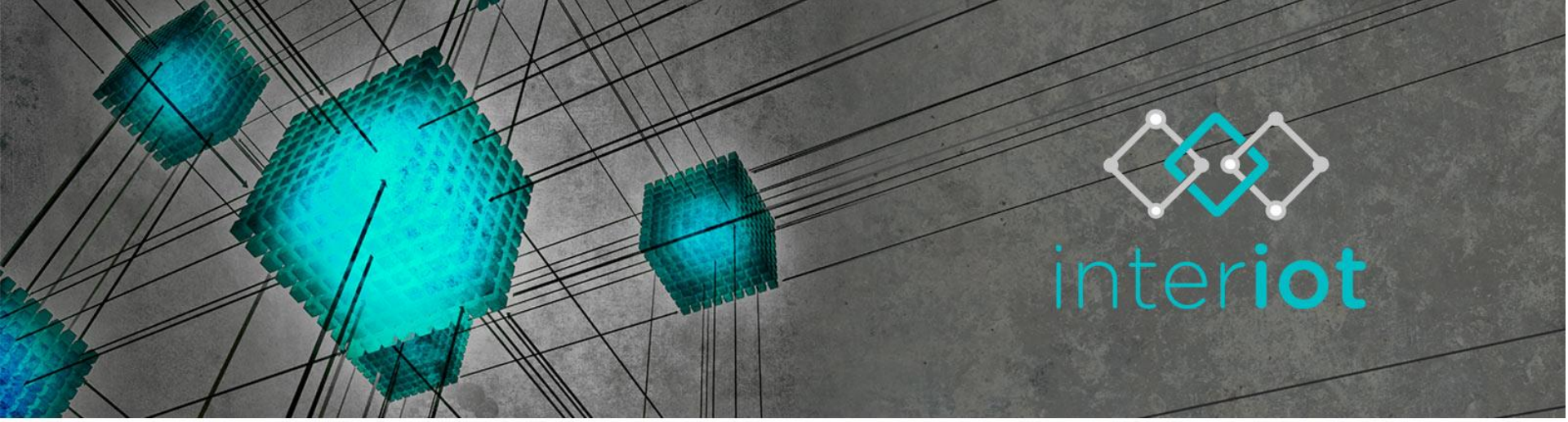


Internet of secure things: issues and perspectives

Pasquale Pace
Dimes - UNICAL
ppace@dimes.unical.it

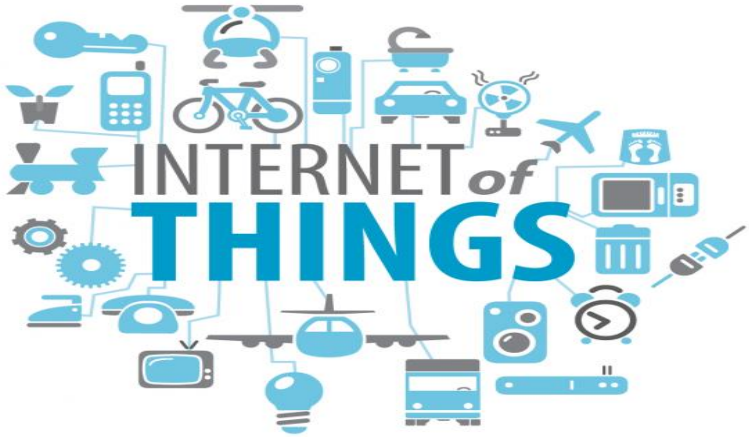


Table of Contents:

