UNIVERSITÀ DI PARMA
Dipartimento di Ingegneria e Architettura

IoT Security

Luca Veltri

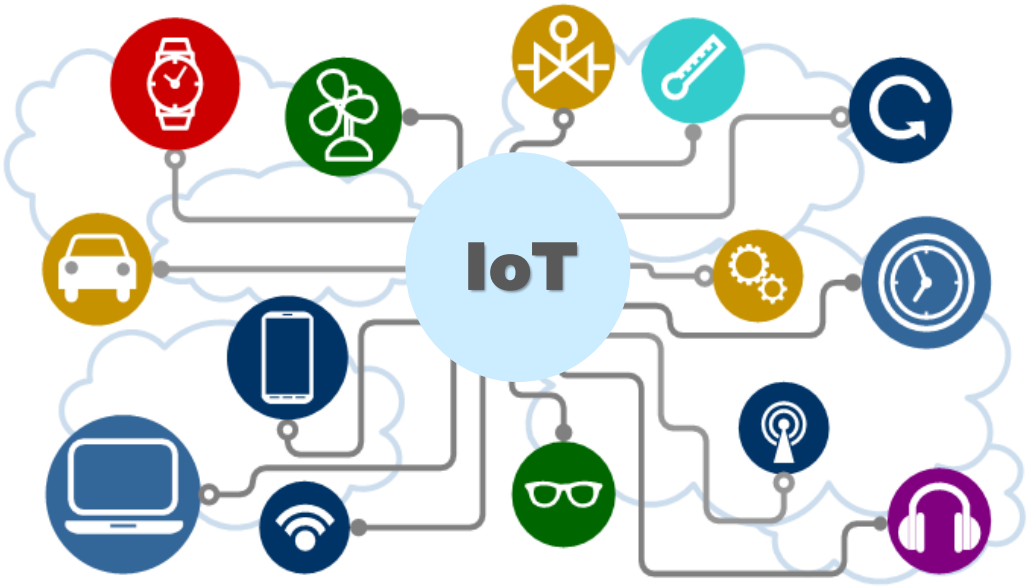
(mail.to: luca.veltri@unipr.it)

http://netsec.unipr.it

Cyber Security - Parma 14/11/2019

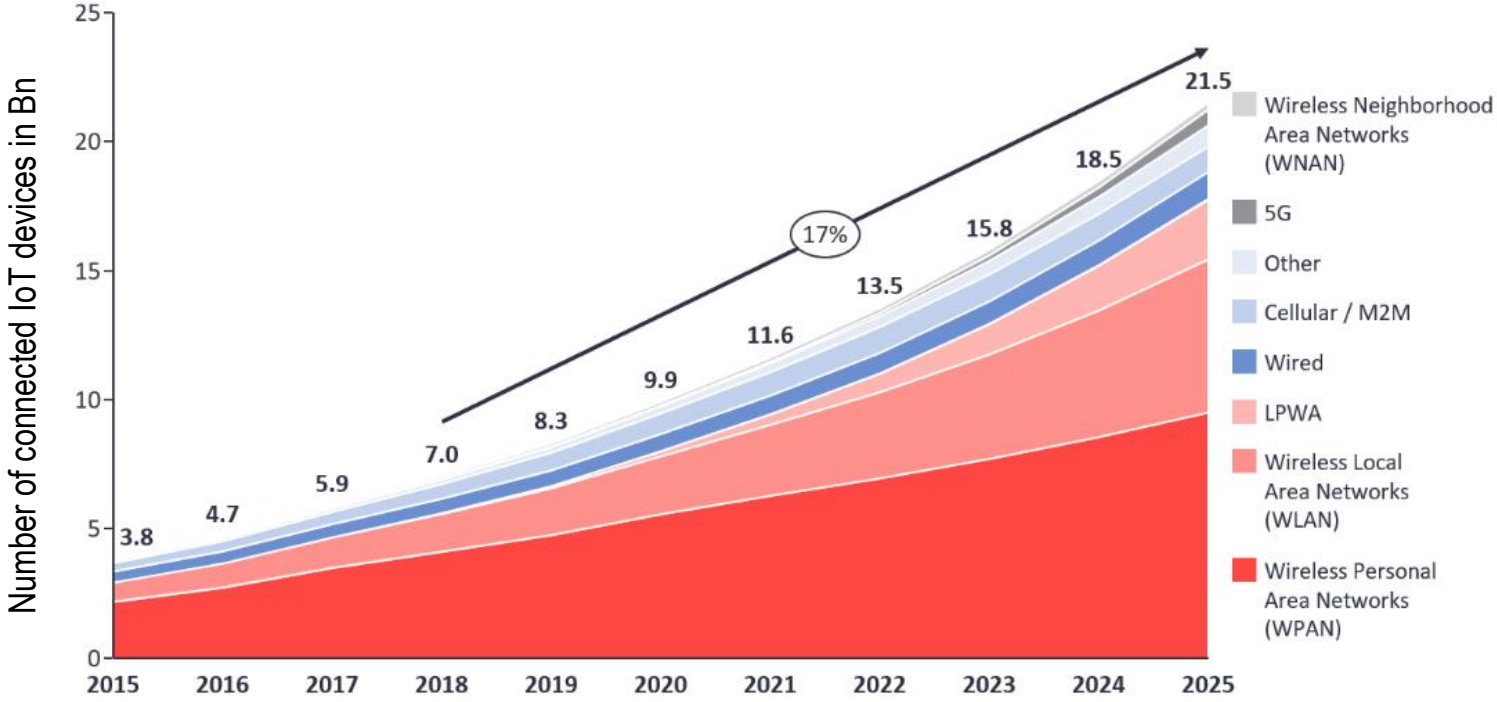
Internet of Things

- Internet of Things (IoT)
  - **interconnects billions of heterogeneous devices/smart objects**
  - **enabling new forms of interaction between physical objects and people**
  - **used in practically every field**



