The Internet of broken Things: a short film of the future security challenges

Andrea Melis @wildboar
Ulisse Lab Unibo
6th December 2017

Agenda

- Information Gathering
  - History and Definition
  - The context
  - My Definition
  - Motivations
- Service Disclosure
  - What's a Thing?
  - Technologies Involved
  - Hardware (Rasp, Arduino, Sensors,..)
  - Software (MQTT, Blue*,ZigBee, ..)
- Exploits
  - Attack Surface
  - 10 OWASP
  - Real Attacks
- Defense
  - Demos
  - Conclusion.

Once upon a time..

Once upon a time..

Ritratto di Kevin Ashton

Once upon a time..

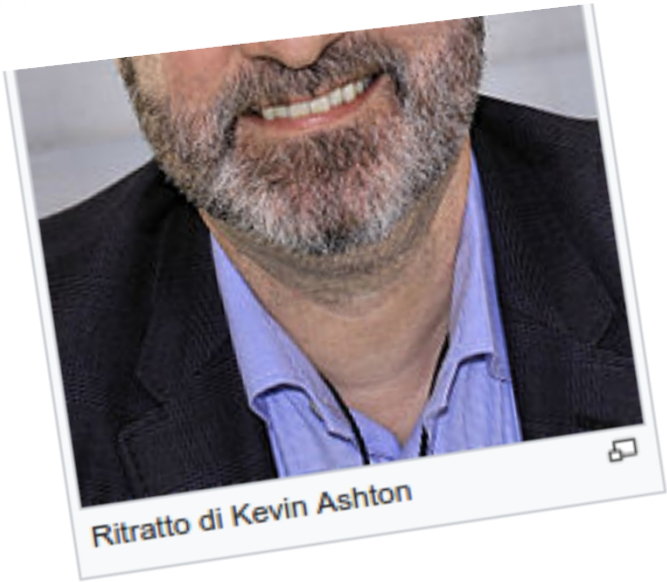
The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crude method alerted the radar crew on the ground that these were German planes and not allied aircraft. Essentially, this was the first passive RFID system.

Ritratto di Kevin Ashton

Once upon a time..

The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crew on the ground that these were G... the first ...

decades. The first Internet appliance , for example, was a Coke machine at Carnegie Melon University in the early 1980s. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.



Ritratto di Kevin Ashton

Once upon a time..

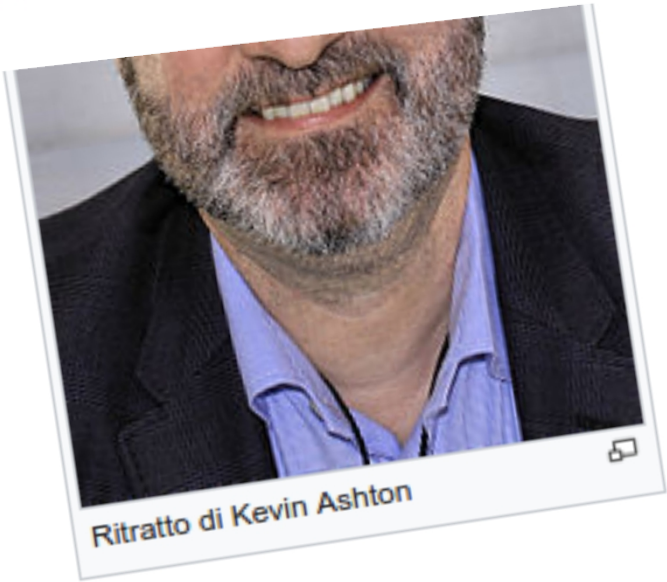
The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crew on the ground that these were C... the first ...

decades. The first Internet appliance , for example, was a Coke machine at Carnegie Melon Univer... in the early 1980s. The programmers could connect to the machine over the Inte... machine and determine whether or not there would be a c... y decide to make the trip down to the machine.

2005

The United Nations first mentions IoT in a published **International Telecommunications Union** report

A new dimension has been added to the world of information and communication...from anytime, anyplace connectivity for anyone, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things.



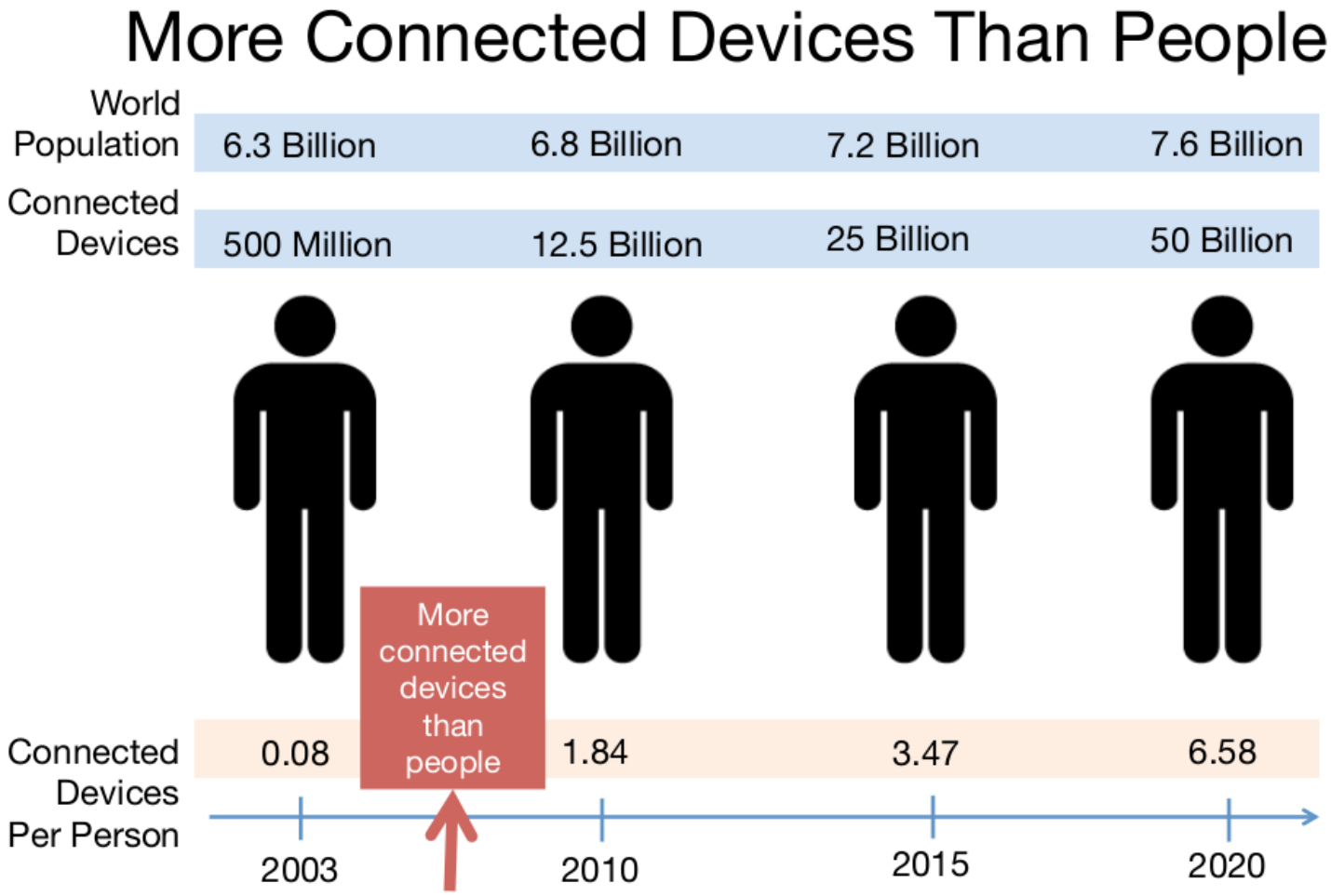
Ritratto di Kevin Ashton

IEEE DEFINITION

Internet of Things, IoT, is an application domain that integrates different technological and social fields. The IoT covers many areas ranging from enabling technologies and components to several mechanisms to effectively integrate these lowI level components.

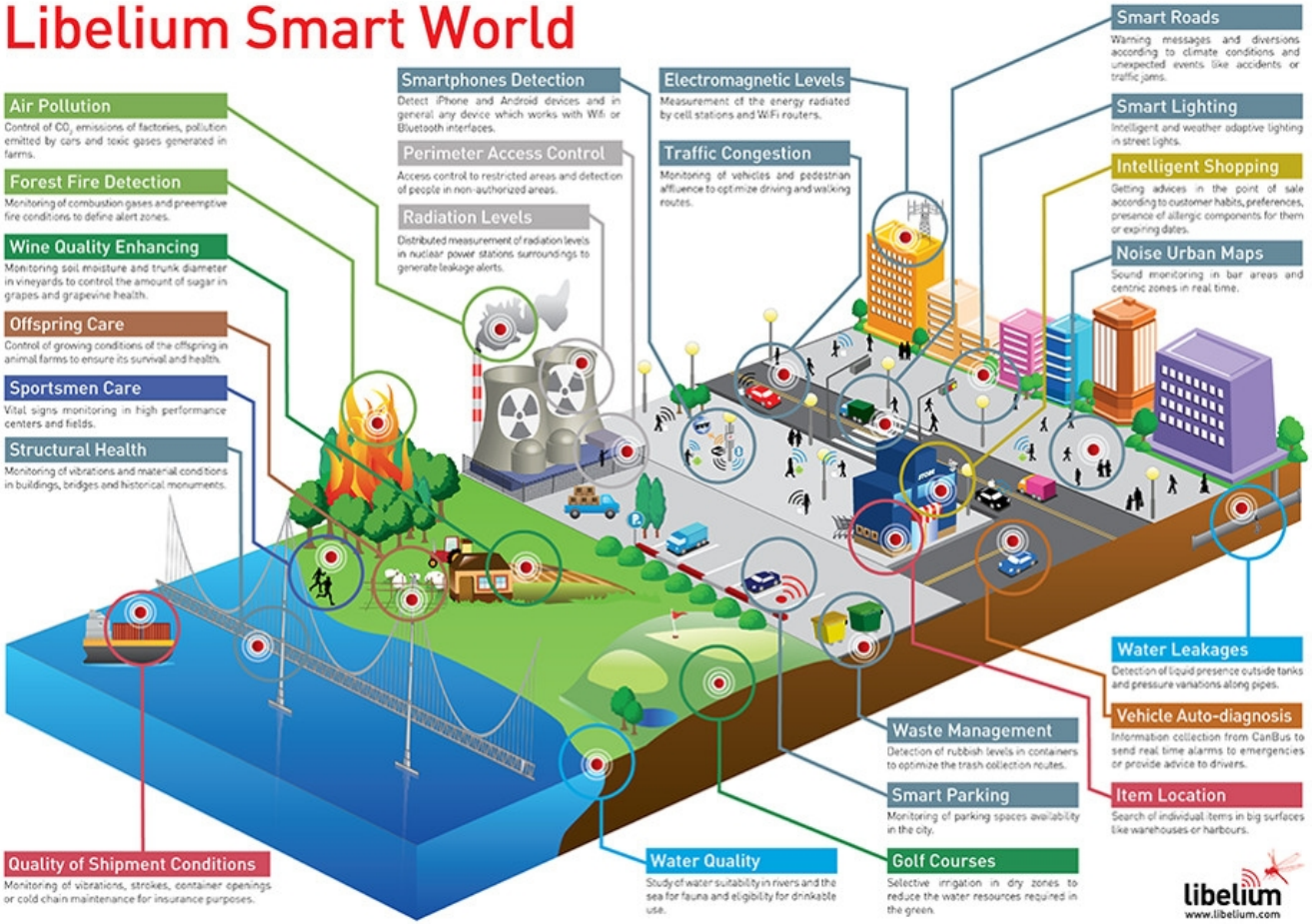
Software is then a discriminant factor for IoT systems. IoT operating systems are designed to run on small scale components in the most efficient way possible, while at the same time providing basic functionalities to simplify and support the global IoT system in its objectives and purposes.