- Inter-IoT European Project
» http://www.inter-iot-project.eu/

- IoT Security
  - IoT Authentication
  - IoT & Blockchain

INTER-IoT Vision and Mission

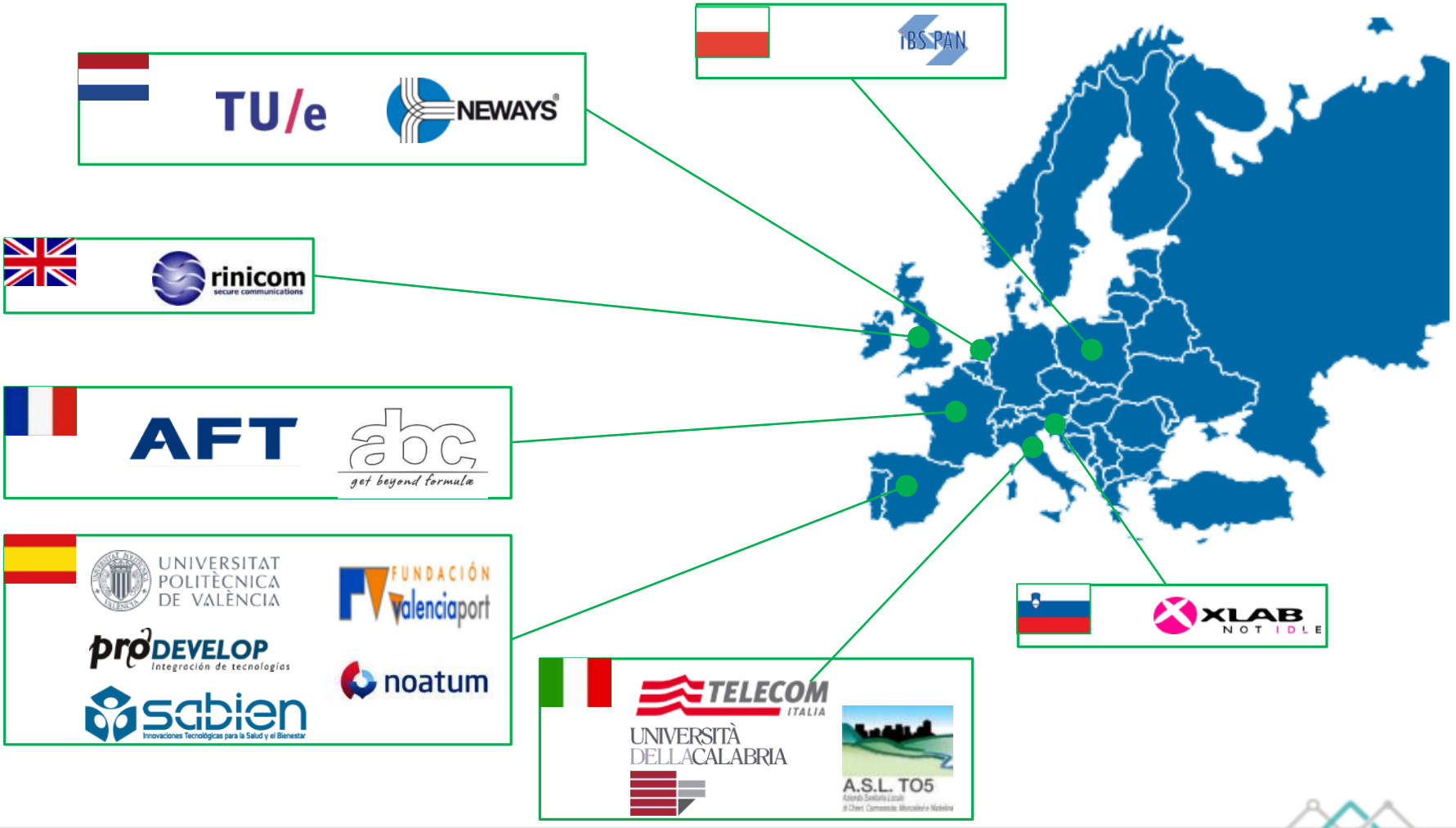
INTER-IoT *vision is to provide all the building blocks needed to achieve interoperability between IoT Platforms, including a framework, methodology, associated APIs and tools.*

By building and demonstrating:

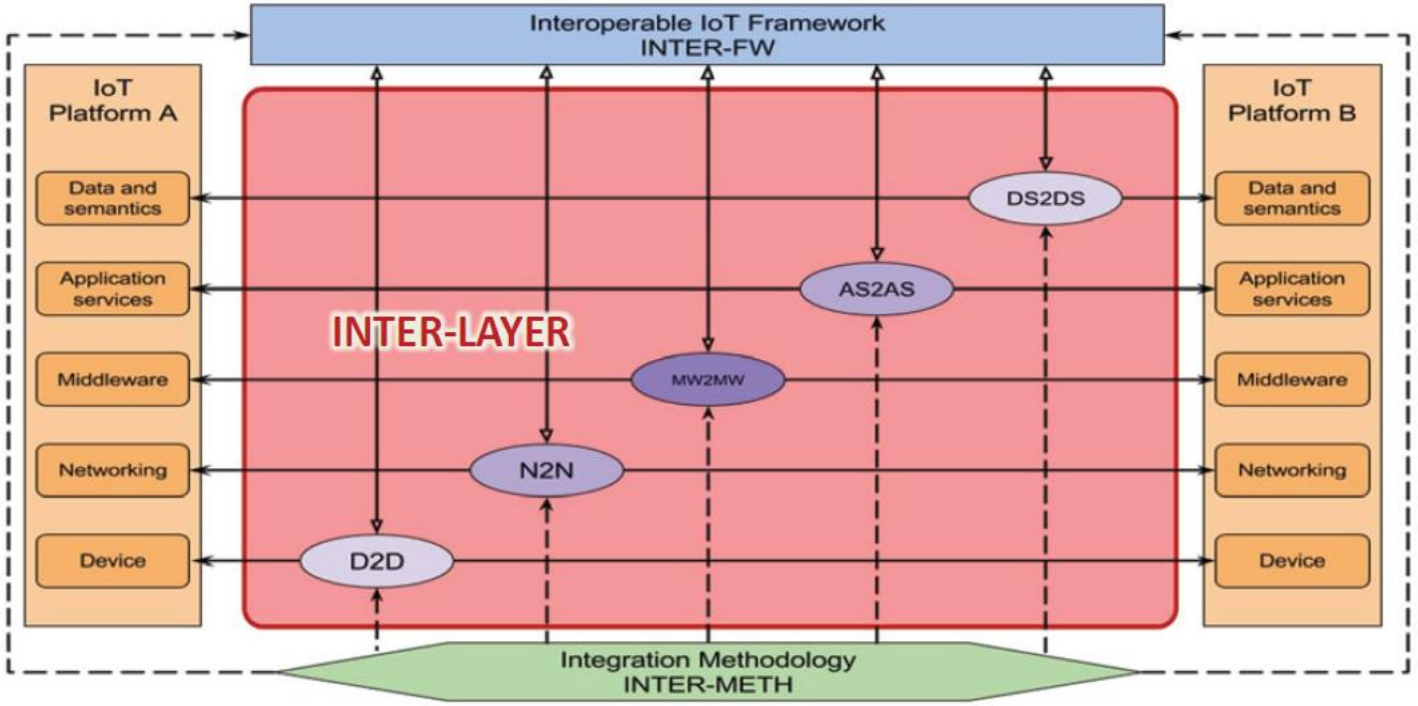
- Seamless inclusion of novel IoT devices
- Seamless support for smart objects mobility
- Service discovery and management
- Reuse and exchange of services between IoT platforms
- Common semantic interpretation of data
- Rapid prototyping of cross-platform IoT applications
- Overcome market barriers

