IoT Security
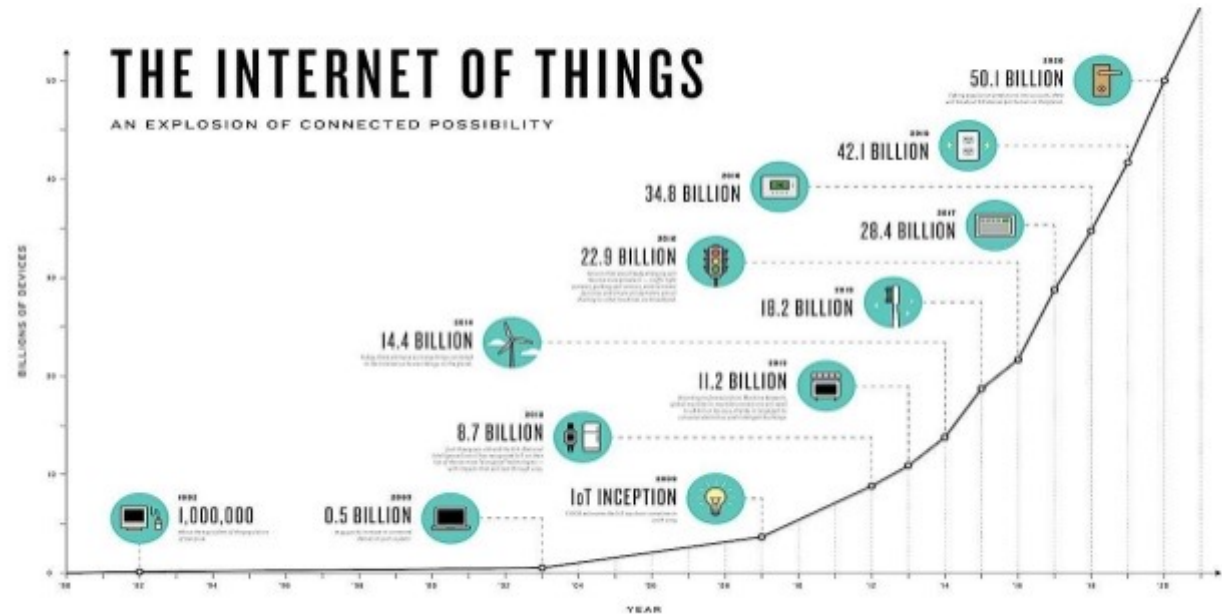
CORSO DI LAUREA MAGISTRALE IN INFORMATICA
(CLASSE LM-18) – Curriculum in Internet of Things
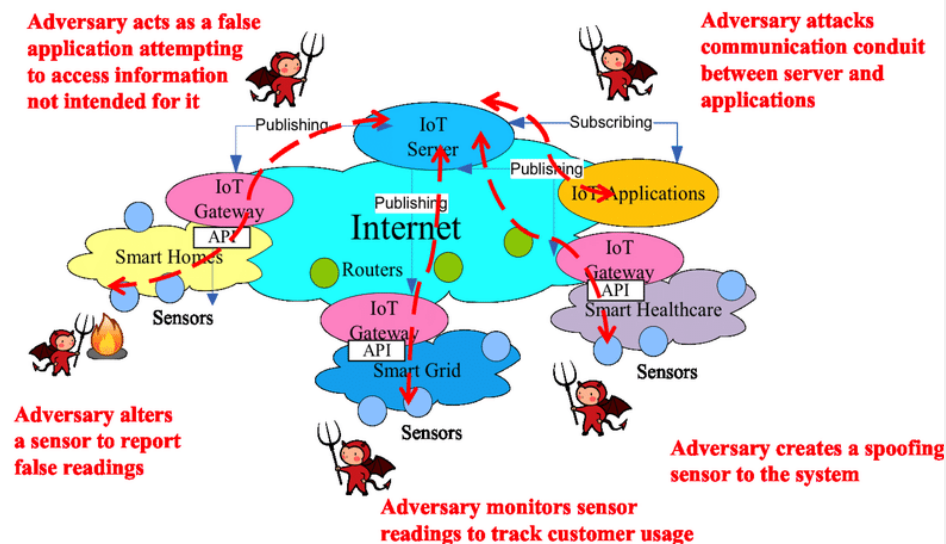
IoT- Explosion of connected possibilities