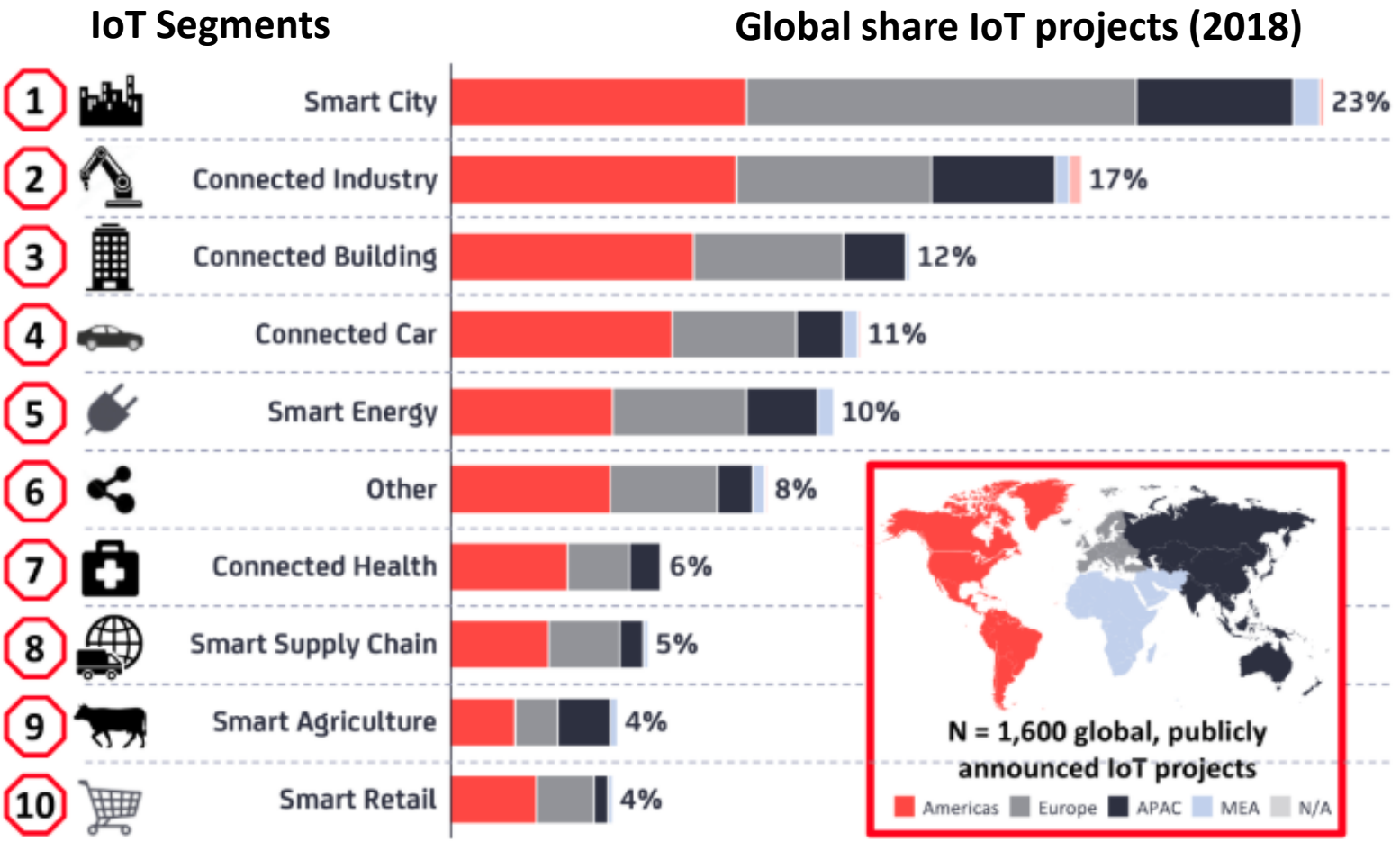
Internet of Things (cont.)

- Smart objects
  - **typically equipped with a radio interface, sensors, actuators, electronics and software**
    - collect and exchange data connecting to each other
  - **limited computational power, energy sources, and available memory**



Source: IoT-Analytics: https://www.statista.com/statistics/666864/iot-spending-by-vertical-worldwide