- http://www.inter-iot-project.eu/

INTER-IoT Consortium

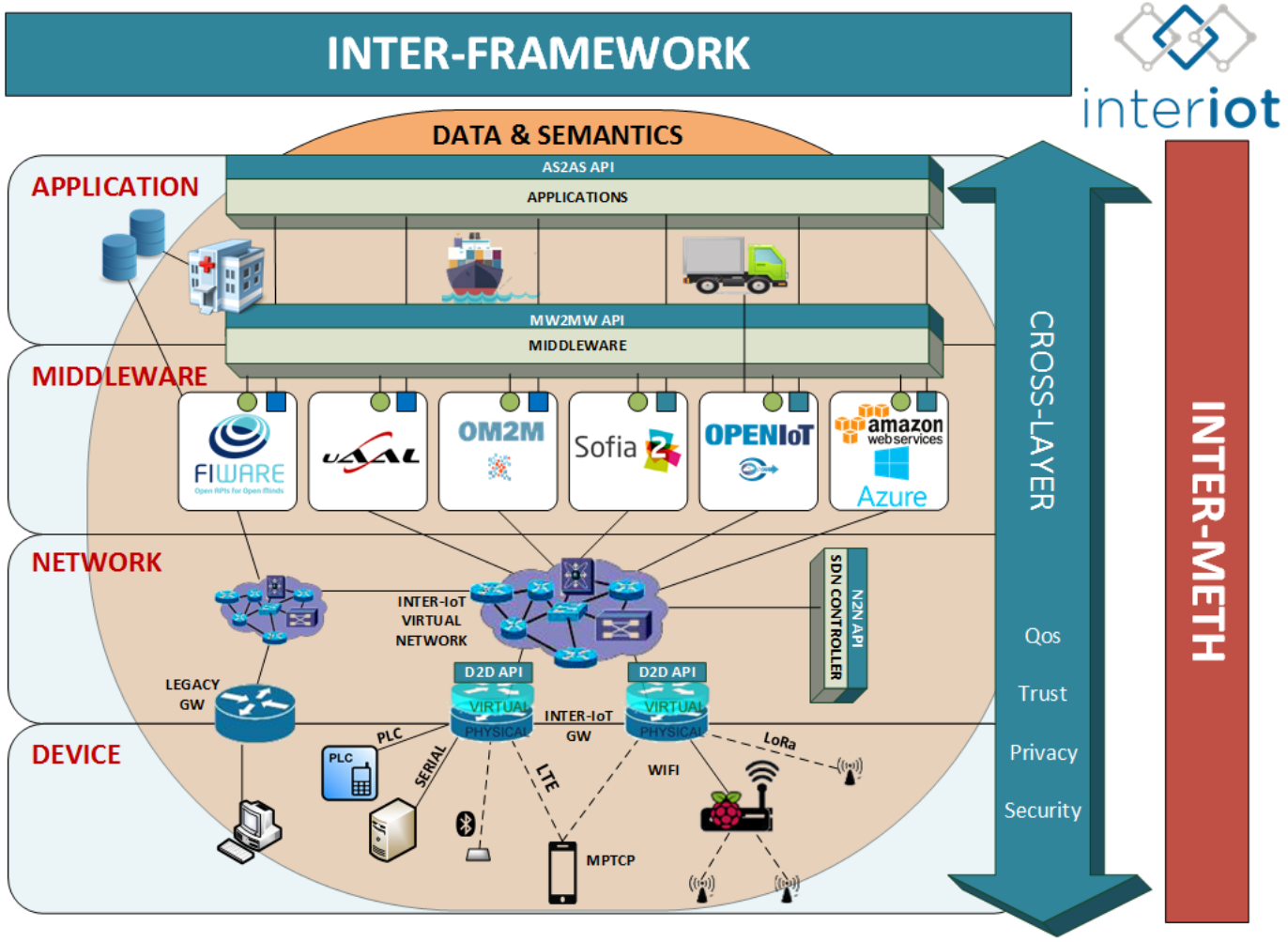


INTER-IoT architecture

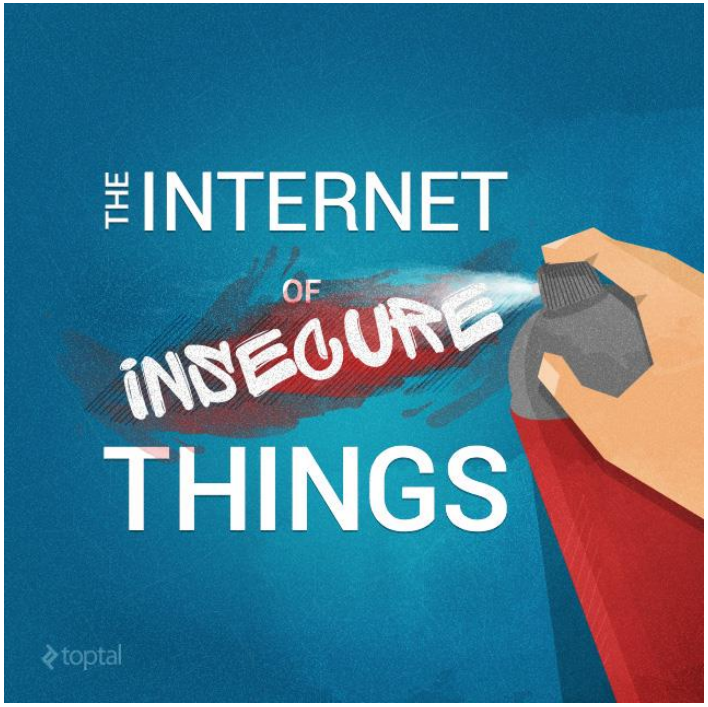


- The INTER-LAYER tools will provide techniques and technology allowing interoperability and integration between the layers of heterogeneous IoT platforms