Present, Past, Future



[Source: Cisco IBSG, April 2011]

Infographic Ecosystem



My Point of View

The actual IoT application domain is a technological consequence of the advent of new hardware and software low-cost developments paradigms.

My Point of View

The actual IoT application domain is a technological consequence of the advent of new hardware and software low-cost developments paradigms.

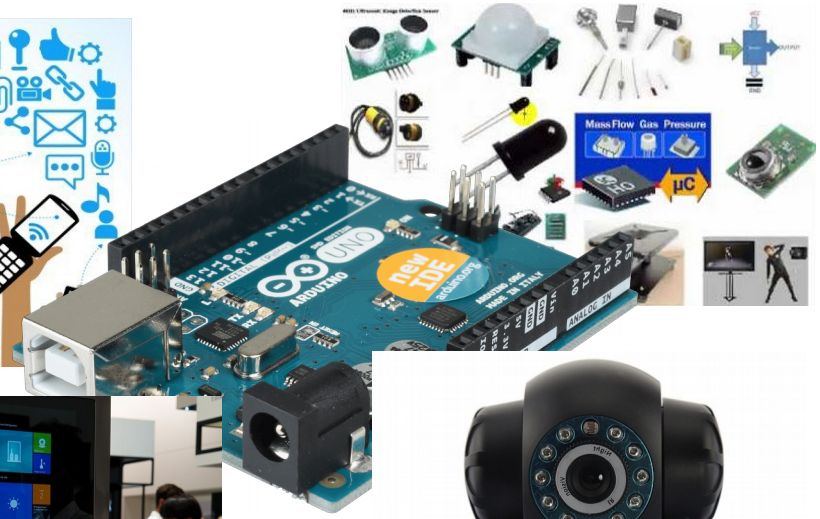
Motivations

Motivations

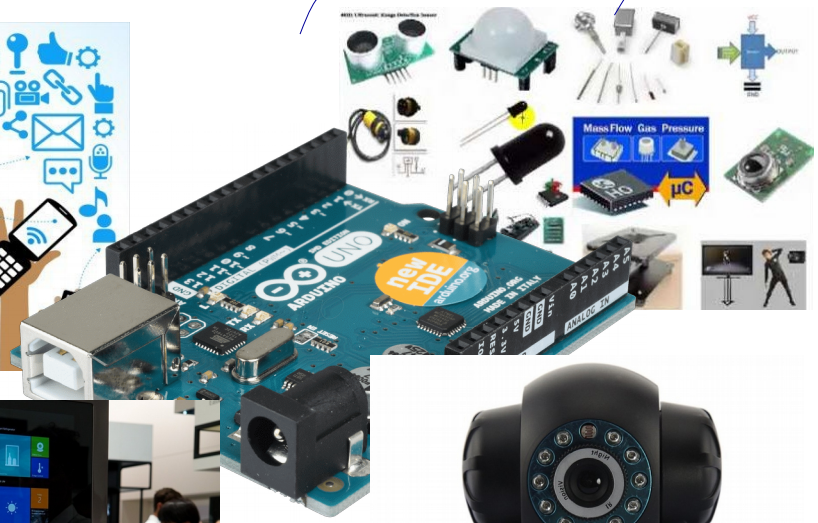
Motivations

Motivations

Motivations

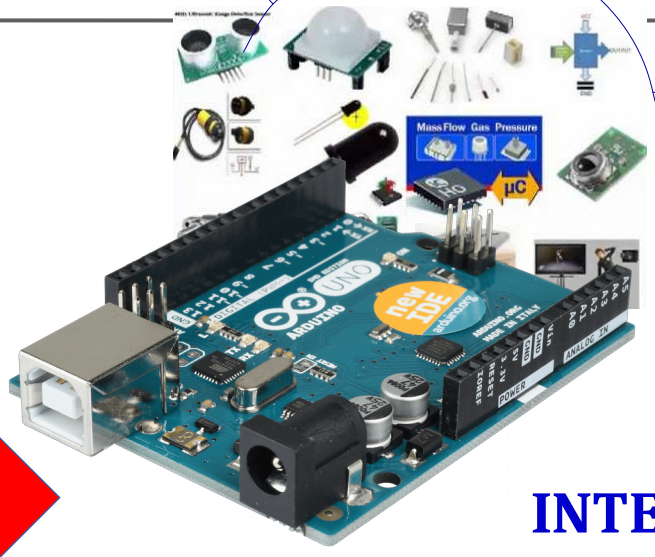


Motivations



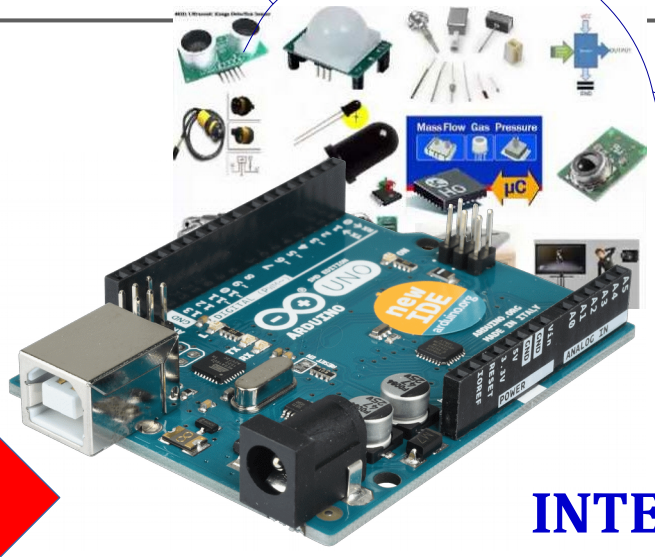
INTERNET

Motivations



INTERNET OF THINGS

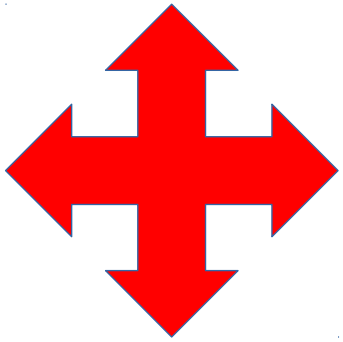
Motivations



???

INTERNET OF THINGS

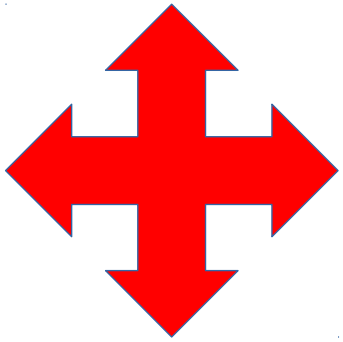
Why “Broken” Things?



Need of set of new communication protocol with this characteristics:

- Consistent with the current standards
- Low battery consumption
- Easy to implement
- Easy to deploy
- Low rate consumption
- Standardizable?

Why “Broken” Things?

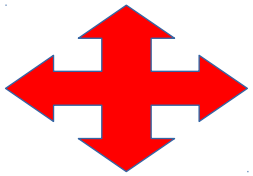


Need of set of new communication protocol with this characteristics:

- Consistent with the current standards
- Low battery consumption
- Easy to implement
- Easy to deploy
- Low rate consumption
- Standardizable?

WHAT ABOUT SECURITY?

Why “Broken” Things?



Need of set of new communication protocol with this characteristics:

- Consistent with the current standards = like Bluetooth 1.1 ?
- Low battery consumption = ...
- Easy to implement = KISS doesn’t mean for dummies
- Easy to deploy = We don’t need security features
- Low rate consumption = And this is NOT a security feature
- Standardizable? = like BLE?

WHAT ABOUT SECURITY?

Agenda

- Information Gathering
  - History and Definition
  - The context
  - My Definition
  - Motivations
- Service Disclosure
  - What's a Thing?
  - Technologies Involved
  - Hardware (Rasp, Arduino, Sensors,..)
  - Software (MQTT, Blue*,ZigBee, ..)
- Exploits
  - Attack Surface
  - 10 OWASP
  - Real Attacks
- Defense
  - Demos
  - Conclusion.

What's a "Thing"?

A Measure

Source: IEEE Internet of Thing World Forum

What's a "Thing"?

A Measure

An action

Source: IEEE Internet of Thing World Forum

What's a "Thing"?

A Measure

An Identity

An action

Source: IEEE Internet of Thing World Forum

What's a "Thing"?

A Measure

An action

An Actuator. A device capable of executing an action
An actuator is the mechanism by which a control system acts upon an environment.

