Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative
Istituto sistemi informativi e networking

SUPSI

Uprise-IoT

User-centric PRIvacy & SEcurity in the IoT

Alan Ferrari, Ph.D
alan.ferrari@supsi.ch

25 aprile 2018

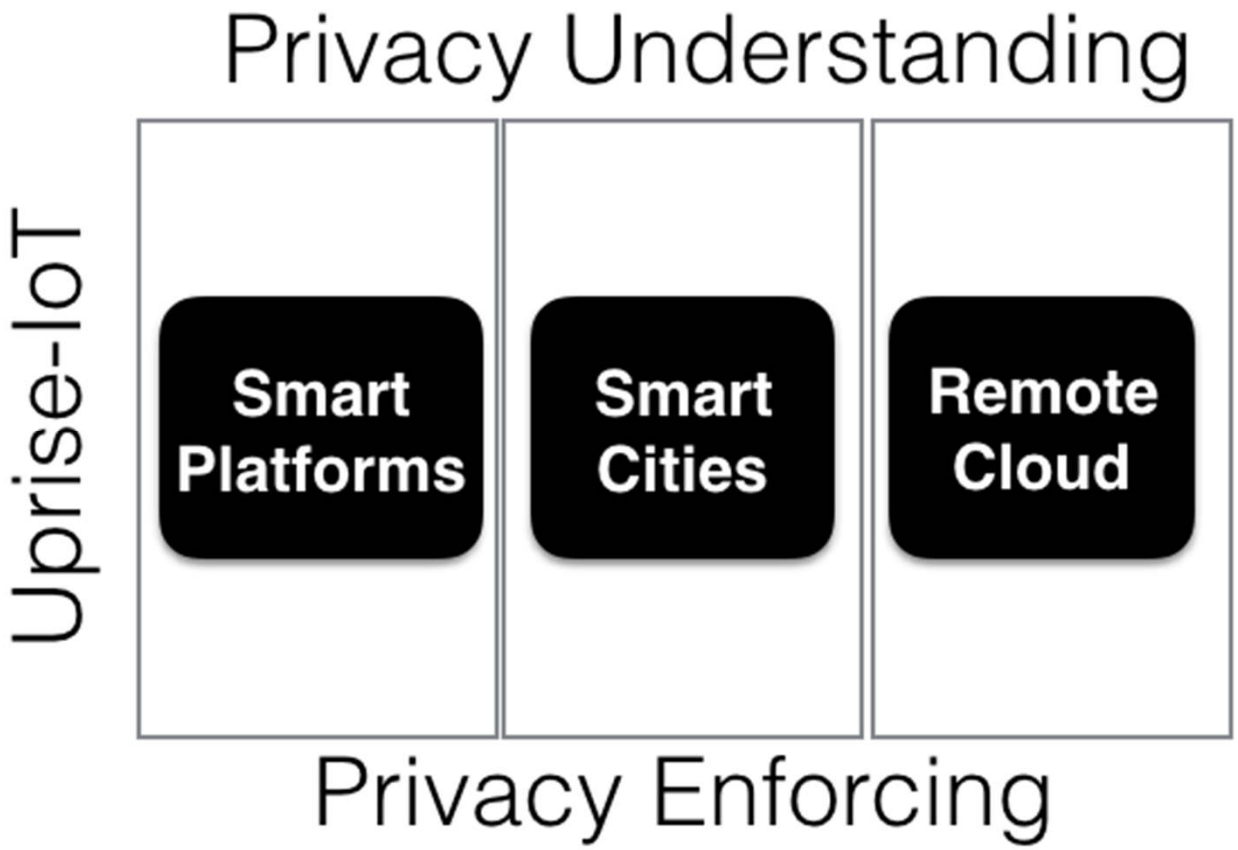
Uprise-IoT Facts

- 2015 CHIST–ERA call SPTIoT:
  - CHIST-ERA – international framework for basic research
  - SPTIoT: User-Centric Security, Trust and Privacy in the Internet of Things
- Starting date: 1.11.2016
- Ending date: 31.10.2019
- Partners: SUPSI, INRIA, EURECOM, UCL
- Requested Budget: 1,171,192.05 €

Summary

- UPRISE-IoT's goal is to make **users gain control and awareness** over data generated and collected by the IoT devices surrounding her.
- This project will take **a fresh look at the IoT privacy** space by considering a user-centric approach:
  - by considering user **behaviors and the user context** in order to **improve security and privacy**, and realize so privacy preserving data collection and processing;
  - by increasing **data transparency and control**. Users will be informed about the data that are being collected in a user-friendly manner, and will have the option to oppose to them.

Dimensions

- 
Privacy Understanding
Uprise-IoT
Smart Platforms
Smart Cities
Remote Cloud
Privacy Enforcing

Practical and verifiable objectives

- Define **models for describing the current context of the IoT devices**, and for **predicting the future evolution** of the IoT ecosystem.
- Propose **novel strategies to secure IoT** devices, their M2M and H2M interactions.
- Design and **develop tools that will empower users in IoT**.
- Design solutions to **increase the user's awareness**.
- Design and develop **open libraries for supporting user control** (preferences, filters, accounting and analytics), **transparency**, as well as realization of advanced functionalities and algorithms.

Ongoing Activities (1/6)

- Is Your Privacy Really in Your Hands? (SUPSI)
  - **Problem**: users' information domain is not confined to what they deliberately share.
  - **Goals**: to understand how much knowledge can be inferred about a target user by analyzing others' available information.
  - **Status**: data collection.

Ongoing Activities (2/6)

- Local Internet of Things (EURECOM)
  - **Problem**: Designing protocols for secure bootstrap and data management in IoT.
  - **Status:**
    - Design of a protocol enabling lightweight secure boostrap and message attestation in the IoT [SAC 2018].
    - Implementation of the local solution: development of an in-house IoT platform allowing direct communication among devices**.**

Ongoing Activities (3/6)

- Study on Third-Party Services in Smart Devices(SUPSI)
  - **Problem**: We are interested in determining what are the data third party libraries are interested in.
  - **Status:**
    - Collection on app / service execution statistics on ral devices.
    - We are developing the framework to analyze those libraries via reverse engineering.

Ongoing Activities (4/6)

- Providing transparency on data collection and processing in the smart city (INRIA)

  - **Problem**:
    - The General Data Protection Regulation (GDPR) requests from data controllers to display information about data collection and processing.
    - We propose a visual registry for the smart city : **Map of Things**, to display devices collecting personal data and their privacy policies.

  - **Status:**
    - A prototype website is online and working, it displays various devices with their privacy policies.
    - Collaboration with French cities is planned, to experiment the solution.

Ongoing Activities (5/6)

- Study on User Perception about privacy in Smart devices (SUPSI + UCL)
  - **Problem**:
    - Study the changes in perception and behavior of different subjects when confronted with the data leakage on their Smartphones..
  - **Status:**
    - Build an app that queries the user about possible data leackages.
    - Testing the first prototype of the app.

Ongoing Activities (6/6)

- Interpretable Machine Learning for Privacy-Preserving Pervasive Systems (UCL)
  - **Problem**:
    - Development of a framework for **interpretable machine learning** from personal data (in particular mobile and social media data).
  - **Status:**
    - We have developed an abstract architecture for supporting privacy-preserving machine learning.