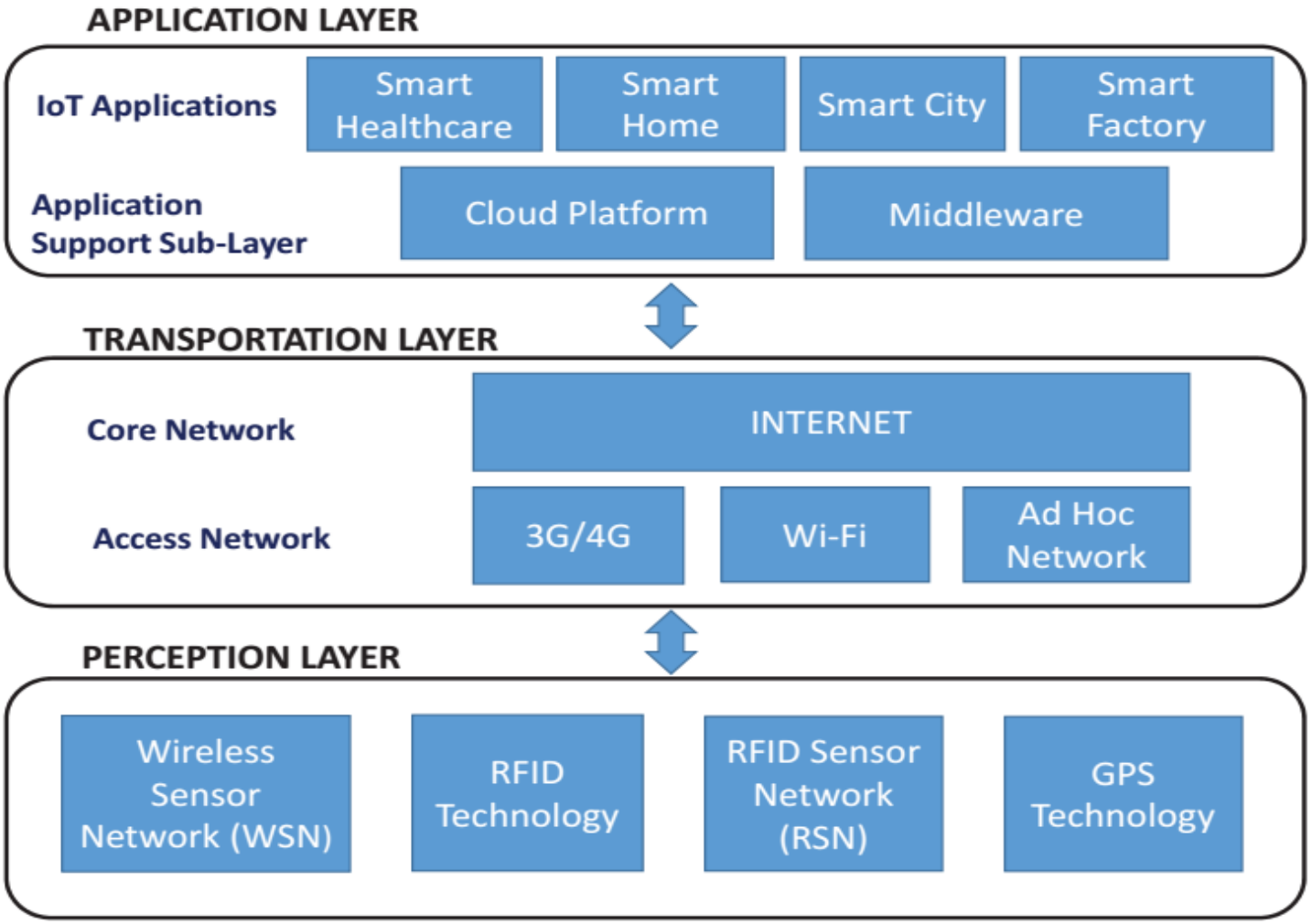
INTER-LAYER


INTER-FRAMEWORK
interiot
DATA & SEMANTICS
APPLICATION
AS2AS API
APPLICATIONS
MW2MW API
MIDDLEWARE
MIDDLEWARE
FIWARE
OM2M
Sofia 2
OPENIoT
amazon web services
Azure
NETWORK
INTER-IoT VIRTUAL NETWORK
SDN CONTROLLER
N2N API
LEGACY GW
D2D API
VIRTUAL
PHYSICAL
INTER-IoT GW
DEVICE
PLC
SERIAL
LTE
WIFI
LoRa
MPTCP
CROSS-LAYER
Qos
Trust
Privacy
Security
INTER-METH

IoT Security



IoT System Model

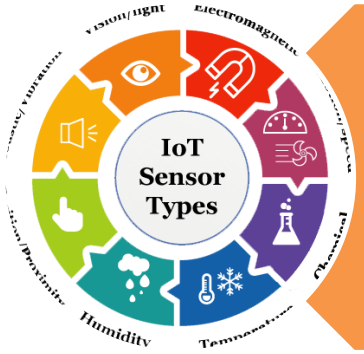


Application Layer

- Large users Accessibility
- Some Critical Applications
- Tested security methods

Transportation Layer

- Heterogeneous networks
- Intensive research about vulnerabilities



Perception Layer

- Physical Exposure
- Resource- constrained devices
- Technological heterogeneity

Vulnerable

Traditional IT Security vs IoT Security

Traditional IT Security	IoT Security
Add-on Security	Built-in Security
Complex algorithms	Lightweight algorithms for resource-constrained devices
User Control	Privacy issue: IoT devices often automatically collect user information
Small technological heterogeneity	Large technological heterogeneity (thus also large attack surface)
Many security guards	Few security guards
Devices are placed in closed environments	IoT devices are placed in both open and closed environments