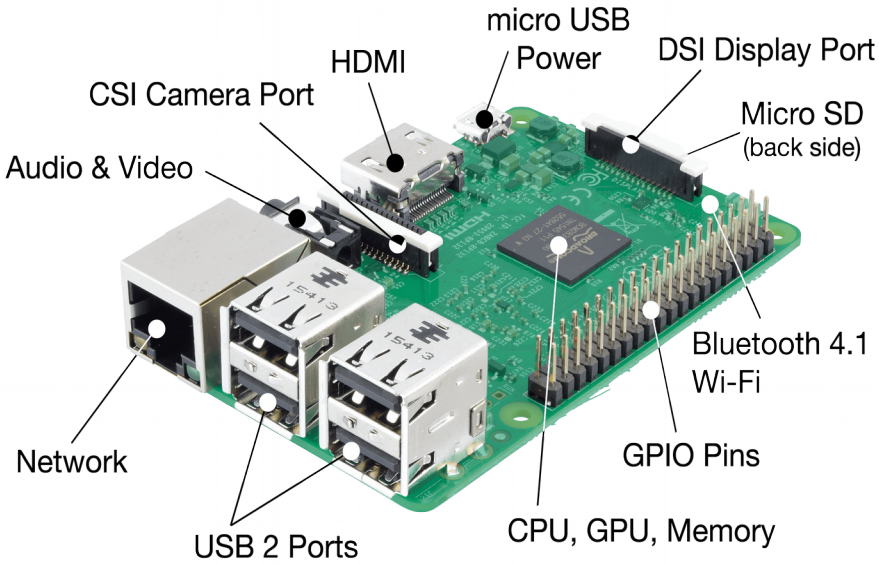
A sensor is an object whose purpose is to detect events or changes in its environment, and then provide a corresponding output

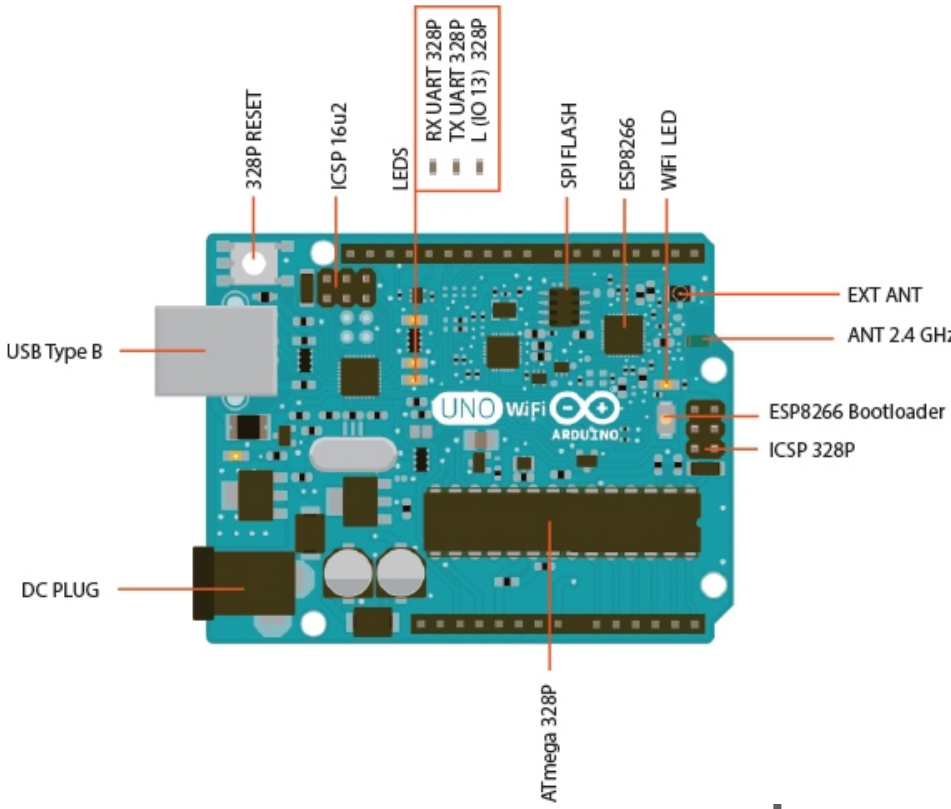
An Identity

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

Source: IEEE Internet of Thing World Forum

Hardware Rasp. Vs Arduino



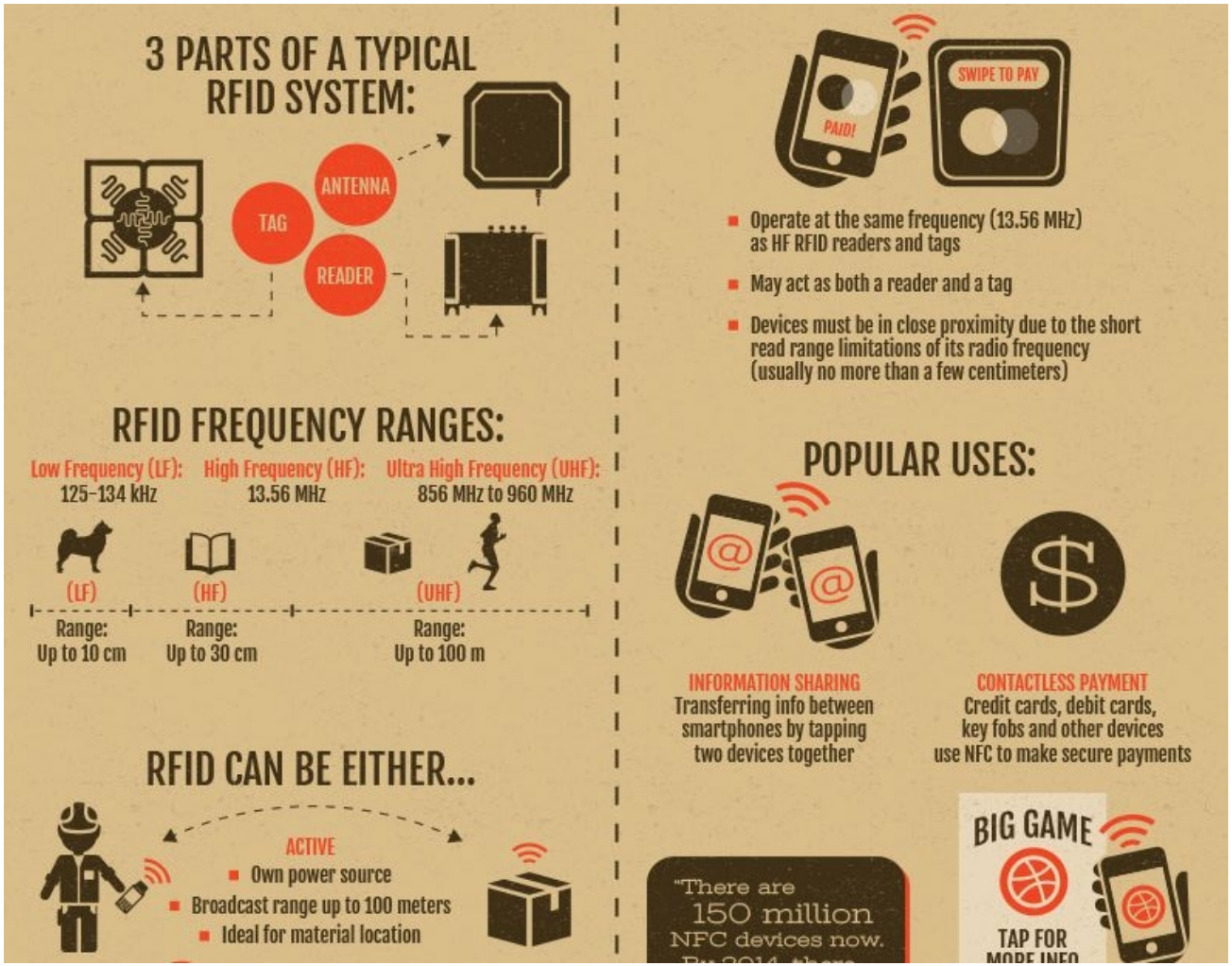


Hardware Rasp. Vs Arduino

Arduino vs Raspberry Pi

Specs	Arduino Uno 	Raspberry Pi 3 Model B 
CPU type	Microcontroller	Microprocessor
Operating System	None	Linux (usually Raspbian) or Win 10
Speed	16 Mhz	1.2Ghz
RAM	2KB	1GB
GPU/Display	None	VideoCore IV GPU
Disk	32KB	Depends on SD card
GPIO pins	14 digital pins (includes 6 analog)	26 digital pins
Other connectivity	None	USB, Ethernet, HDMI, audio
Power consumption	0.25W	6W

RFID vs NFC

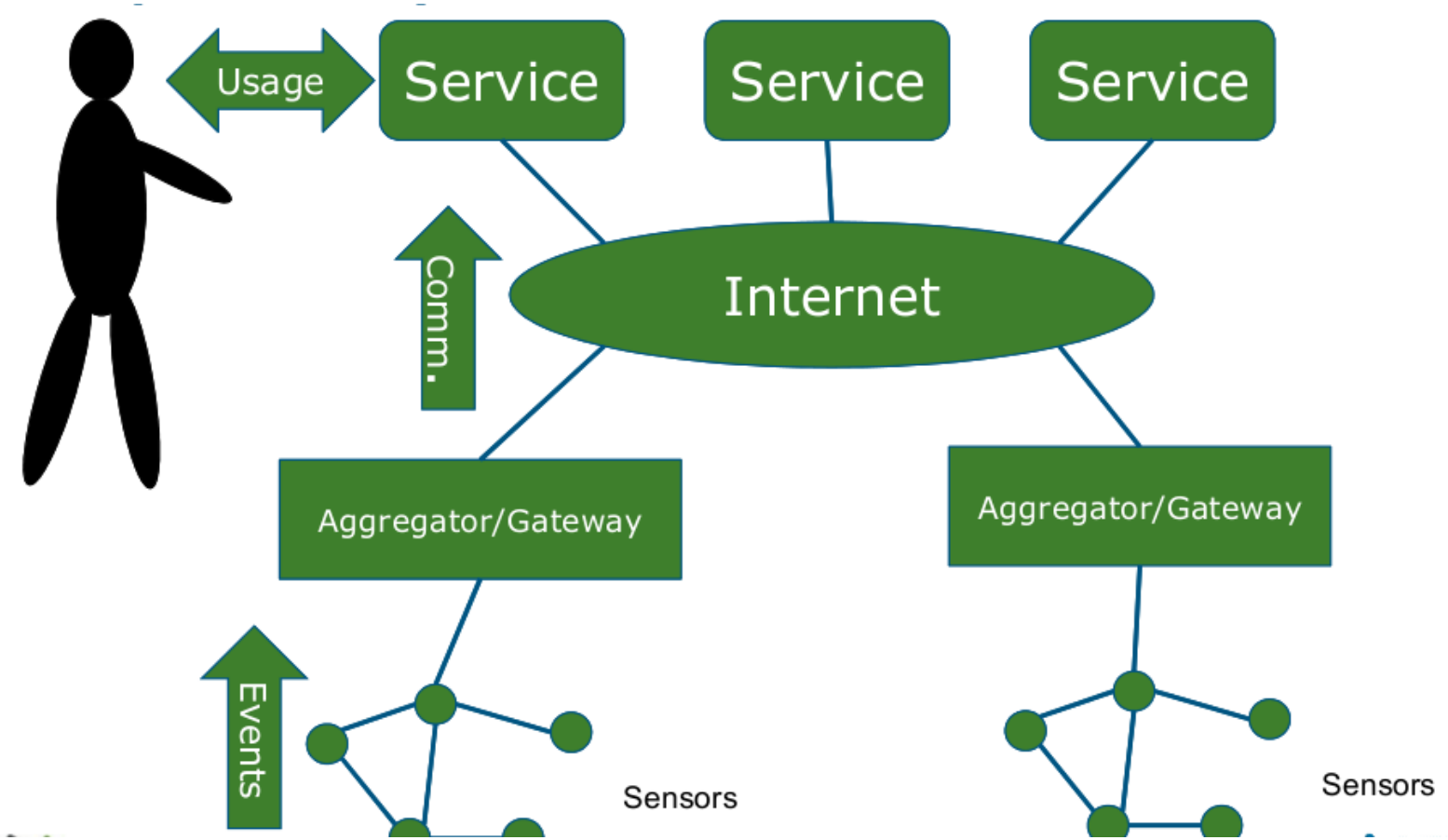

3 PARTS OF A TYPICAL RFID SYSTEM:
ANTENNA
TAG
READER
RFID FREQUENCY RANGES:
Low Frequency (LF): 125–134 kHz
High Frequency (HF): 13.56 MHz
Ultra High Frequency (UHF): 856 MHz to 960 MHz
(LF)
(HF)
(UHF)
Range: Up to 10 cm
Range: Up to 30 cm
Range: Up to 100 m
RFID CAN BE EITHER...
ACTIVE
Own power source
Broadcast range up to 100 meters
Ideal for material location
SWIPE TO PAY
PAID!
Operate at the same frequency (13.56 MHz) as HF RFID readers and tags
May act as both a reader and a tag
Devices must be in close proximity due to the short read range limitations of its radio frequency (usually no more than a few centimeters)
POPULAR USES:
INFORMATION SHARING
Transferring info between smartphones by tapping two devices together
CONTACTLESS PAYMENT
Credit cards, debit cards, key fobs and other devices use NFC to make secure payments
"There are 150 million NFC devices now.
BIG GAME
TAP FOR

