Taxonomy
Threat analysis

Security Threats
Definitions

- **Security Threat**: is anything that could cause **something bad** to an information system.
- **Attack**: consists in **intentionally** making **bad things** happening.
- **Vulnerability**: is a **weakness** that **enables an attack**.
- **Exploit**: is an **implementation of an attack**

Security Threats
Definitions

- A **threat** has the potential to exploit a vulnerability of the system to turn it into an attack
- A threat might or might not happen
- An attack may break (at least) one security property/concept
- The **consequence** of breaking security properties may be **huge** (even possibly destroying the system physically)
- An exploit typically uses (at least) one vulnerability

Security Threats
Taxonomy

- 9 main kinds of threats according to ENISA
  - **ENISA** = European Union Agency for Network and Information Security4
- During the reporting period (April 2020 to July 2021), the prime threats identified include:
  1. Ransomware;
  2. Malware;
  3. Cryptojacking;
  4. E-mail related threats; (e.g., phishing)
  5. Threats against data;
  6. Threats against availability and integrity;
  7. Disinformation – misinformation;
  8. Non-malicious threats;
  9. Supply-chain attacks

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Security Threats
Taxonomy

- Threats may be distinguished by:
  - Their **sources:**
    - Accidental or intentional, internal or external, low or high capacity
    - Depend on the context (e.g., a company with temporary workers using IoT objects connected to its servers might consider extra external sources)
  - Their **targets:**
    - Sensors, servers, databases, networks, software, users, ...
  - Their **operational modes:**
    - Modification of usage, overstepping of functional limits, deterioration, destruction, spying, ...

Security Threats
Taxonomy

- **Some threats related to IoT:**
  - Vulnerabilities
  - Malwares (ransomwares;)
  - Botnets
  - Denial of services (Threats against availability and integrity;)
  - Physical attacks (threats against data; Threats against availability and integrity;)
  - Information theft and unknown exposure (threats against data;)
  - Device mismanagement and misconfiguration
  - Lack of encryption (Threats against availability and integrity;)
  - Firmware updates Missing
  - …