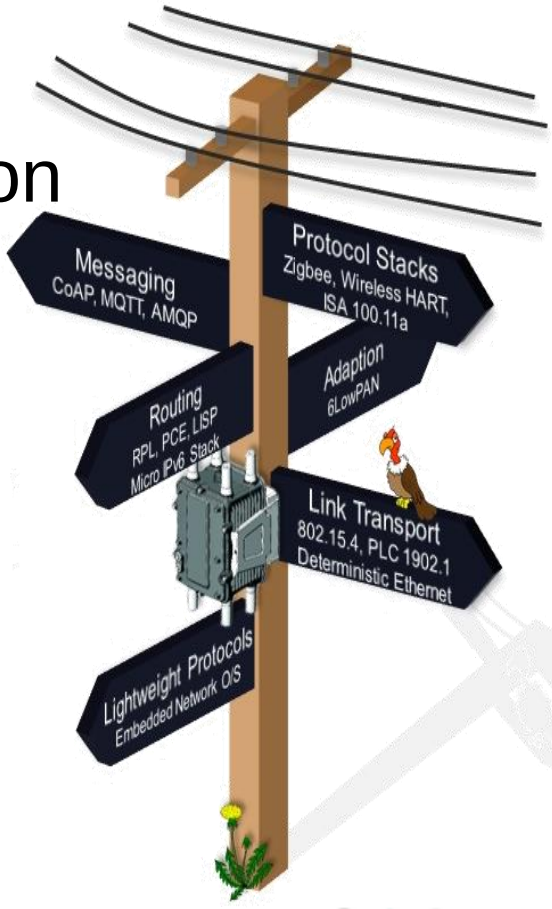
IoT Security as a «*chain*»

- IoT system as a whole system and security can be thought of as a *chain* that is robust as much as its weakest link.

Multi & Cross Layer Security

IoT Communication Protocols

- To design IoT security solutions for cross layers usage you have to overcome *heterogeneous* integration issues.



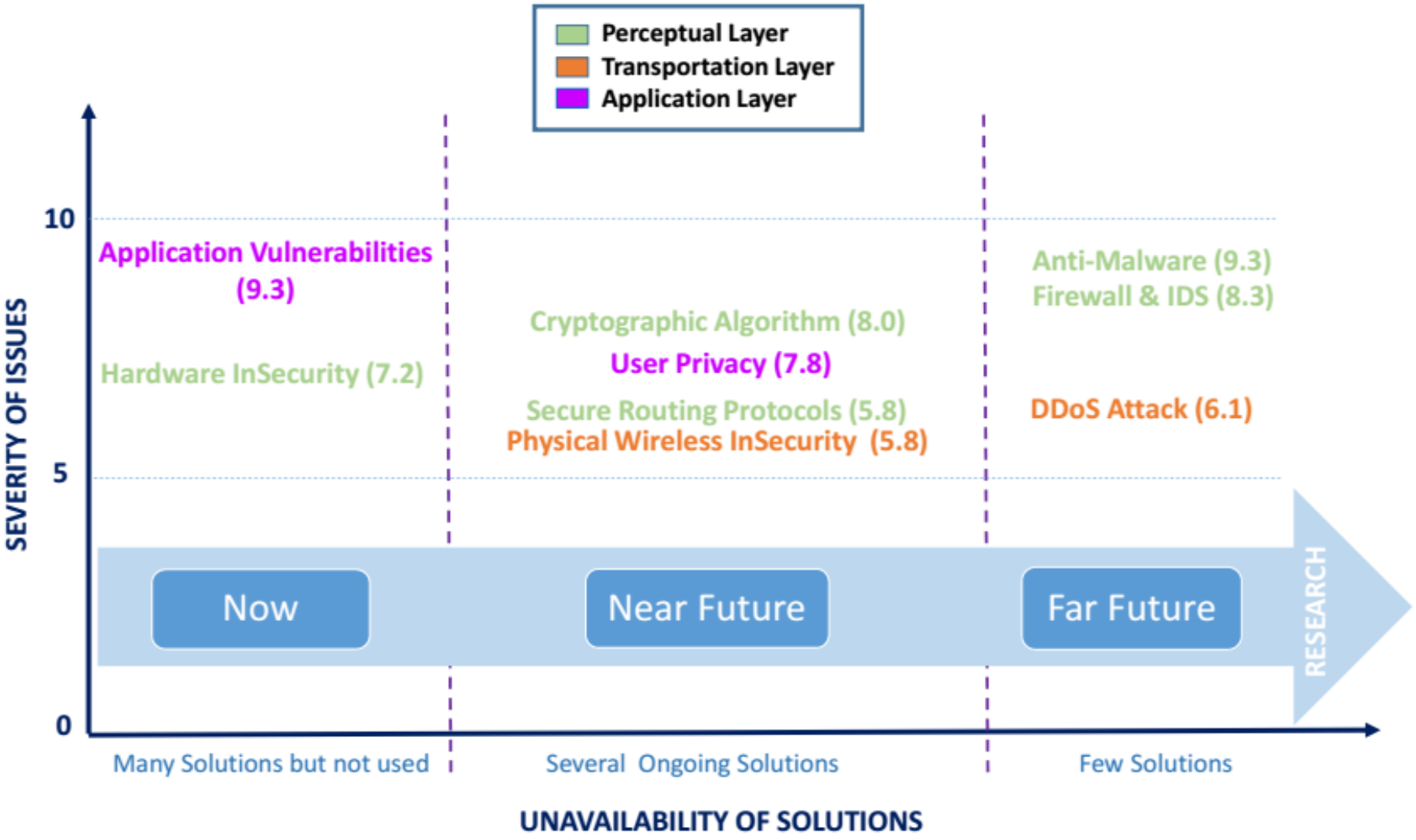
Interoperability
become one of the enabling factors for IoT security.