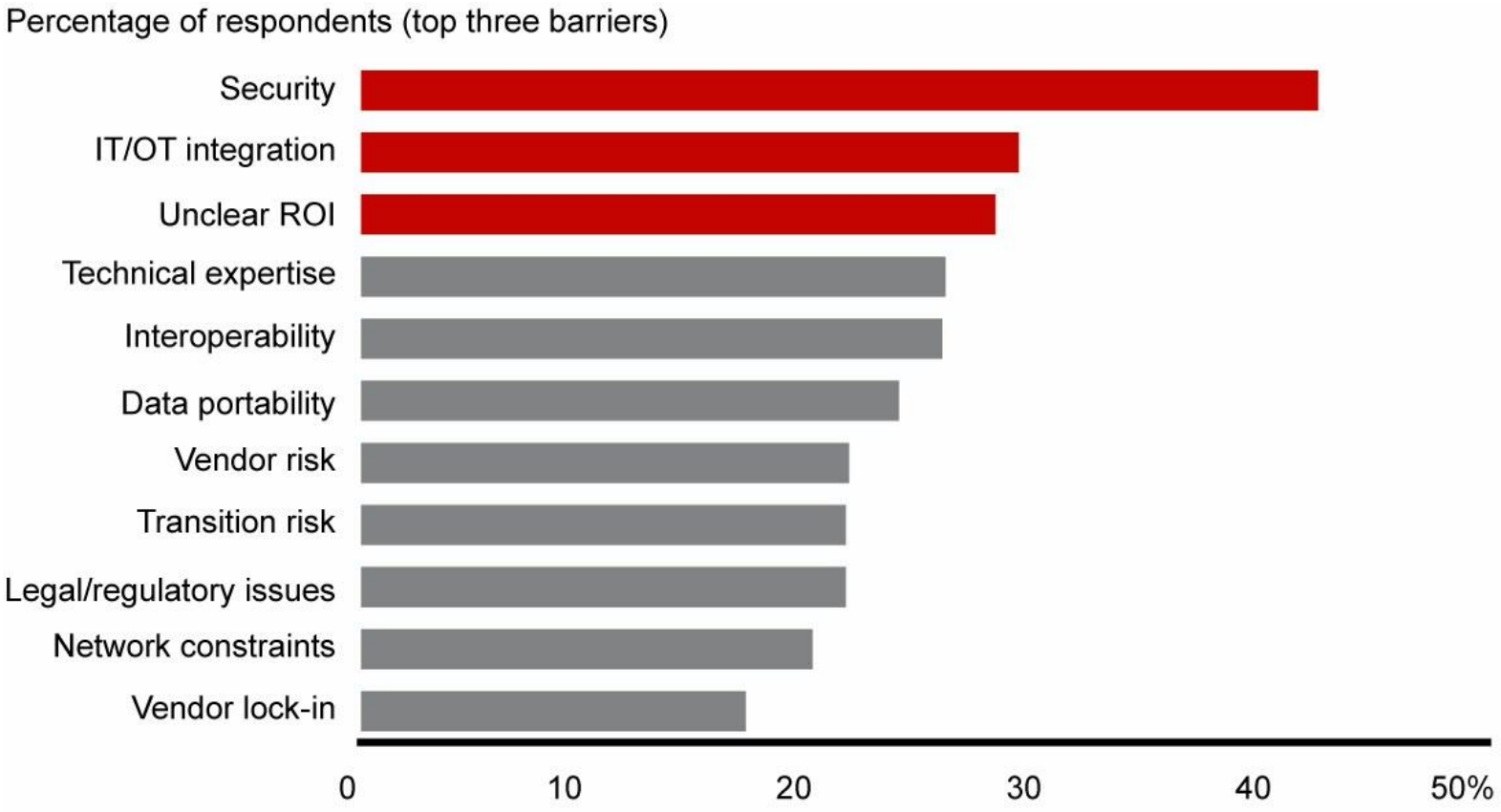
Internet of Things (cont.)



Source: IoT-Analytics: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

Internet of Things (cont.)

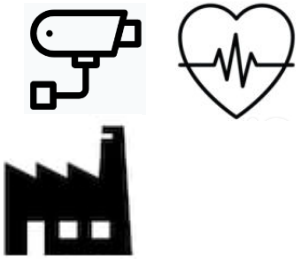
- What are the most significant barriers limiting your adoption of IoT solutions? (Forbes 2018)



Source: https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/

Security in IoT

- Very important requirement due to:
  - **the type of information that is exchanged/stored**
  - **the type of services that are implemented**



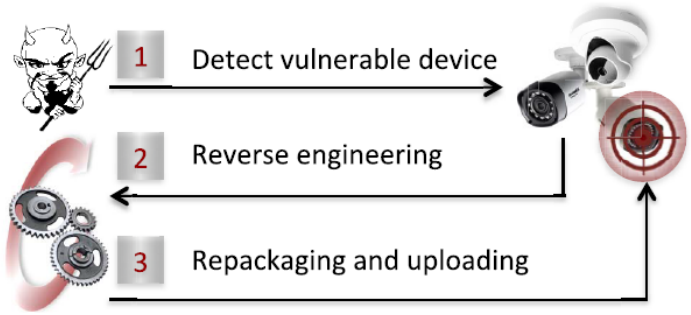
- Securing IoT is particularly complicated by:
  - **(possible) limited computational power**
  - **(possible) limited memory capabilities**
  - **(possible) limited communication resources**
  - **(possible) limited battery-powered**
  - **(possible) limited user interface**
  - **closed devices**
  - **heterogeneity**
  - **high distributed architectures**
  - **very low maturity**

Threat layers

- Threats can be based on:
  - **physical access**
    - if IoT devices operate in an unattended fashion with no or limited tamper resistance policies and methodologies
  - **network**
    - Internet and IoT-specific vulnerabilities caused by network or protocol weaknesses
  - **software**
    - attackers can gain remote access to smart IoT nodes by exploiting software vulnerabilities