Security Threats
Attacks

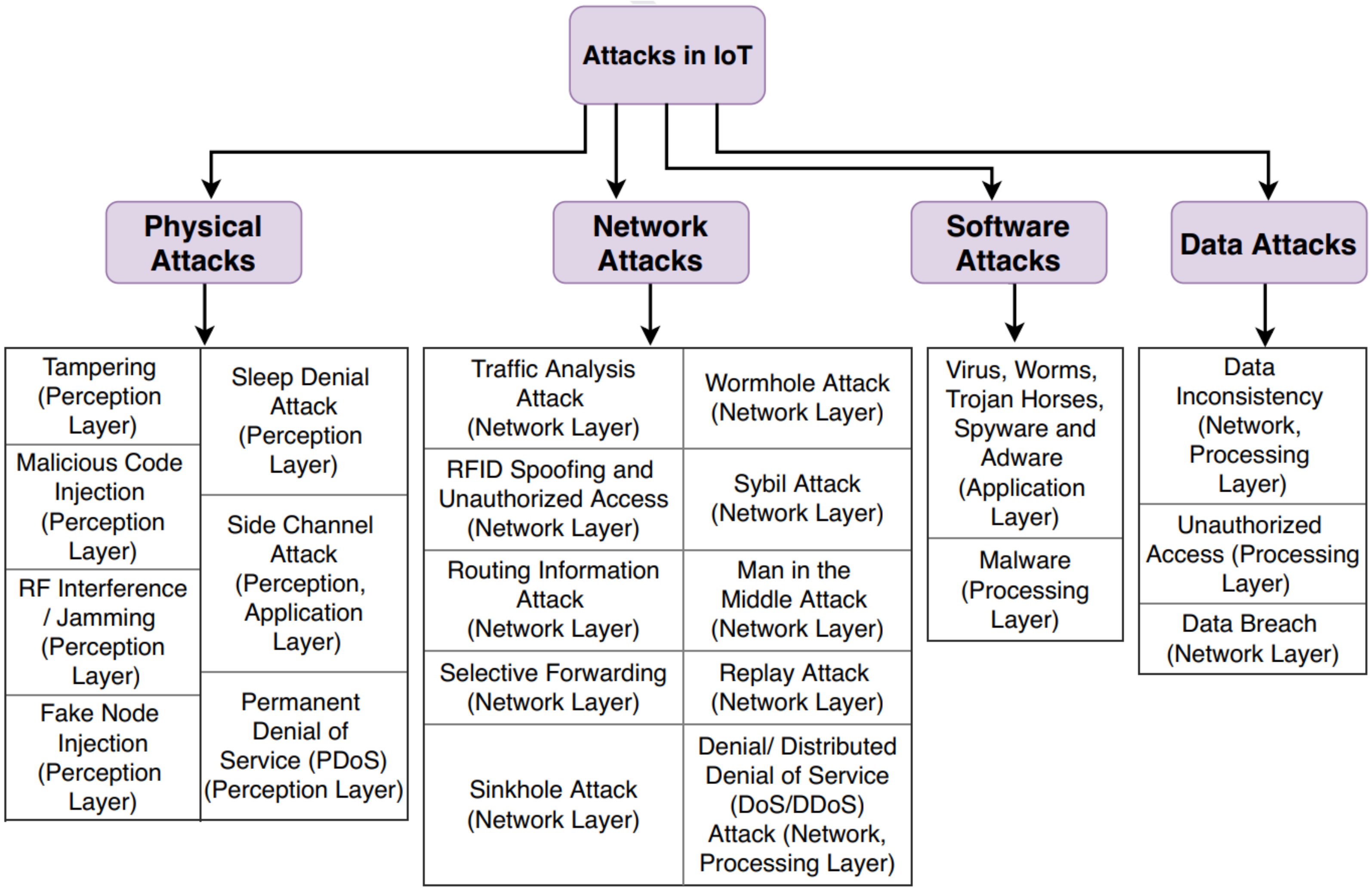


Figure 2: *Attacks in IoT*

* Source image: [9]