Smart Things

Combination of measuring and acting through sensors, and micro-controller create a smart object

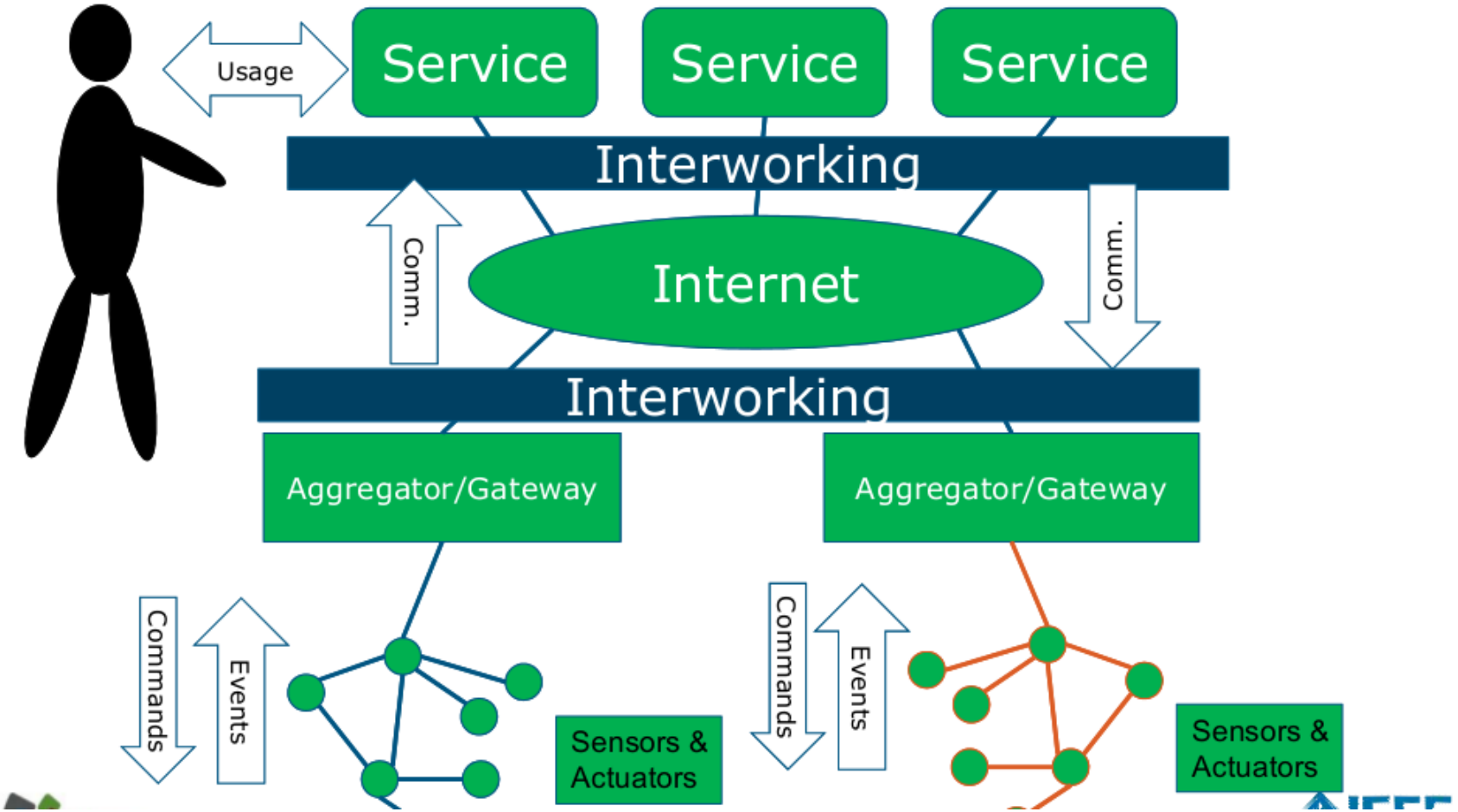
"A hw and sw system capable of making measures, execute rules, and subparts capable to execute tasks"

An IoT Application



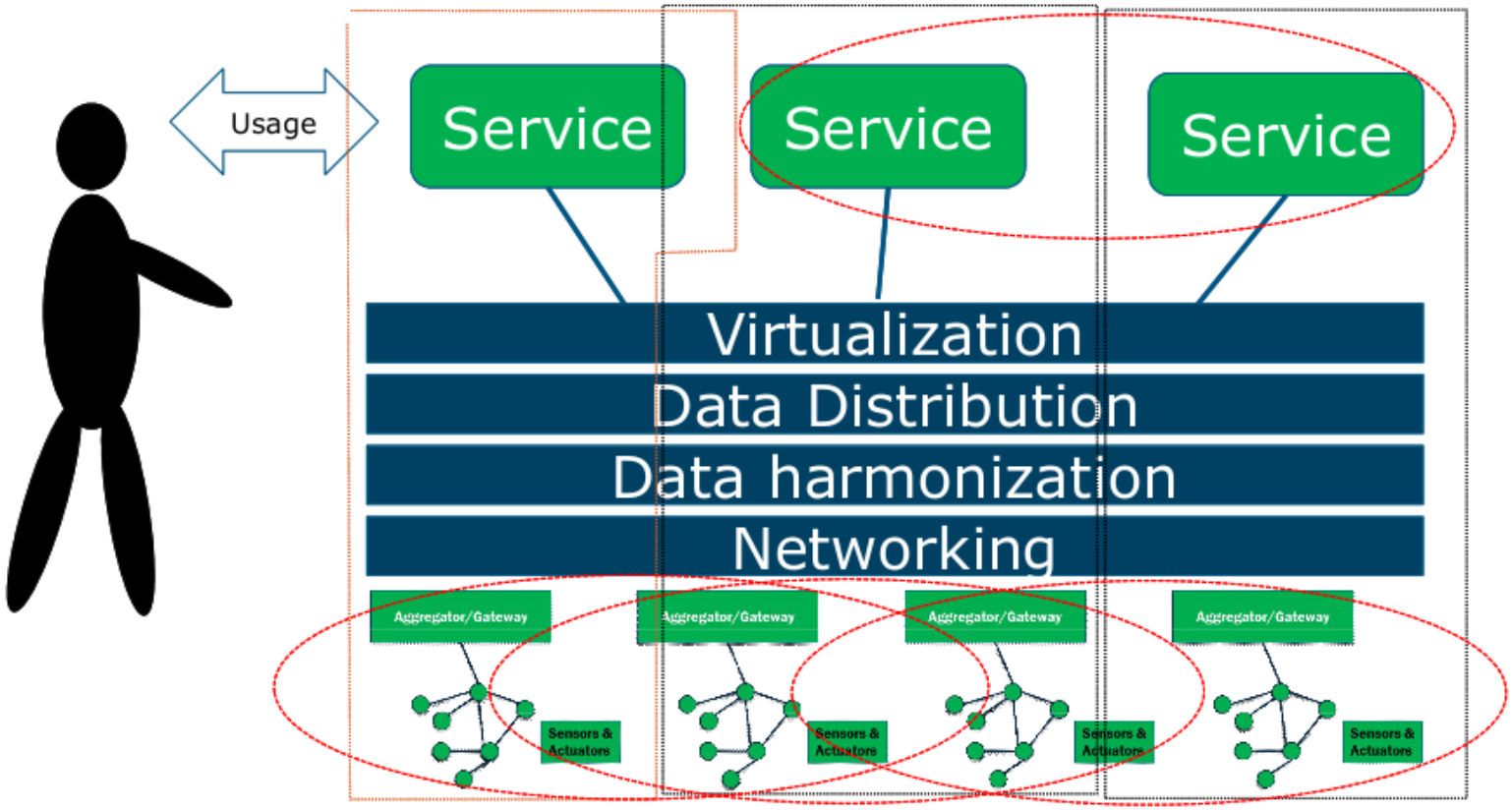
Source: IEEE Internet of Thing World Forum

An IoT Application



Source: IEEE Internet of Thing World Forum

An IoT Application



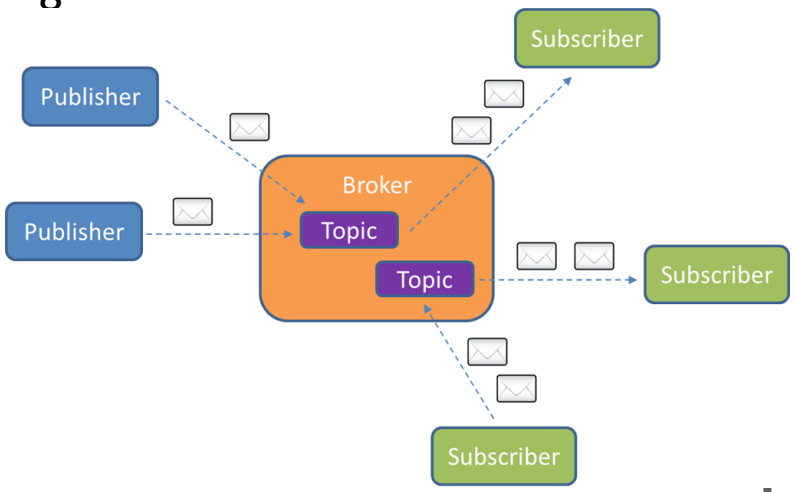
Source: IEEE Internet of Thing World Forum

We need a protocol!