IoT vulnerabilities

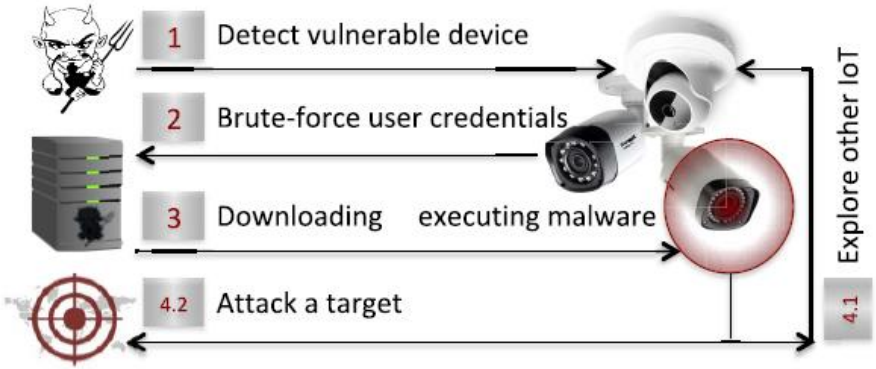
- Deficient physical security
  - **the majority of IoT devices operate autonomously in unattended environments**
    - with little effort, an adversary might obtain unauthorized physical access to such devices and thus take control over them



- Insufficient energy harvesting or limited computational power or communication resources
  - **an attacker might drain the stored energy by generating flood of legitimate or corrupted messages, rendering the devices unavailable for valid processes or users**

IoT vulnerabilities (cont.)

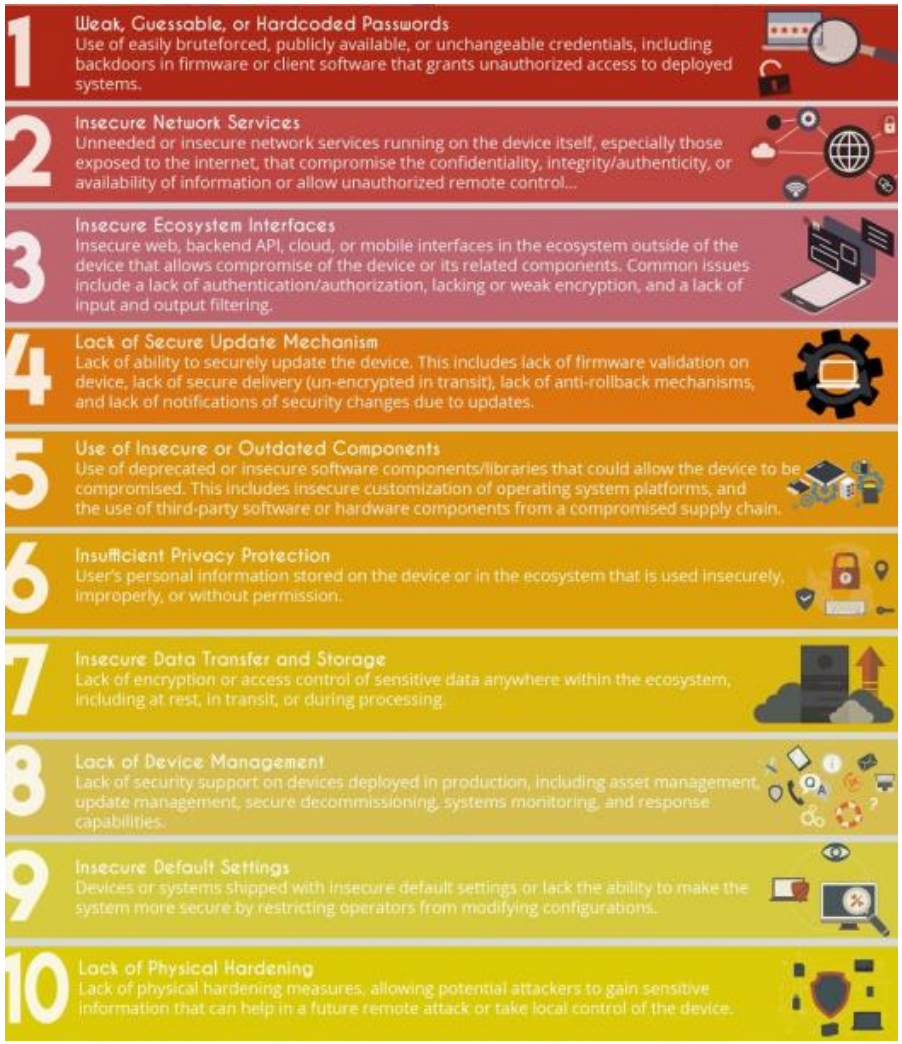
- Improper encryption
  - **resource limitations of the IoT affects the robustness, efficiency and efficacy of such algorithms**
- Inadequate authentication and access control
  - **when the keys are not being stored or transmitted securely, sophisticated (or otherwise effective) authentication algorithms become insufficient**
    - strong credential management should be required to protect devices and data from unauthorized access



IoT vulnerabilities (cont.)