Critical Security Issues evaluation

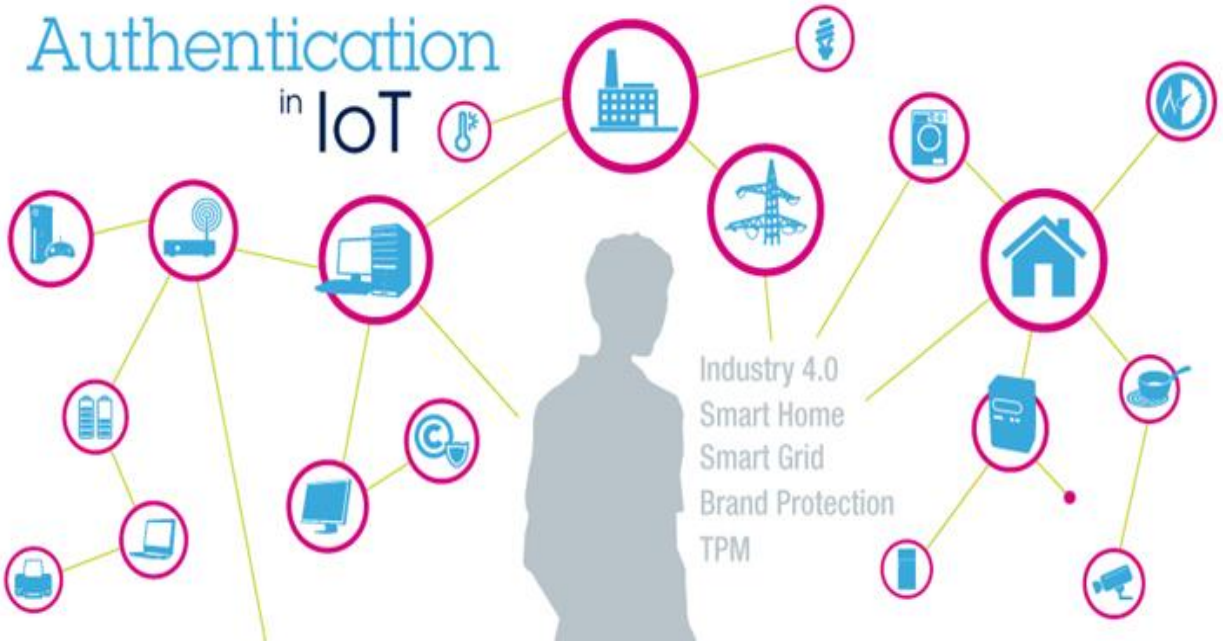
- Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

- Using CVSS to evaluate some IoT critical security issues.
  - CVSS, https://en.wikipedia.org/wiki/CVSS.
  - CVSSv2, https://www.first.org/cvss/v2/guide