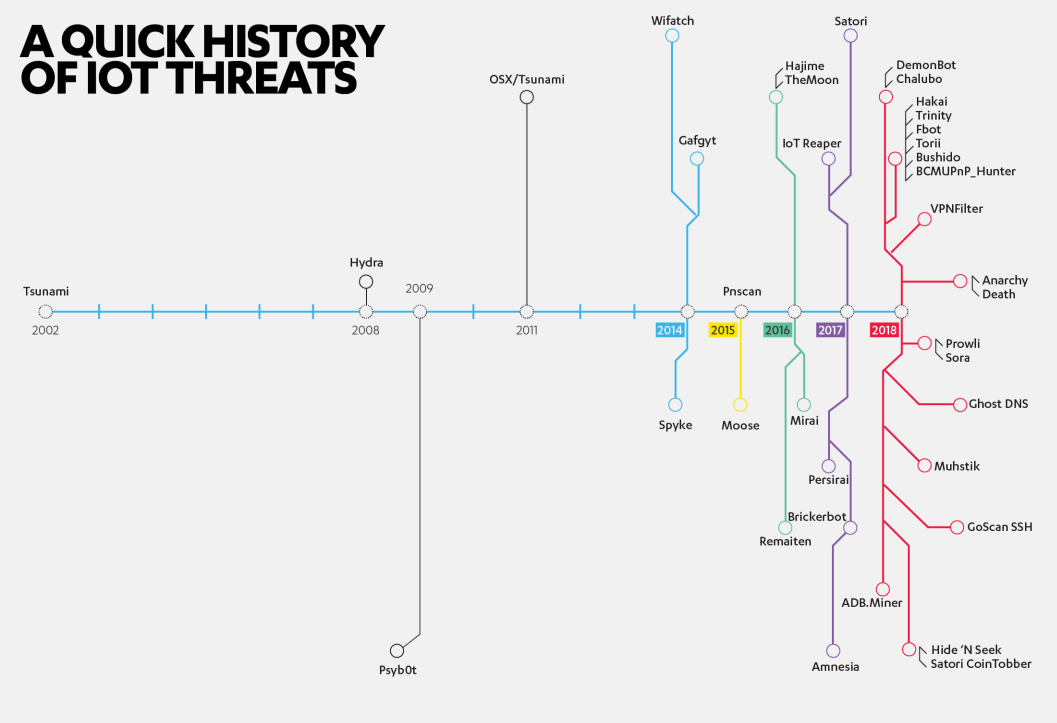
We are witnessing a dramatic increase of smart devices being deployed to support various kinds of projects and applications.
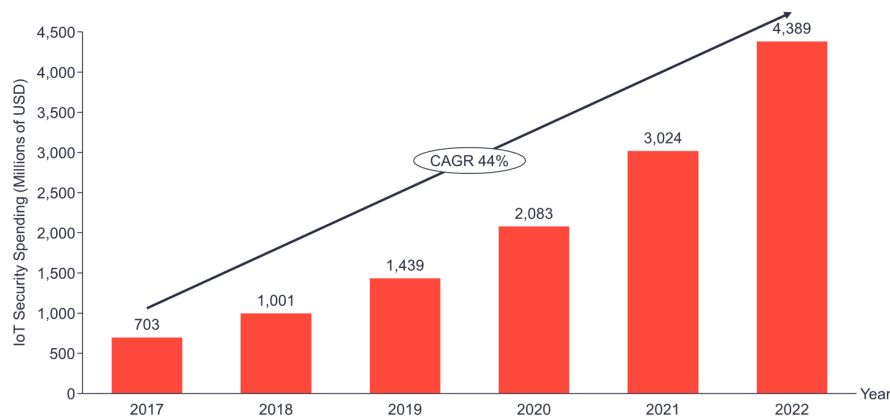

THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY

Recently, hacking events targeting IoT devices have increased, with negative effects achieving higher impacts.
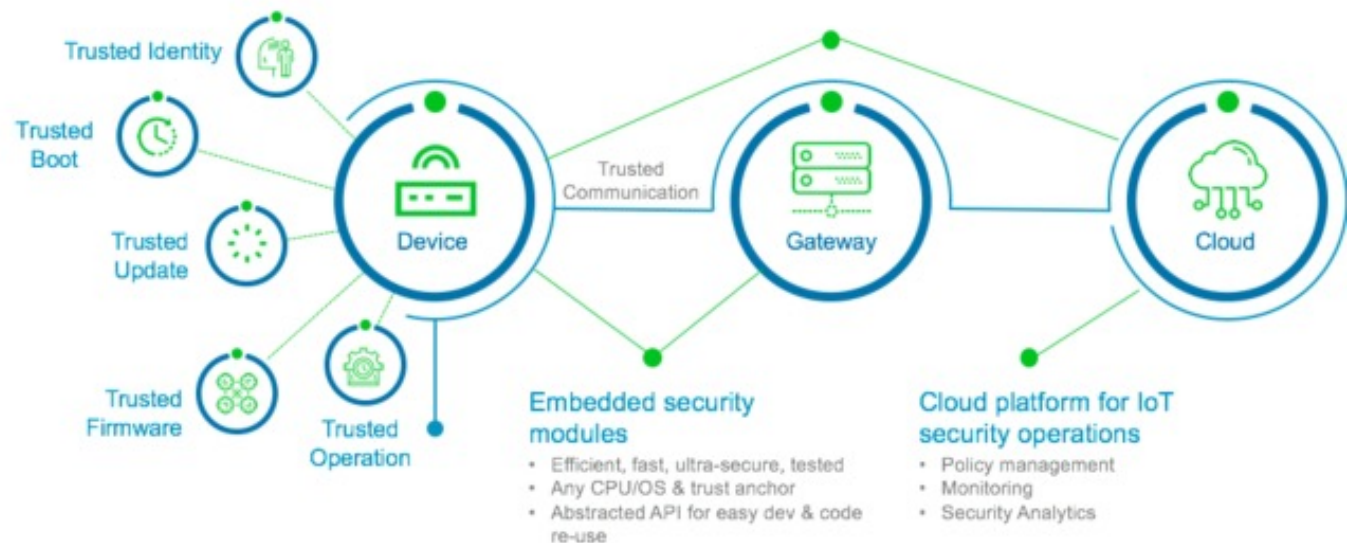

A QUICK HISTORY OF IOT THREATS

Global spending on IoT security is forecasted to grow at a Compound Annual Growth Rate of 44% over the six-year period to become a $4.4B market opportunity by 2022

IoT Security is very challenging as it involves multiple aspects and requires heterogeneous competences.

IoT nodes hold sensitive data about their users, and here it comes the privacy issues to be also considered and the compliance with the GDPR.

Trusted Identity

Trusted Boot

Trusted Update

Trusted Firmware

Trusted Operation

Device

Trusted Communication

Gateway

Cloud

Embedded security modules
- Efficient, fast, ultra-secure, tested
- Any CPU/OS & trust anchor
- Abstracted API for easy dev & code re-use

Cloud platform for IoT security operations
- Policy management
- Monitoring
- Security Analytics

PRIVACY 62%

SECURITY 54%

WHAT WOULD CONCERN YOU ABOUT A WORLD OF CONNECTED DEVICES?