- Week programming
  - **firmware are often released with known vulnerabilities (including backdoors, root users as prime access points) and lack of data encryption usage**
- Improper configuration
  - **Various IoT devices have unnecessarily open ports while running vulnerable services**
    - permitting an attacker to connect and exploit a plethora of vulnerabilities
- Improper patch management capabilities
  - **IoT operating systems and embedded firmware/software should be patched appropriately to continuously minimize attack vectors**
    - abundant cases report that many manufacturers either do not recurrently maintain security patches or do not have in place automated patch-update mechanisms, or done in an insecure way
- Insufficient audit mechanisms
  - **a plethora of IoT devices lack thorough logging procedures, rendering it possible to conceal IoT-generated malicious activities**

OWASP IoT Top 10 Vulnerabilities (2018)



Weak Guessable, or Hardcoded Passwords

Insecure Network Services

Insecure Ecosystem Interfaces

Lack of Secure Update Mechanism

Use of Insecure or Outdated Components

Insufficient Privacy Protection

Insecure Data Transfer and Storage

Lack of Device Management

Insecure Default Settings

Lack of Physical Hardening

Source: Open Web Application Security Project : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Countermeasures

- Countermeasures against physical threats:
  - **when possible, protect smart objects in safe places**
  - **safe supplying and installation measures**
    - avoiding untrusted manufacturers and installers
- Countermeasures against networked threats:
  - **secure communication protocols and cryptographic algorithms**
    - to enforce proper security services
      - peer authentication/authorization, data protection (authentication/integrity, confidentiality), anonymity
    - using proper cryptographic tools
      - (lightweight?) symmetric block ciphers, hash functions, asymmetric cryptography
    - avoid security function duplication
      - impact on the power computation and transmission performance
      - preserve interoperability
  - **robust authentication and key management**
    - security bootstrapping
    - a solid key management infrastructure
      - more complicated in IoT scenarios than in standard Internet

Countermeasures (cont.)

- Countermeasures against network and software threats:
  - **Vulnerability Assessment**
    - executing security evaluations undoubtedly aids in discovering IoT vulnerabilities prior to them being exploited
  - **Honeypots**
    - already proposed some IoT-specific honeypots
  - **Intrusion Detection**
    - ML-based NIDS

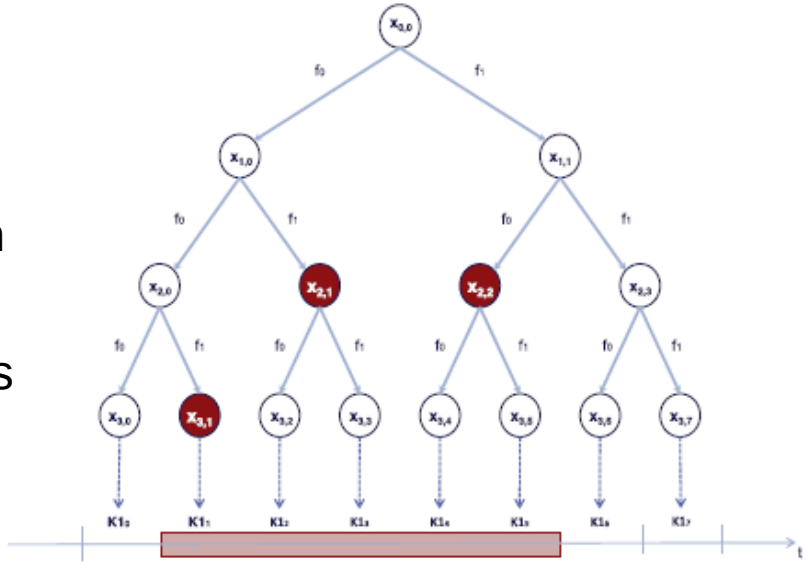
Our IoT Security research projects

EU Project Calipso (2011-2014)

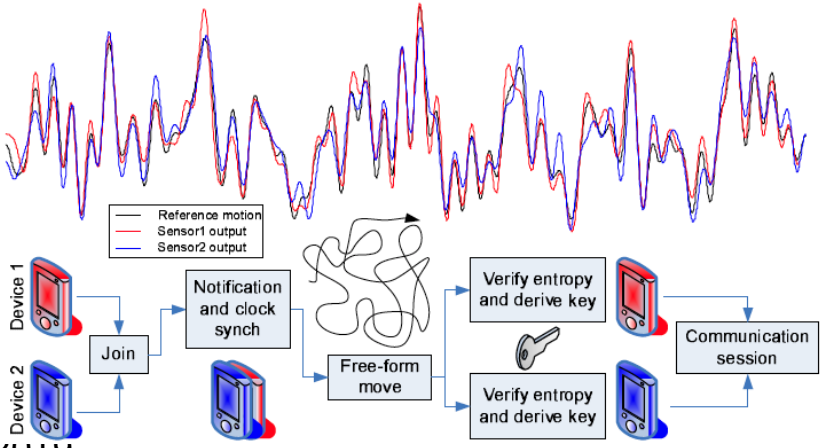
- Focus on Internet Protocol (IP)-connected smart object networks, with novel methods to attain very low power consumption
- Partners
  - **Thales, CNRS @Grenoble, Swedish Institute of Computer Science, University of Parma, Disney Research Zurich, Worldsensing (ES), CISCO**
- IETF/IPv6 framework (6LoWPAN, RPL, CoAP)
- Platform for developments: Contiki
- Three applications/testbeds:
  - **Smart Infrastructures**
  - **Smart Cities/Parking**
  - **Smart Toys**

Key management

- Group key distribution
  - **group key**
  - **users join/leave**
  - **KDC-based group key distribution**
  - **per-slot keys**
    - no re-keying when a user leaves
  - **collusion resistant**