Security Threats
Attacks

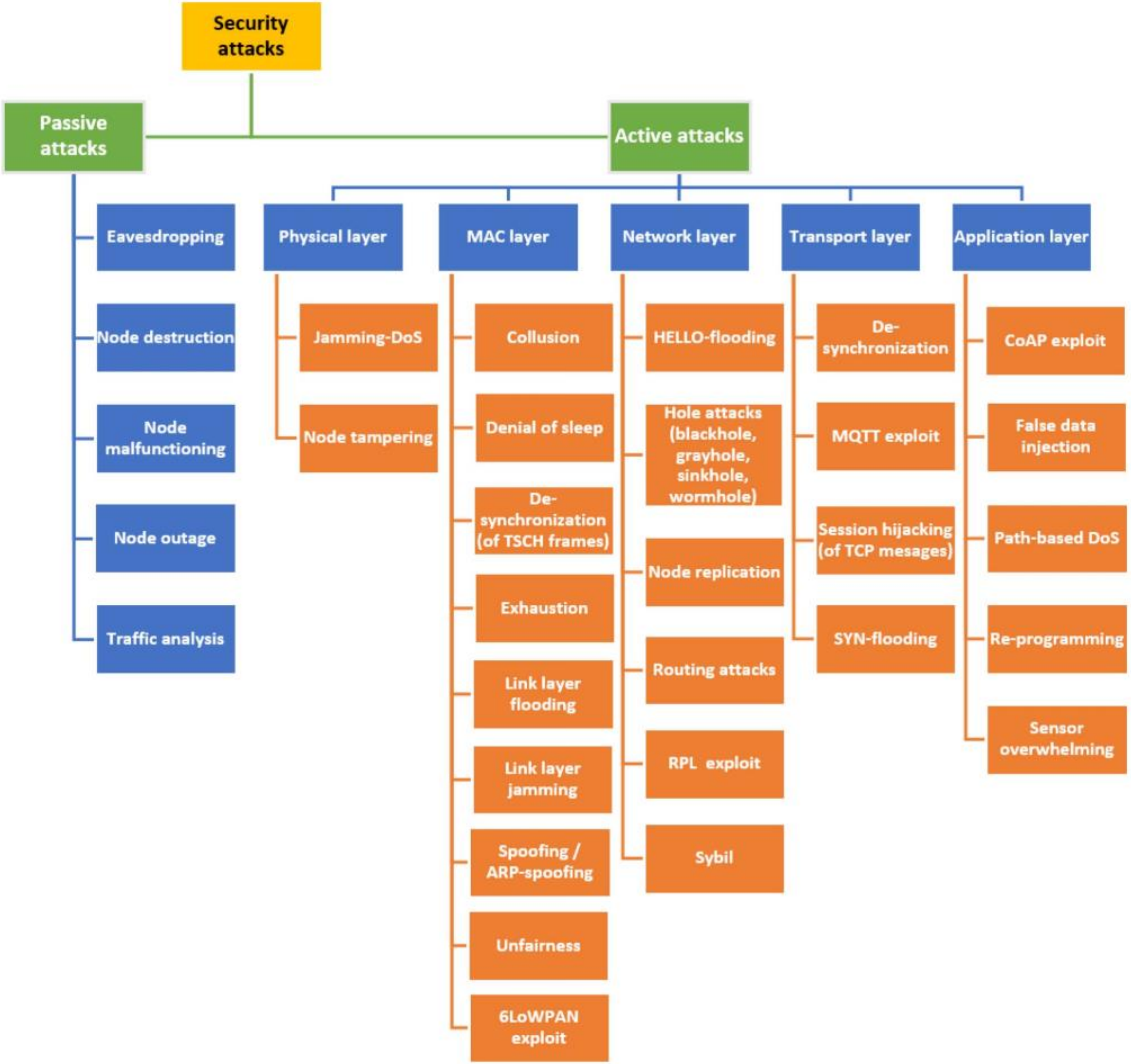


Fig. 3. Security attacks towards the WSNs and IoT - OSI stack protocol layered description.

* Source image: [10]

04

IoT and Smart Infrastructures

ENISA
Shodan

ENISA: Good practices for IoT and smart Infrastructures

- **ENISA**: European Union Agency For Cybersecurity

- **Smart infrastructure**, enabled by technologies like IoT, offer numerous of advantages bringing serious cost savings and efficiencies.

- These kinds of **data-driven environments**, fuelled by **connected devices** and network connectivity, become a **new attack surface for cyber threats**.

- **ENISA** develops **guidance** to **secure IoT and Smart Infrastructures** from cyber threats, by **highlighting good security practices** and proposing **recommendations** to operators, manufacturers and decision makers.

Source: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

ENISA: Good practices for IoT and smart Infrastructures

- It provides also a Good practices for IoT and Smart Infrastructures **Tool**
- This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.
- It provides:
  - Baseline security IoT
  - Smart cars security
  - Smart hospitals security
  - Smart cities
  - Industry 4.0
  - Smart Airports

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

Shodan

SHODAN

- Is a **search engine** for Internet-connected devices

- If a device is directly hooked up to the Internet, then Shodan queries it for various **publicly-available information**.
  - **Device name:** What your device calls itself online. For example, Samsung Galaxy S21.
  - **IP address:** A unique code assigned to each device, which allows the device to be identified by servers.
  - **Port #:** Which protocol your device uses to connect to the web.
  - **Organization:** Which business owns your "IP space". For example, your internet service provider, or the business you work for.
  - **Location:** Your country, city, county, or a variety of other geographic identifiers.

- The types of devices that are **indexed** can vary tremendously:
  - Baby monitors
  - Internet routers
  - Security cameras
  - Maritime satellites
  - Traffic light systems
  - Nuclear power plants
  - Etc.

https://www.shodan.io/

Shodan

- It allows to **search for very specific types of devices**
  - Can be used to **exploit vulnerabilities !**
  - To **protect yourself / your organization**

- **Be careful when using this tools:** you don't have the right to access unauthorized information (rules change from one country to another)

https://www.shodan.io/

60

Années d'excellence

www.isep.fr