- HTTP is not suitable for the internet of things
  - Has been created for verbose documents and lot of metadata
  - The client and server load is not adequate for micro-controllers
  - It does not provide guarantees of successful communication
  - The client / server model requires a polling interaction
  - Thousands of devices that do little = thousands of useless requests
  - Pollution cycles necessarily rarefied = poor reactivity to events
- Solution: protocols based on the PubSub model
  - Model asynchronous events
  - Semantic richness sacrificed in the name of lightness
  - Contrast to packet loss due to unreliable channels
  - Many solutions (MQTT, AMQP, XMPP, CoAP, DDS, STOMP, ...)

Publish / Subscribe (PubSub)

- Emphasis on messages
  - Published by a manufacturer
  - A consumer is notified
- The infrastructure (called the message broker or event bus) decouples the two types of actors and does not need to know them a priori, as
  - Producers manifest themselves by sending messages (events) identified by a topic (topic)
  - They manifest themselves by subscribing to a topic and receive the folders of new messages
- Disadvantages: requires a definition of the
- types of messages supported
- Ex: GUI, XMPP, MQTT, RSS, DDS



MQTT

- MQ (Message Queue) Telemetry Transport
  - Created by IBM / Eurotech in the 90s
  - Opened in 2010, OASIS standard since 2014
  - The official website: http://mqtt.org/
- Main features:
  - PubSub with transitional or permanent submissions to a topic
  - Topic can be organized into hierarchies
  - You can subscribe flexibly to parts of a topic
  - Three levels of service quality / delivery guarantee
  - Agnostic about the message content

MQTT – topics

- Example: Home environment track activity
  - [Building] / [plan] / [Environment] / [device]
  - corticella186 / PIANO1 / aulabiagi / light
- I can subscribe to a set of topics using wildcards
  - + → any value of a given element in the hierarchy
  - # → any combination of all the elements below
- Examples
  - All the lights of the building: corticella186 / + / + / light
  - All devices in a specific environment: corticella186 / floor1 / aulabiagi / +
  - All building devices: corticella186 / #

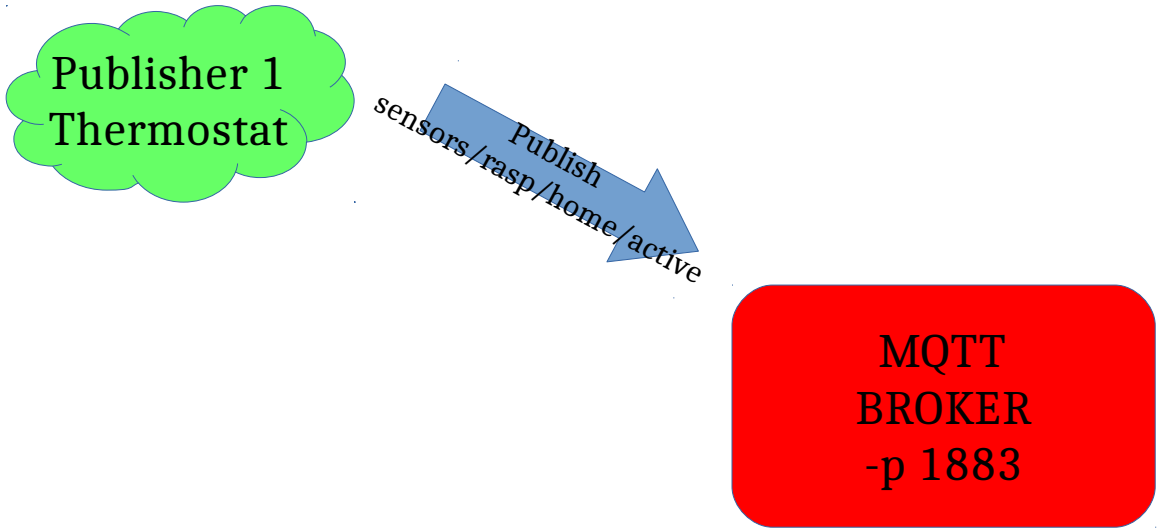
MQTT – PubSub

- Devices can communicate asynchronously and bidirectionally
  - They connect to a broker
  - They declare on what topic they intend to do PUBLISH
  - They declare which topics they are interested to do SUBSCRIBE
- The broker
  - Receive, store and notify events
    - It can provide the last valid message of a topic to a client who signs up, even after his arrival
  - Detects accidental disconnections of clients
    - If a client reconnects, all subscriptions are recovered
    - A client can indicate a “LWT”.

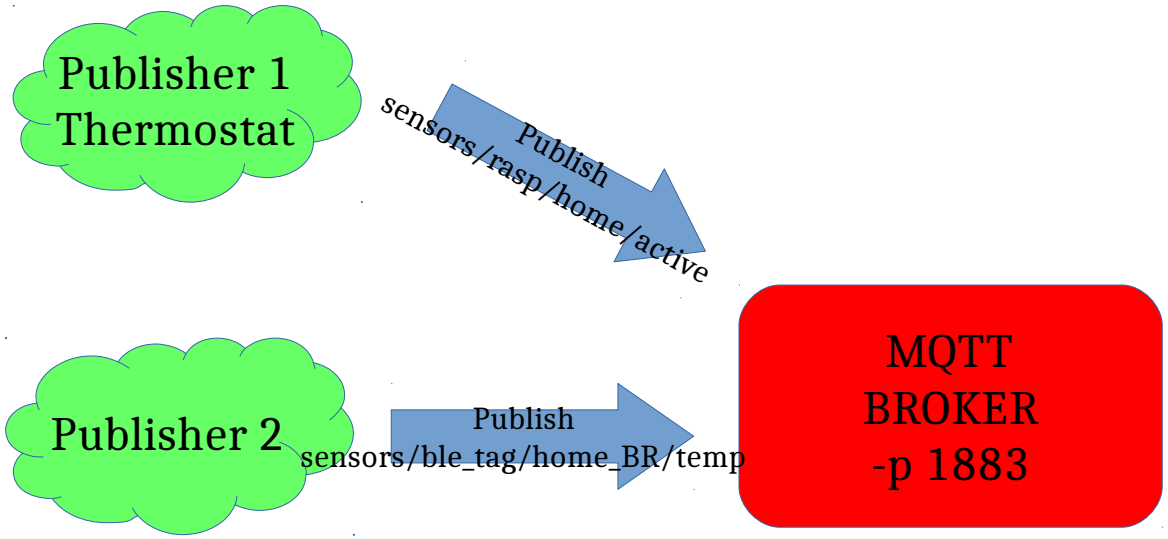
Publish / Subscribe (PubSub)

MQTT
BROKER
-p 1883

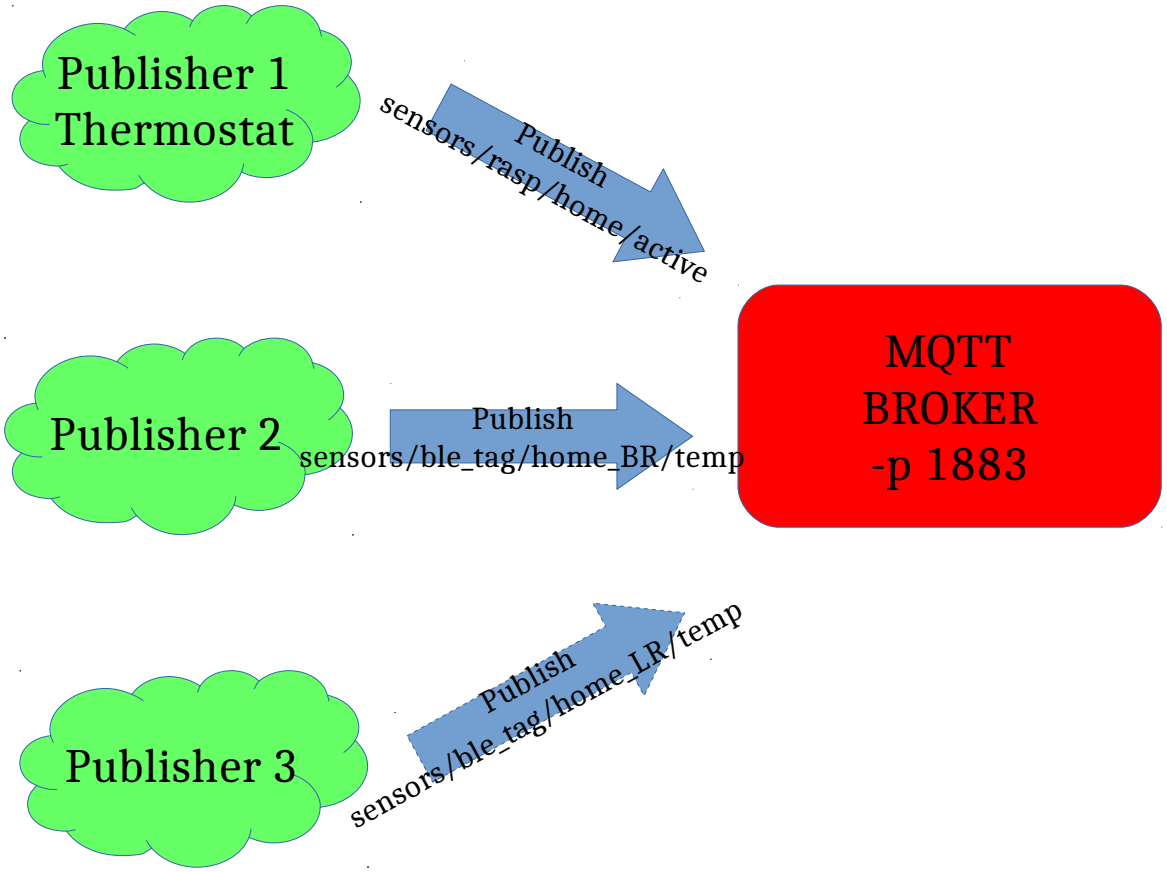
Publish / Subscribe (PubSub)