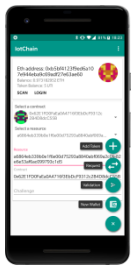


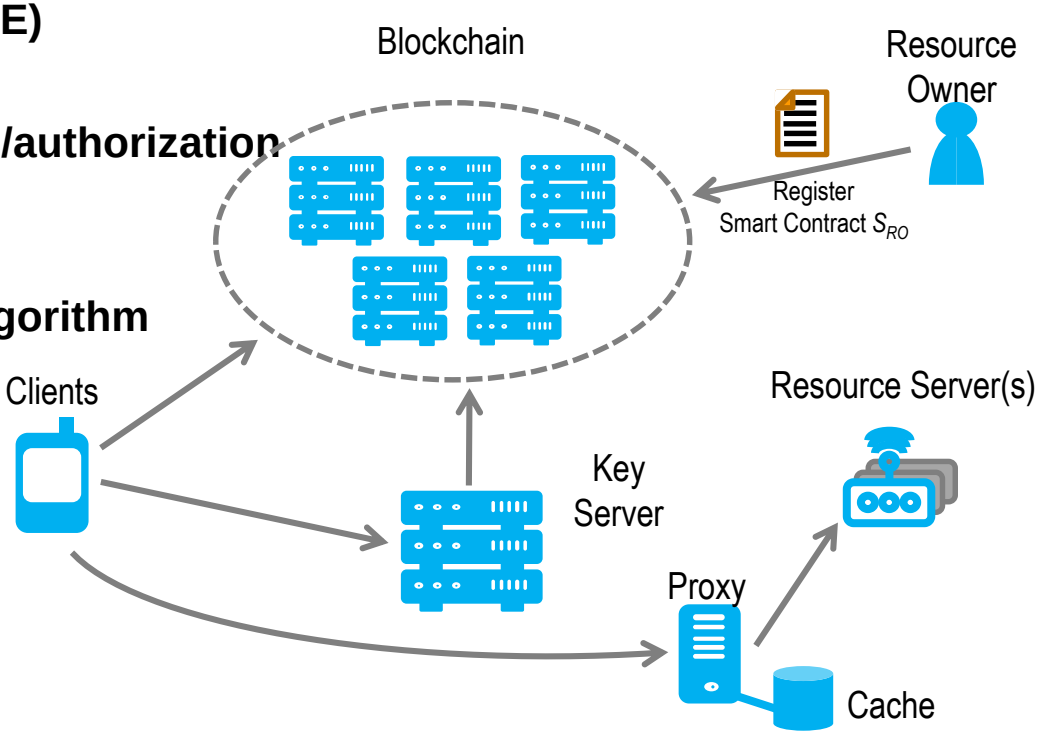
- Martini-synch key exchange
  - **exploits closeness**
  - **inertial data**



IoT and Blockchain

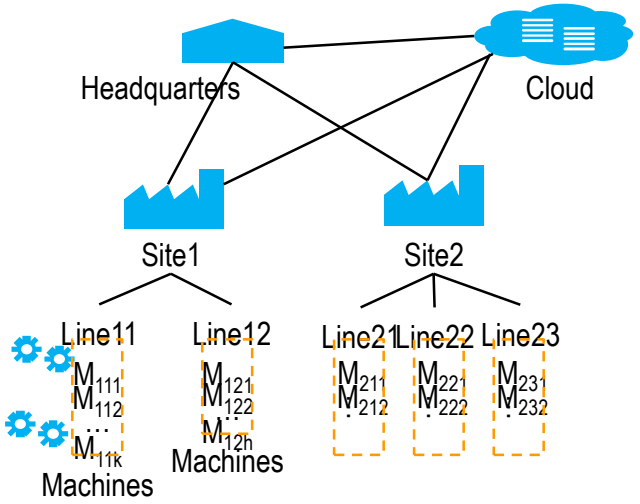
- With Univ. Grenoble Alpes, CNRS France
- IoTChain: Use of blockchain for fully distributed authentication and authorization
  - **data oriented security (E2E)**
  - **key-based authorization**
  - **distributed authentication/authorization based on blockchain**
  - **use of smart contracts**
  - **proper key distribution algorithm**
- Implementation
  - **Ethereum**
  - **CoAP**
  - **mobile UA**



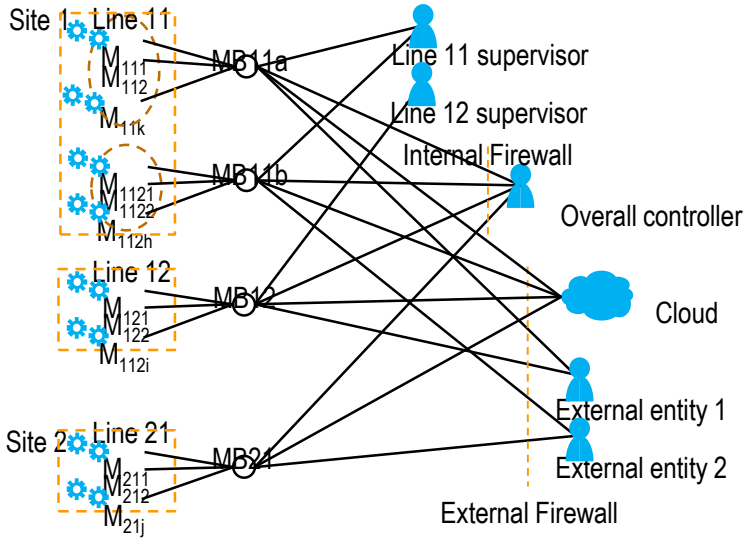


Secure Pub/Sub-based Industrial IoT

- IIoT scenario:
  - **company with one or more production sites and a headquarter**
  - **each site may include one or more production lines formed of different machines**
  - **PLCs, SCADAs and distributed sensing systems, formed by IoT devices and organized as WSN**
    - they are interconnected to per-line and per-site remote controllers
    - they may also be interconnected to the headquarter site and/or to an external Cloud system to enable cross-site monitoring and control