PHYSICAL SAFETY 27%

UNABLE TO REPAIR 24%

MACHINES TAKING OVER THE EARTH 21%

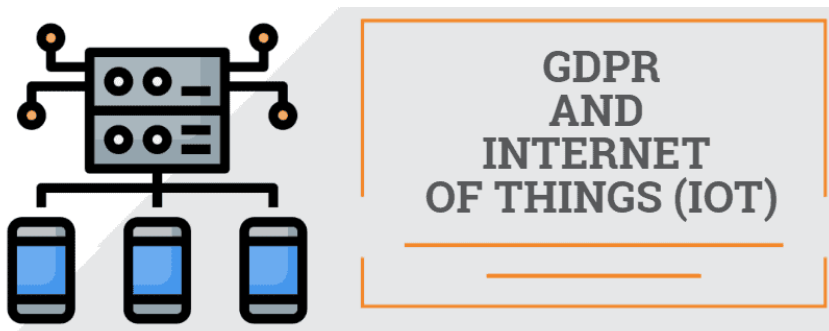NOT KNOWING HOW TO USE THEM 17%

NO TANGIBLE BENEFITS 11%

IoT Security happens on four different levels

Device, Communications, Cloud, and Lifecycle Management
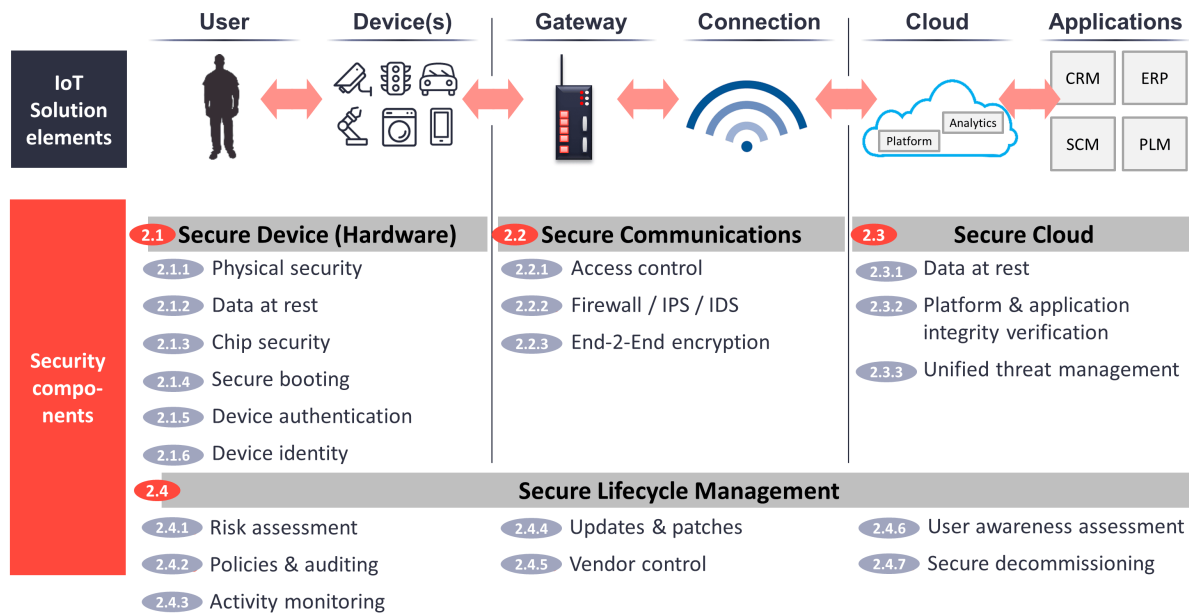
The aim is to teach the main solutions from the hardware, software and network-perspective to protect IoT deployments, and ways to test the provided security guarantees.

During the course, privacy and data protection measures for IoT will be described, by highlighting the technological solutions to be introduced at the design stage, and how respecting the accountability principle introduced by the GDPR.

Cource Outline

- Introduction to the platforms, middleware and networking technologies

- Security properties and attacks

- Hardware design for protection means

- PenTesting for the IoT Devices

- Physical Unclonable Functions

- Lightweight Cryptography

- Secure D2D protocols and networking

- Trusted Execution Environments

- Blockchain for IoT Security

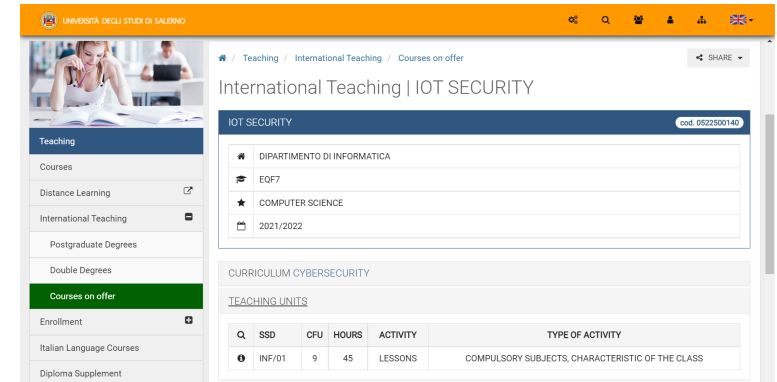- IoT Privacy and GDPR compliance

Teaching Approach

Lessons are held on Monday from 9:00 to 11:00 and on Tuesdays from 11:00 to 13:00, for a total of 45 hours and 9 CFU, and the used language is English.

30 hours of lessons are about the topics of the course, while the remaining ones consist in lab experience on real devices and boards.

No background on IoT programming is required. Expertise on C programming, networking protocols and distributed systems is required.

