Multi-layered Security Technologies
for hyper-connected smart cities

A EU-Japan collaboration

Vanessa Clemente, Worldline
The Consortium as a whole
Problem Overview

In modern smart city applications there is an emerging need of end-to-end security since many data sources may contain sensitive information that raises issue on privacy and data protection.

- **Application**
  - Unauthorized Permission and Manipulation of Sensitive Data

- **Data Accumulation**
  - Attacks to Private Data Confidentiality and Integrity

- **Physical Devices**
  - Node Failure, Sybil Attack

- **Connectivity**
  - Hacking, DoS, Man-in-the-Middle Interception

- **Data Abstraction**
  - Replay Attack, Account List Attack
According To the IoT Analytics Press Research, the most common IoT breaches that happened between 2015-2017 were caused by malware (24%), followed by human's factor “man in the middle” (22%), brute force (18%) and denial of service (15%).
M-Sec goals

We aim to research, develop, deploy and demonstrate Multi-layered Security Technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages Cloud, IoT, device, BigData, blockchain, and end-end security, upon which they can build innovative smart city applications.
M-Sec Framework

Development & Security Designing Tools
Set of methodologies and tools to support development of secure smart city applications and reduce number of tests to be conducted

Secure & Trusted Storage
Mechanisms to encrypt data off-chain and store the corresponding metadata and interactions-related data on-chain through Blockchain for data tamper proof.

Secure City Data Access
Distributed and federated infrastructure for IoT sensor data with anonymous subscription function and interconnection of different networks to achieve secured access and communication with embedded devices.

Secure Devices
Hardware based solution to provide embedded security layer for IoT devices and software-based solution to provide secure IoT mobile sensing platform by monitoring and preventing cyber attacks.

IoT Data MarketPlace
IoT sensor data and media exchange platform based on blockchain technology and Trust and Reputation Model engine to ensure reliability, trustworthiness and reputation of the resources exchanged

Privacy Management Tool
Tool to automatically remove objects with privacy risk from image camera data based on advanced deep learning image processing technology.

End to End Security
Fully interoperable security backend that enables authentication of parties, encryption of data, attestation of devices and anonymization of data sources.
Advancing to end-to-end IoT Security Application

**Secure IoT**
- HW Security
  - Secure, robust, distributed and encrypted data Storage
  - Remote attestation platform
  - Secure boot mechanism
  - Secure encryption and decryption of data
  - Intrusion Detection System
  - Zero Day threats

**Secure Gateway**
- SW Security
  - Image Privacy, removing personal data in streaming
  - Visualization Tool for threat monitoring & health check
  - Vulnerability assessment mechanisms

**Secure Cloud**
- Secure, robust, distributed and encrypted data Storage
  - Encrypted Storage of sensitive data with asymmetric
  - public/private key pair
  - Smart Contracts where to store transactions, hashes
  - from data encrypted for data tamper proof reasons
  - Data Access Control Authentication & Authorization mechanisms

**Secure Application**
- Application Security Guidelines & Secure City Data Access
  - Abstraction layer to hide the heterogeneity of IoT devices
  - Exchange data with anonymous subscription function.
  - Client/server and publish/subscribe access protocols
  - Northbound access security
  - Mechanisms to analyze security requirements
  - A Modal System Transition Analyzer to eliminate both human errors in designing the application logic

**Transport Layer Security**
- Secure Communication

**Audit**
- Anonymization
- Attestation
- Authorization
- Authentication
Do you want to know more?

Media Kit

Relevant Initiatives

Scientific Papers

Deliverables

Get Involved

Press Coverage

www.msecproject.eu
...and don’t forget to follow us on

@MSecProject
Thank you!