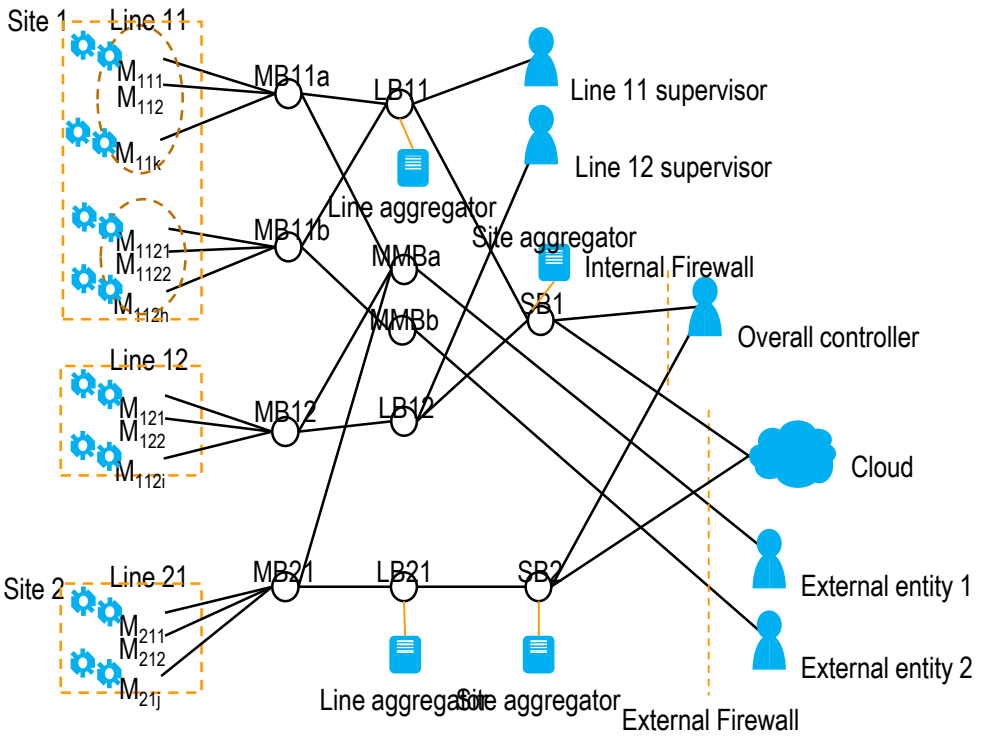
- From the security point of view, complex and non-scalable architecture
  - due to the high number of M2M interactions that has to be separately



Secure Pub/Sub-based Industrial IoT (cont.)

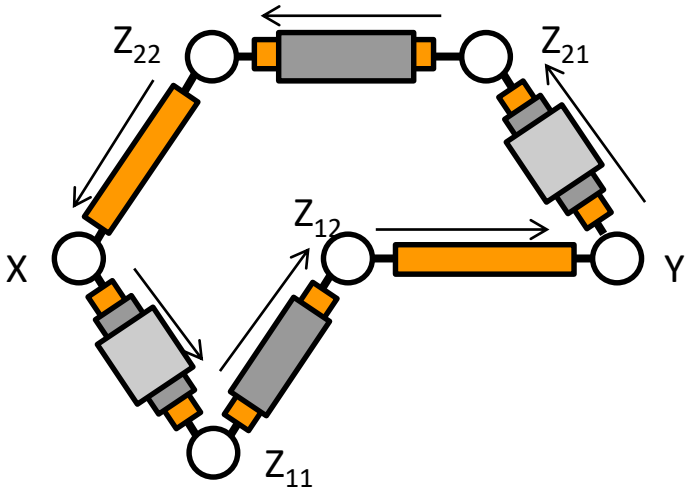
- MQTT-based multi-stage IIoT architecture
  - **multi-level of brokers according to different access classes**

- Advantages:
  - **simplification of client-to-broker relations for the authentication and authorization**
  - **simplification NAT and firewall configurations**
  - **scalability in terms of total number of flows**
  - **simplification of new data processing functions, fully integrated with the multistage pub/sub architecture**