A project will be required at the exam: a presentation of an advanced topic related to the course aim or the implementation of a security solution. After project presentation, an oral discussion will take place.
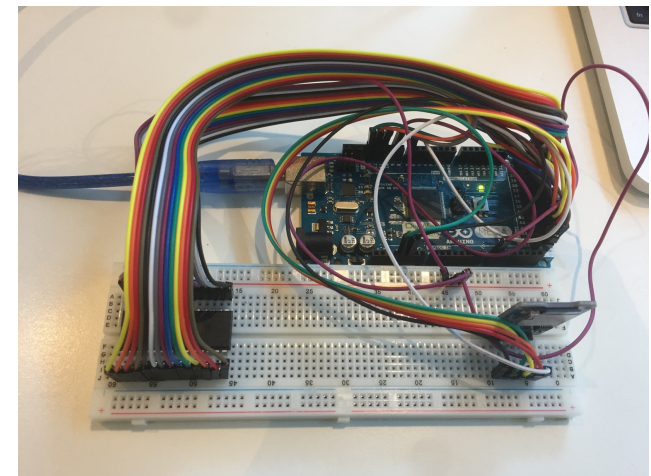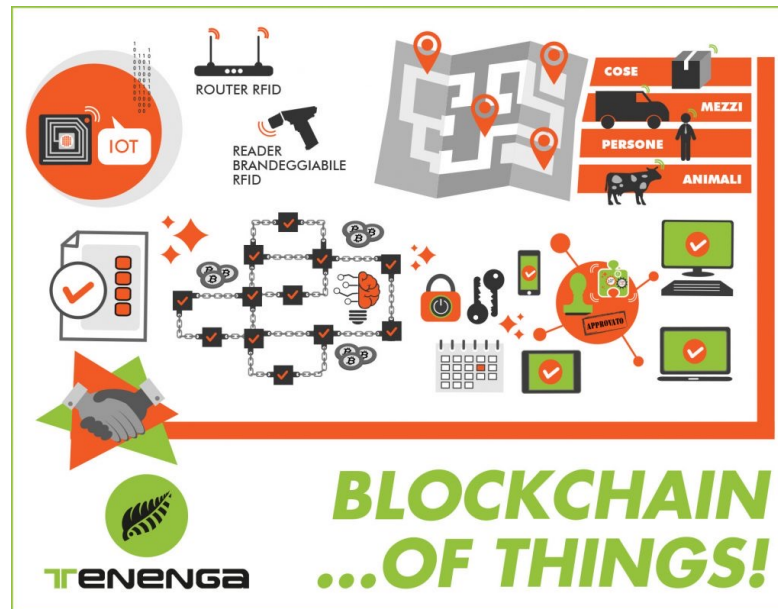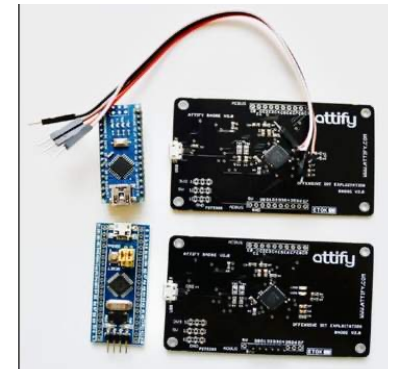
Teaching Material

The lessons of the taught theory will be supported by slides in MS PowerPoint available at the department's Moodle.
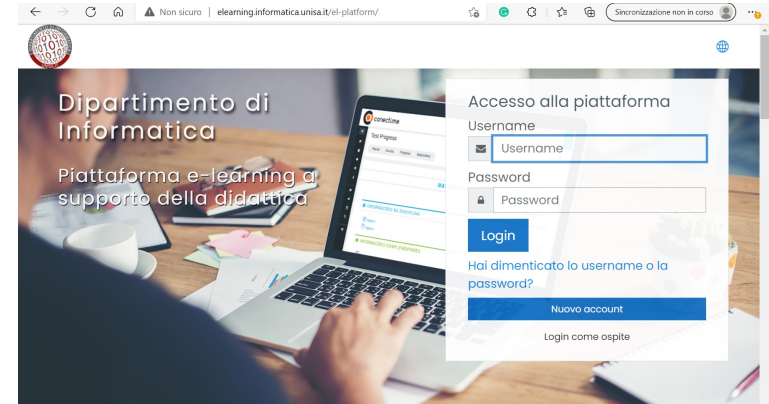
The laboratorial exercises will be realised by mainly using Arduino/STM32/ESP32 boards, and devices and libraries supporting several security features. Blockchain will be used to device security solutions for IoT.

Per maggiori informazioni

@
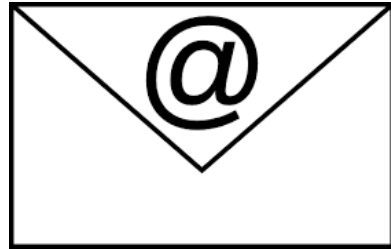
Christian Esposito
esposito@unisa.it