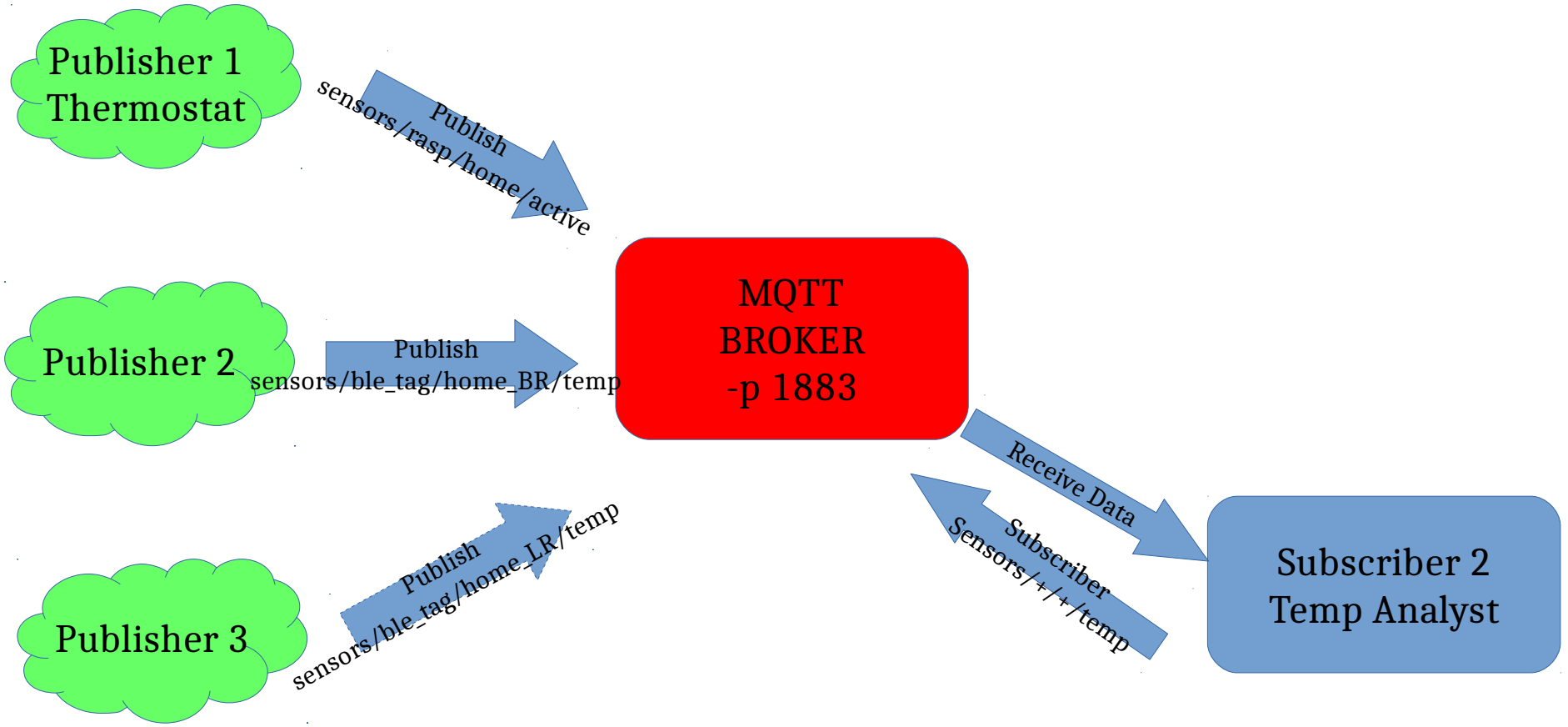
Publish / Subscribe (PubSub)



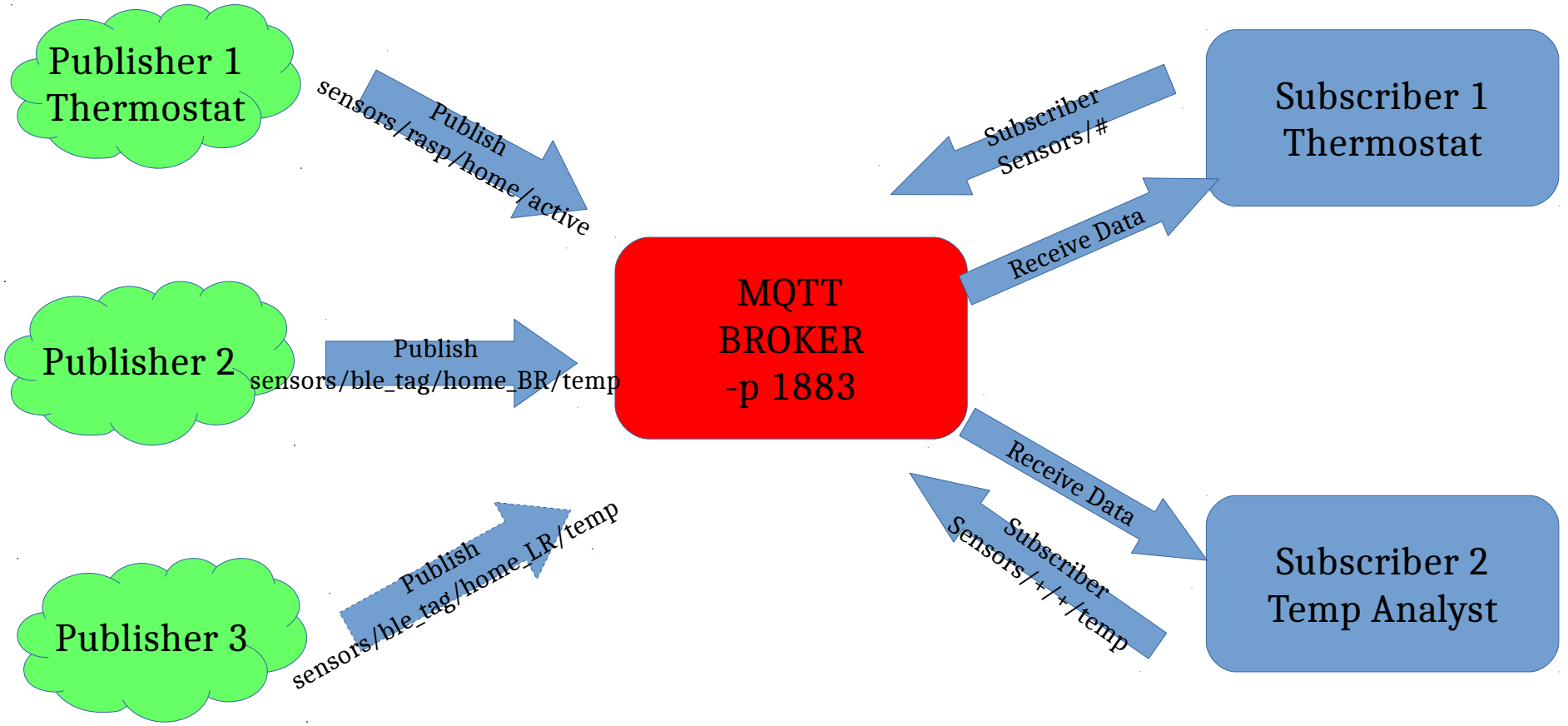
Publish / Subscribe (PubSub)



Publish / Subscribe (PubSub)

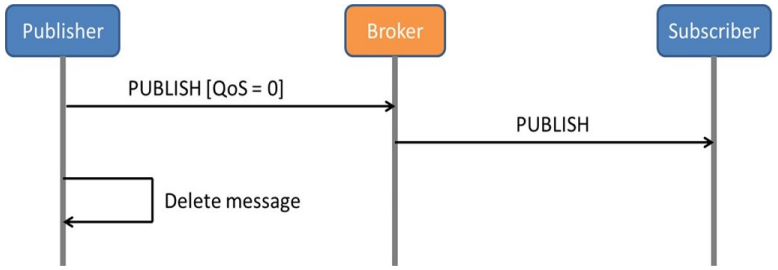


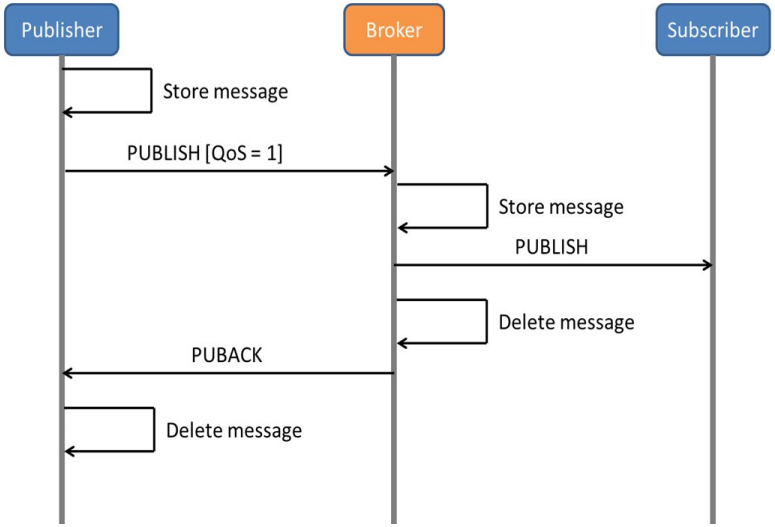
Publish / Subscribe (PubSub)

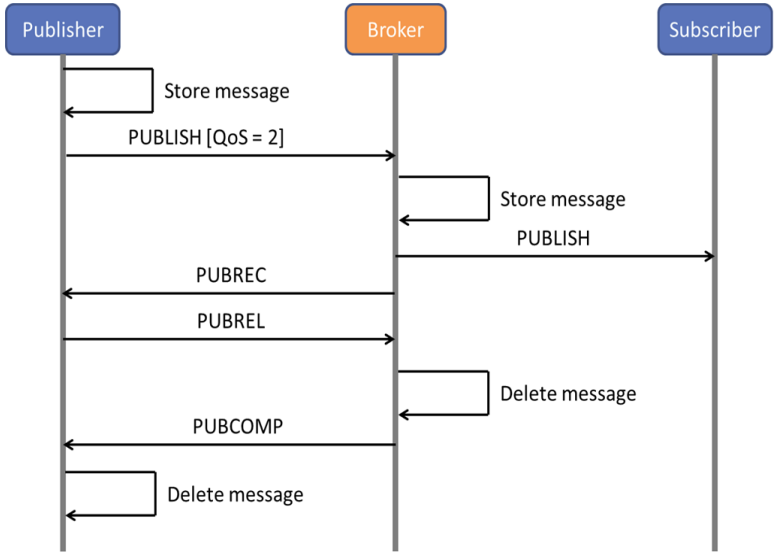


MQTT – QoS

- 3 possible levels:
  - 0 “at most once”
  - 1 “at least once”
  - 2 “exactly once”