Research Direction



IoT Authentication

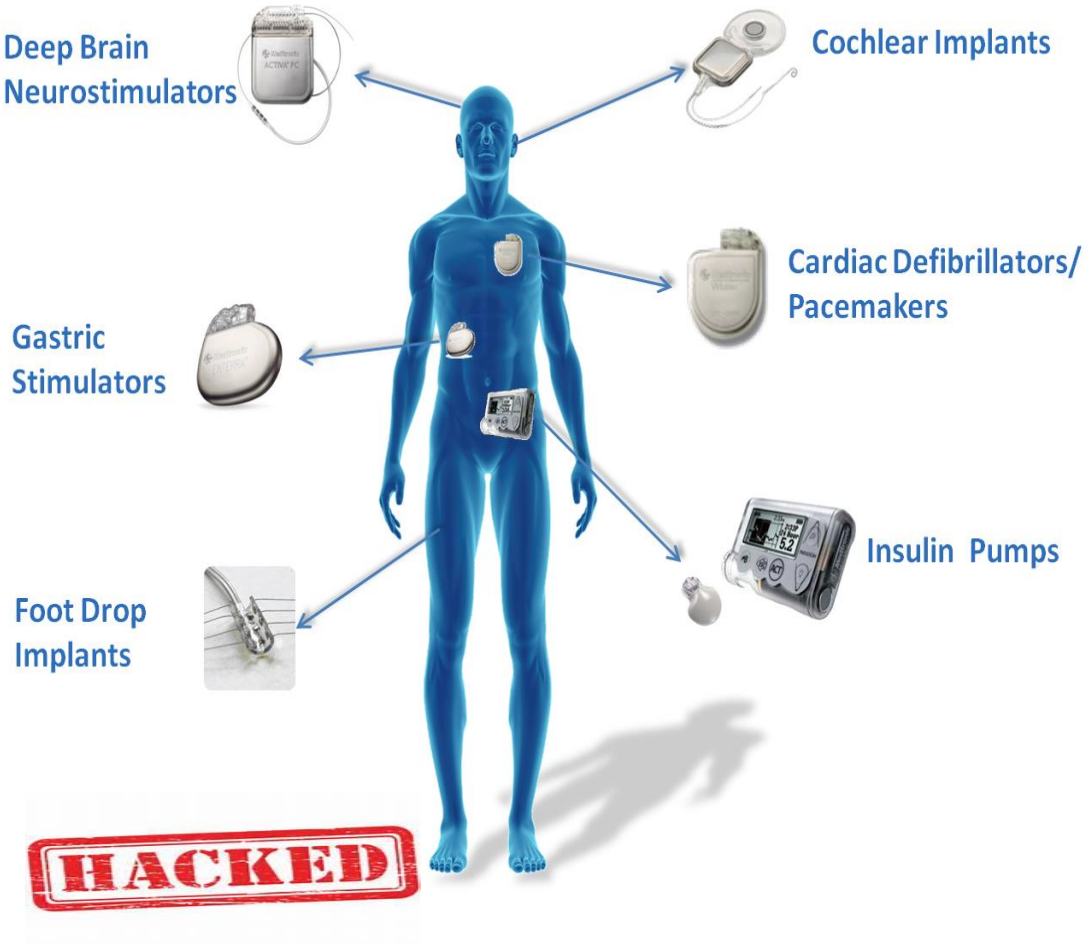


Top 10 IoT Vulnerabilities (OWASP) Open Web Application Security Project

Top 10 IoT Vulnerabilities Project The OWASP Top 10 IoT Vulnerabilities are as follows:	
Rank	Title
I1	•Insecure Web Interface
I2	•Insufficient Authentication/Authorization
I3	•Insecure Network Services
I4	•Lack of Transport Encryption/Integrity Verification
I5	•Privacy Concerns
I6	•Insecure Cloud Interface
I7	•Insecure Mobile Interface
I8	•Insufficient Security Configurability
I9	•Insecure Software/Firmware
I10	•Poor Physical Security

- 10/10 security systems accept '123456'
- 10/10 security systems with no lockout
- 10/10 security systems with enumeration
- SSH listeners with root/"" access
- 6/10 web interfaces with XSS/SQLi
- 70% of devices not using encryption
- 8/10 collected personal information
- 9/10 had no two-factor options
- Unauthenticated video streaming
- Completely flawed software update systems

WIRELESS IMPLANTABLE MEDICAL DEVICES



IoT Device Authentication

Authentication Factors	Description
Something the device *knows*	credential (device key, e.g., a secret key or a private key)
Something the device *has*	integrated authentication IC, authentication dongle
Something the device *is*	logical properties (e.g. the device type); physical properties: device fingerprint

"Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things" (*Rainer Falk and Steffen Fries*) . CYBER 2016

IoT Device Authentication

Unconventional Authentication Factors	Description
Something the device *knows about its environment*	Sensing informations
Something the device *does*	behavior, functionality, e.g., automation control protocol
The context of the device	neighbors, location, connected periphery

"Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things" (*Rainer Falk and Steffen Fries*) . CYBER 2016

IoT & Blockchain

Advantages of Blockchain:

- It is *public*: everyone participating can see the blocks and the transactions stored
- It is *decentralized*: there is no single authority that can approve the transactions
  - (the participants in the network have to reach a consensus to accept transactions)
- It is *secure*: it uses public-key cryptography and it is tamper-proof
  - the ledger cannot be manipulated by malicious actors because it doesn't exist in any single location, and man in the middle attacks cannot be staged because there is no single thread of communication that can be intercepted

Blockchain & IoT

- To enable message exchanges, devices will leverage ***smart contracts*** which then model the agreement between the two parties.

- *True autonomous smart device* without also the need of human intervention
  - smart devices in a manufacturing plant that can place orders for repairing some of its parts without the need of human or centralized intervention
  - smart vehicles in a truck fleet will be able to provide a complete report of the most important parts needing replacement after arriving at a workshop

Main challanges

- Resource-constrained devices
- Large technological heterogeneity

The utility of an ***IoT Gateway***

“A Mobile Multi-Technology Gateway to Enable IoT Interoperability”