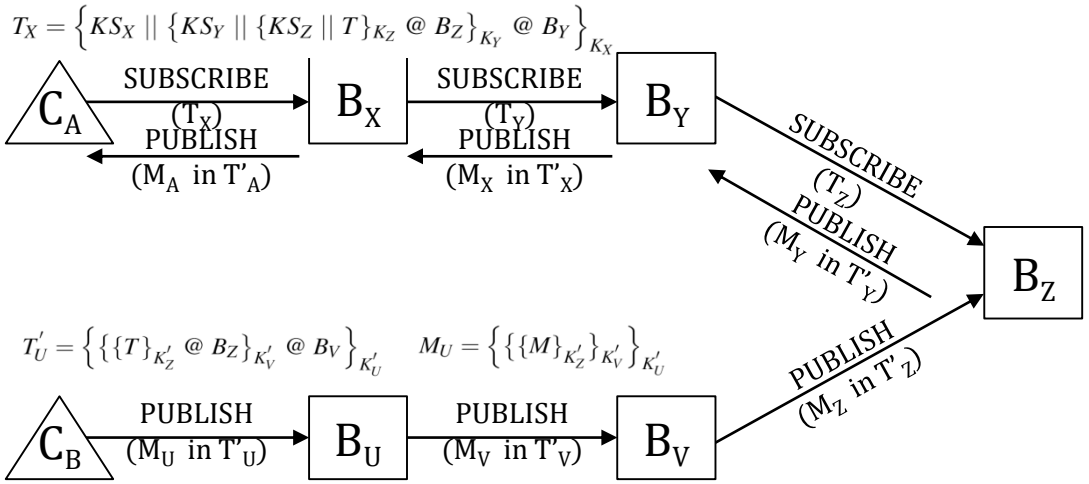


Anonymity

- New anonymity mechanisms
  - **new requirements**
- Network level
  - **Datagram-based Onion Routing**
  - **different paths can be considered**
  - **per-message routing**



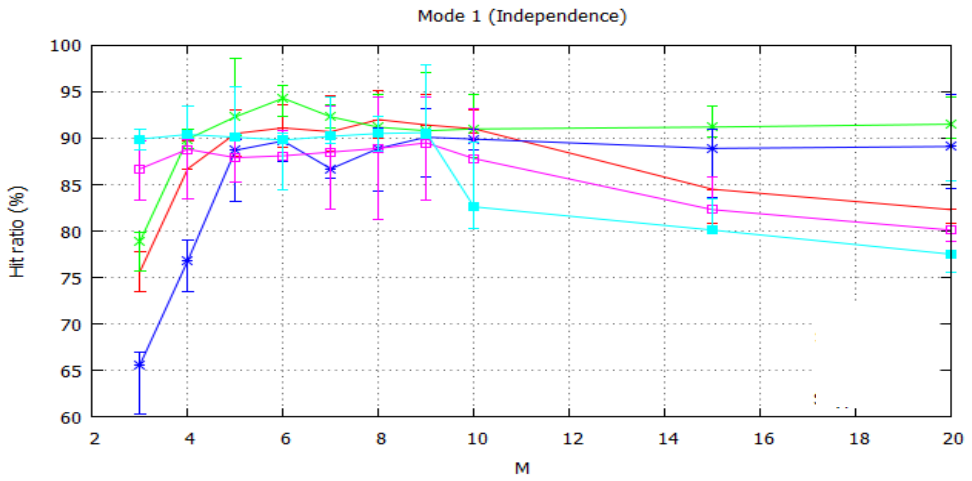
- Application level
  - **Publish-Subscribe**
  - **MQTT**



Other security-related projects

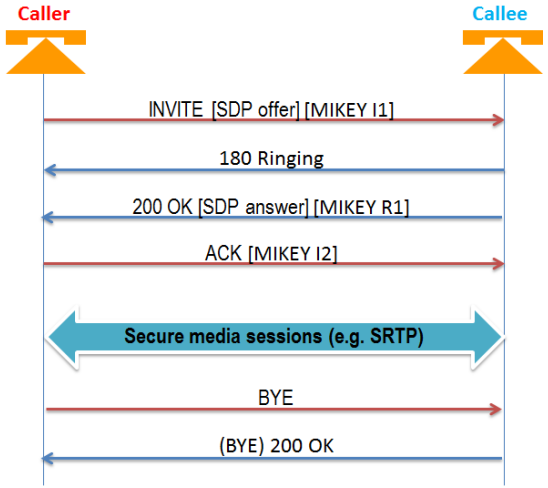
Blind traffic classification and IDS

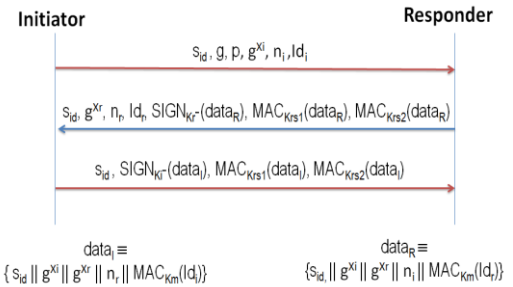
- Classical traffic classification methods
  - **Session-based: well known port matching, session behaviour modelling, etc.**
  - **Content-based: protocol inspection, signature matching, etc.**
- New constraint-based statistical method
  - **fine-grained (specific application), supervised, probabilistic**
  - **maximum likelihood strategy**
  - **session packets characterized by size, time,and sqn**
- ML analysis/learning
- Anomaly-based NIDS



VoIP/IM Security

- Vulnerabilities
  - **weak protocols**
  - **E2E security**
- UA to UA security
  - **end-to-end authentication and confidentiality**
    - end-to-end authentication and key agreement
  - **symmetric key through authenticated DH**
  - **the DH key authenticated using a short authentication string and side-channel**
    - e.g. voice
- Development activity
  - **mjSIP open-source project**
    - TLS, SRTP, ZRTP, etc.
    - http://www.mjsip.org





Quantum security projects

- Team
  - **Michele Amoretti (PhD, associate professor)**
  - **Davide Ferrari (PhD student)**
- Topics
  - **high performance computing (classical and quantum)**
  - **quantum compiling**
  - **quantum networking**
- Quantum security projects:
  - **quantum anonymity**
    - https://github.com/qis-unipr/qsip-practical-anonimity
  - **entanglement verification**
    - https://github.com/qis-unipr/entanglement-verification

Thank you!

Luca Veltri

mail.to: luca.veltri@unipr.it

http://netsec.unipr.it