MQTT Security

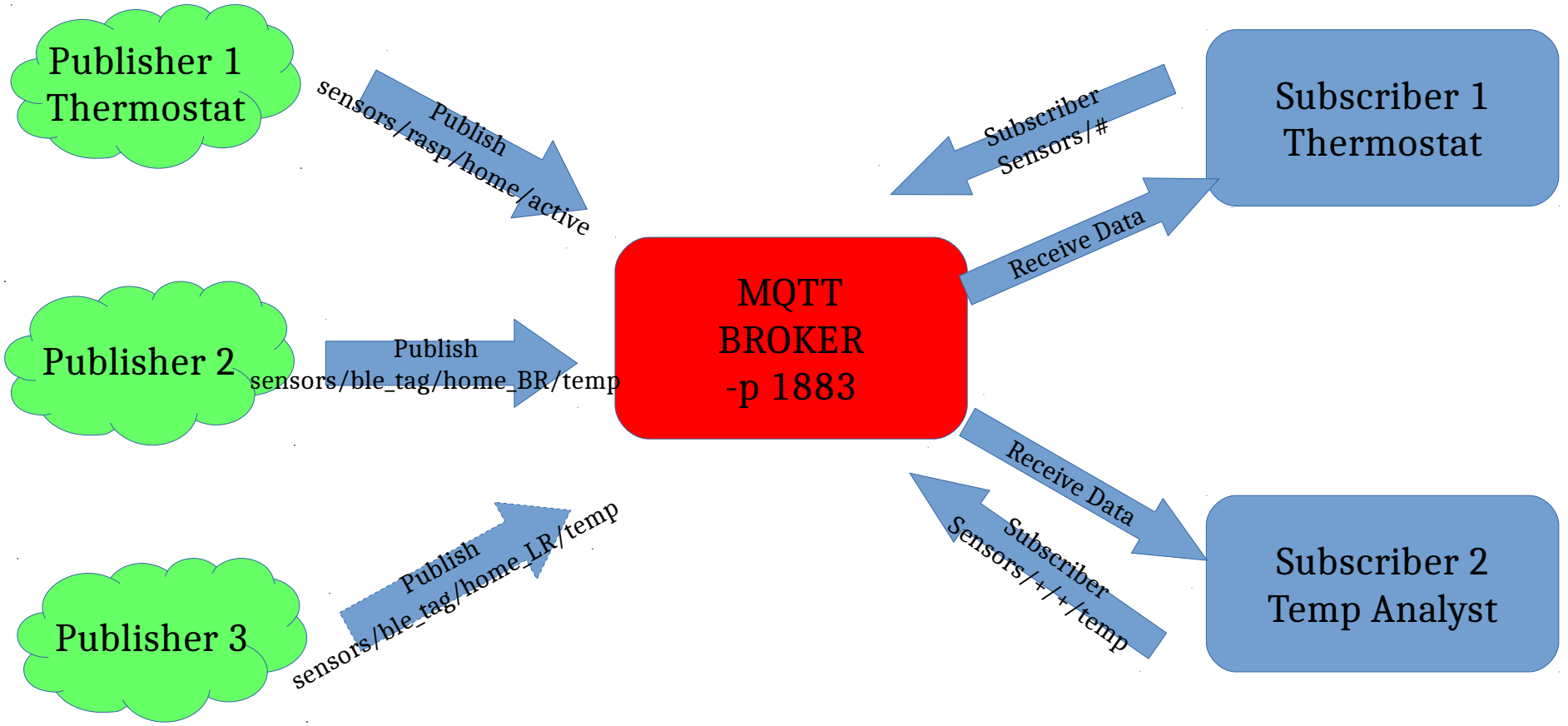
- By default nothing is enabled!
  - Username and password in CONNECT
    - Optional encryption of the payload
    - Transport
  - MQTT over TLS
    - Authentication with certificate x.509
    - Broker
      - Configurable permissions for PUBLISH and SUBCRIBE at the topic level
      - Integration with authentication and authorization systems such as OAuth

MQTT Security

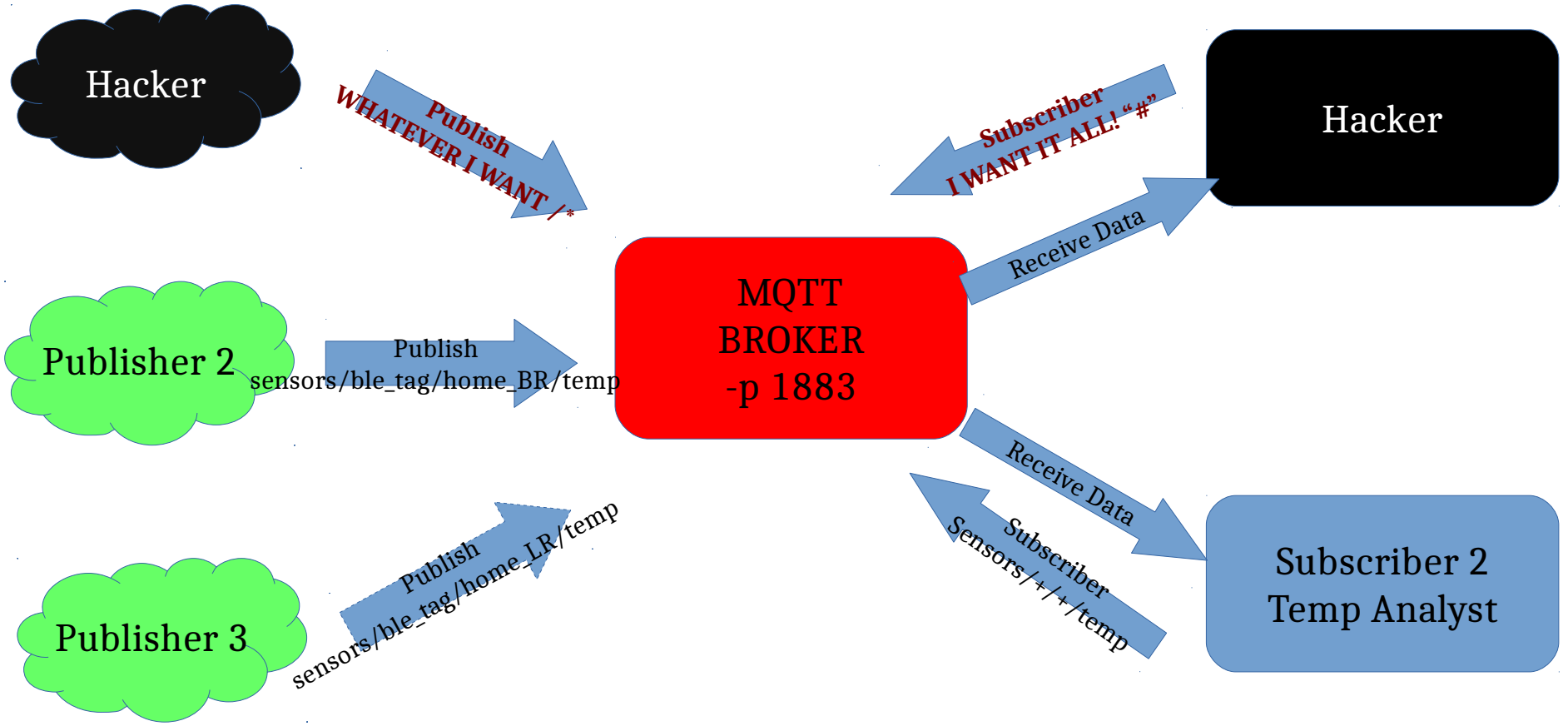
- By default nothing is enabled!
  - Username and password in CONNECT
    - Optional encryption of the payload
    - Transport
  - MQTT over TLS
    - Authentication with certificate x.509
    - Broker
      - Configurable permissions for PUBLISH and SUBCRIBE at the topic level
      - Integration with authentication and authorization systems such as OAuth

HINT: “ By default / Optional / Configurable” are the keys!

Publish / Subscribe (PubSub)



Publish / Subscribe (PubSub)



Classic BlueTooth

- The “conventional” Bluetooth
- 2.4GHz
- Range: 1m - 100m (10m typical)
- Connection-oriented: audio, file transfer, networking
- Reasonably fast data rate: 2.1 Mbps
- Power consumption:
- Not satisfied with < Wifi < 3G

BLE

- Introduced in Bluetooth 4.0 specification (2010)
  - Also known as Bluetooth SMART
- Target applications
  - Wireless battery-powered sensors eg. heart rate, thermometer, fitness
  - Location tracking and information serving eg. iBeacons
- Requirements for target applications
  - Low-power
  - Low-cost
  - Low bandwidth: ~100 kbps
  - Low latency: Connectionless (fast setup and teardown of connection in ~10ms)
- How?
  - Radio chip off most of the time
  - Small packets
  - MTU: 20 bytes/packet for application
  - Less time transmitting -> less heat -> no need compensatory circuits -> save more power

BLE Devices


POLAR
Ray Maker
Activity
Training summary
Info
Settings
Sign out


Smart Electronic
Padlock


You'll Always Know with the World's First CGM on the Phone
110
mg/dL


UBER
5 min
Work
$12.60
Get a ride
sevenhugs
sevenhugs
sevenhugs

BLE Security

- Uses AES-128 with CCM encryption engine
- Uses Key Distribution to share various keys
  - Identity Resolving Key is used for privacy
  - Signing Resolving Key provides fast authentication without encryption
  - Long Term Key is used
- Pairing encrypts the link using a Temporary Key (TK)
  - Derived from passkey
  - Then distribute keys
- Asymmetric key model
  - Slave gives keys to master with a diversifier
  - Slave can then recover keys from the diversifier

For more info:
https://www.bluetooth.com/~/media/files/specification/bluetooth-low-energy-security.ashx

BLE Pairing: How To?

- Just Works
  - Legacy, most common
  - Devices without display cannot implement other
  - Its actually a key of zero, that's why it just works...
- 6-digit PIN
  - In case the device has a display
- Out of band (OOB)
  - Does not share secret key over the 2.4 GHz band (used by protocol)
  - Makes use of other mediums (e.g. NFC)
  - Once secret keys are exchanged, encrypts the channel

"None of the pairing methods provide protection against a passive eavesdropper" -Bluetooth Core Spec!

BLE Pairing, there is even more!

- In practice, ~80% of common devices do not implement BLE-layer encryption (Source: AppSec Labs, OWASP 2017 Report!)

- Why?
  - As always, security is left behind (cost, time, etc.)
  - Multiple users/apps using the same devices
  - Access sharing
  - Backups to the cloud
  - Public access devices (e.g. cash register)
  - Hardware, software or even UX compatibilities/requirements

BLE Pairing, there is even more!

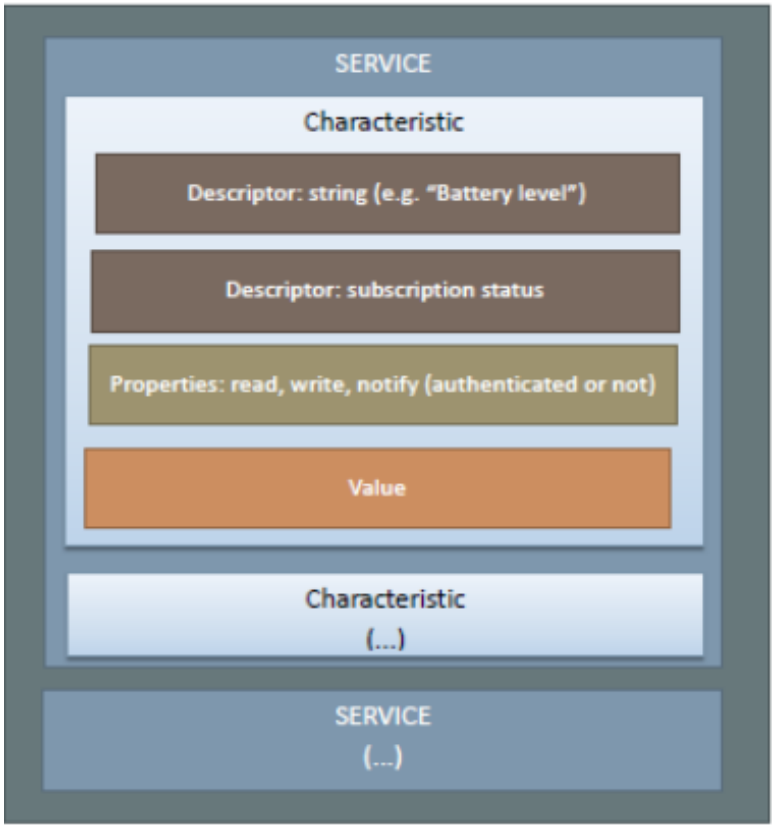
- In practice, ~80% of common devices do not implement BLE-layer encryption (Source: AppSec Labs, OWASP 2017 Report!)

- Why?
  - As always, security is left behind (cost, time, etc.)
  - Multiple users/apps using the same devices
  - Access sharing
  - Backups to the cloud
  - Public access devices (e.g. cash register)
  - Hardware, software or even UX compatibilities/requirements

BLE: GATT

BLE Model

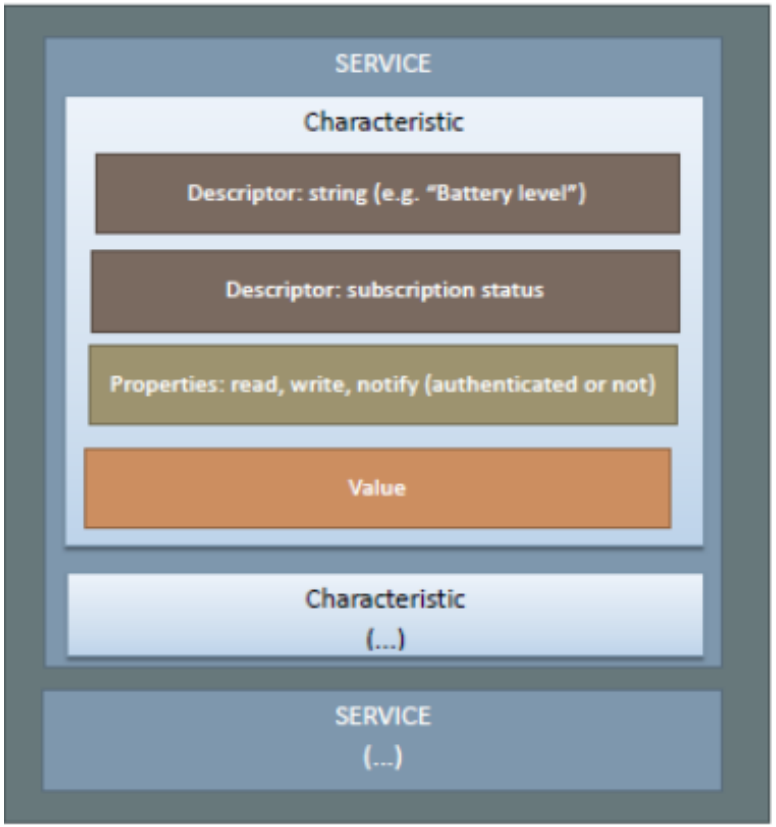
- Generic Attribute Profile (GATT) used by BLE to communicate with each other
- Services and characteristic are identified by an associated UUID
- A characteristic contains a single value (“attribute”)
- Can be read, written to or subscribed for notifications



BLE: GATT

BLE Model

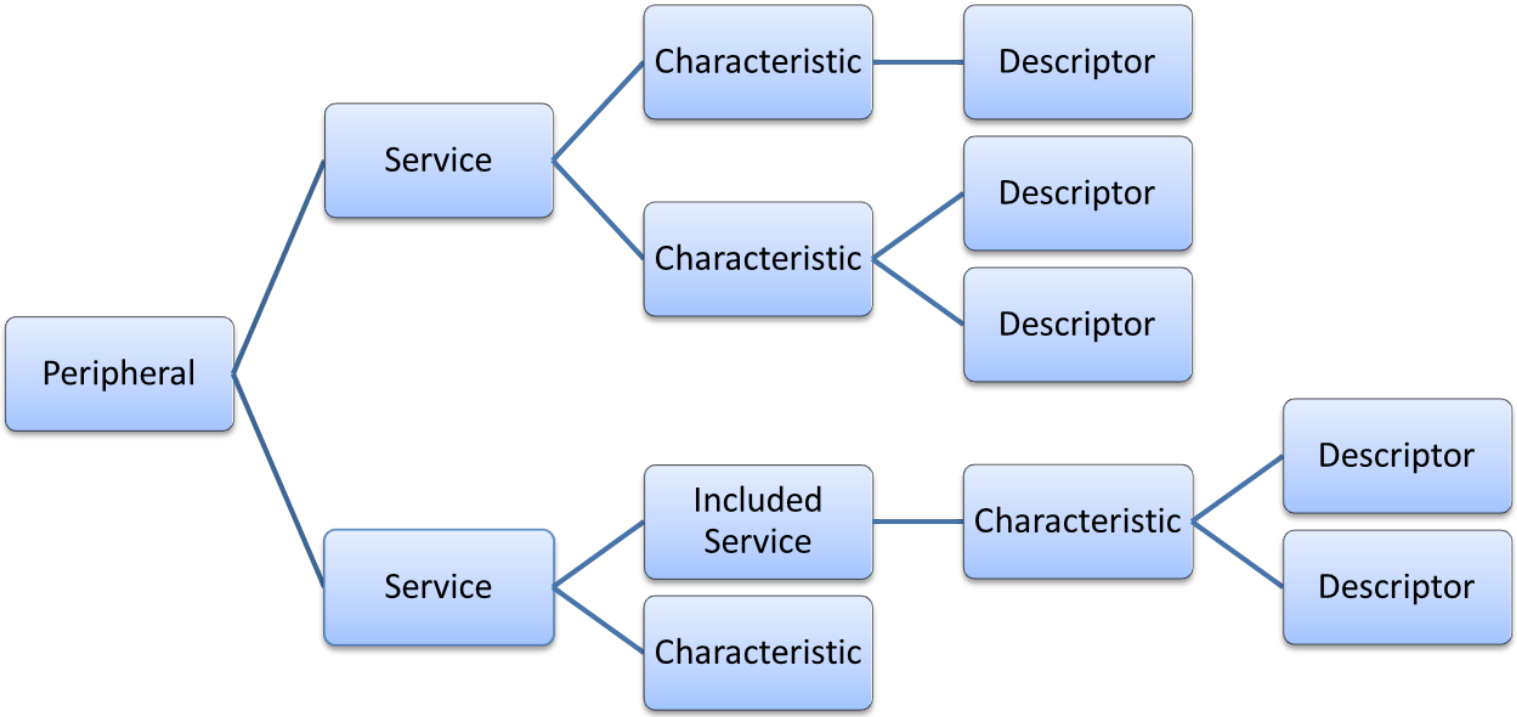
- Generic Attribute Profile (GATT) used by BLE to communicate with each other
- Services and characteristic are identified by an associated UUID
- A characteristic contains a single value (“attribute”)
- Can be read, written to or subscribed for notifications



Those Attribute are “broadcasted” continuously by the device!!

(Source: AppSec Labs, OWASP 2017 Report)

BLE Model


Peripheral
Service
Characteristic
Descriptor
Characteristic
Descriptor
Descriptor
Service
Included Service
Characteristic
Descriptor
Descriptor
Characteristic

BLE Attack Quick Look

```
a8:66:7f:3c:41:38 (-75 dBm)
Vendor                | Apple
Allows Connections    | ✓
Flags                 | LE General Discoverable, BR/EDR
Manufacturer          | u'4c0010020700'

@ Connecting to a8:66:7f:3c:41:38 ... connected.
@ Enumerating all the things .....
```

Handles	Service > Characteristics	Properties	Data
0001 -> 0005	Generic Access (00001800-0000-1000-8000-00805f9b34fb)		
0003	Device Name (00002a00-0000-1000-8000-00805f9b34fb)	READ	u'Alessandro\u2019s MacBook Air'
0005	Appearance (00002a01-0000-1000-8000-00805f9b34fb)	READ	Generic Computer
0006 -> 0009	Generic Attribute (00001801-0000-1000-8000-00805f9b34fb)		
0008	Service Changed (00002a05-0000-1000-8000-00805f9b34fb)	READ INDICATE	
0010 -> 0014	Device Information (0000180a-0000-1000-8000-00805f9b34fb)		
0012	Manufacturer Name String (00002a29-0000-1000-8000-00805f9b34fb)	READ	u'Apple Inc'
0014	Model Number String (00002a24-0000-1000-8000-00805f9b34fb)	READ	u'MacBook9,1'
0020 -> 0023	Apple Continuity Service (d0611e78-bbb4-4591-a5f8-487910ae4366)		
0022	8667556c-9a37-4c91-84ed-54ee27d90049	NOTIFY WRITE	
0024 -> 0027	9fa480e0-4967-4542-9390-d343dc5d04ae		
0026	af0badb1-5b99-43cd-917a-a77bc549e3cc	NOTIFY WRITE	

```
demuro89@demuro89:~$ sudo bleah -e "a8:66:7f:3c:41:38" -u "af0badb1-5b99-43cd-917a-a77bc549e3cc" -d "Passa in netlab"
```

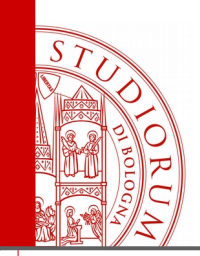
The applications “talks” to device's “attributes” using Bluetooth LE GATT (Generic Attribute Profile) specification . Without any security features enabled they introduce a lot of serious attack vectors.

BLE Attack Quick Look

- Attacks on advertisements
  - The attacker clones the advertisement and broadcasts (without forwarding to the real device)
  - The device will try to connect and fail

- Attacks on exposed services
  - If the device offers services possible to access without authentication
    - BF-ing (e.g. guessing the password)
    - Fuzzing (Sending improper values to characteristics)
    - Logic vulnerabilities

- Attacks on Parining
  - “Just work” – just hacked
    - Access protected characteristic
    - Use for MitM
  - PIN-protected Pairing
    - Trick the user into re-initiation of the pairing
      - Jamming, cloning, etc



Agenda

- Information Gathering
  - History and Definition
  - The context
  - My Definition
  - Motivations
- Service Disclosure
  - What's a Thing?
  - Technologies Involved
  - Hardware (Rasp, Arduino, Sensors,..)
  - Software (MQTT, Blue*,ZigBee, ..)
- Exploits
  - Attack Surface
  - 10 OWASP
  - Real Attacks
- Defense
  - Demos
  - Conclusion.