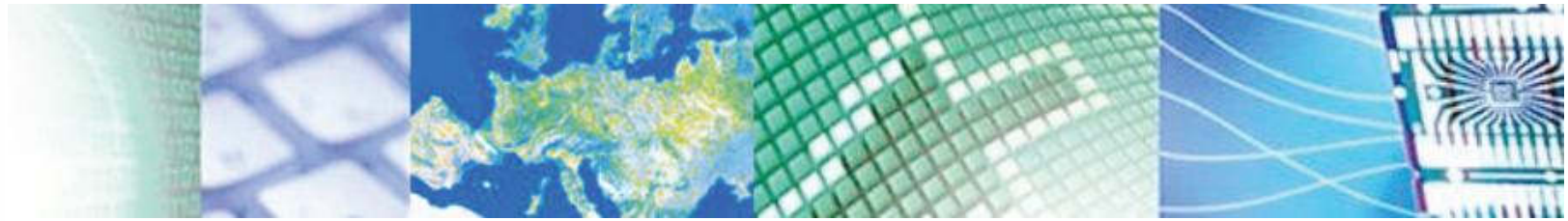


CHIST-ERA Projects Seminar
Cross Topics
SPTIoT

Gareth Howells

Paris, April 12th, 2018

Programme co-funded by the
EUROPEAN UNION

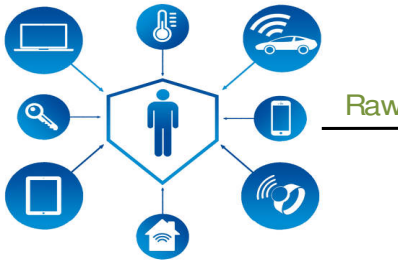
User-Centric Security, Privacy and Trust in the Internet of Things (SPTIoT)

- ✓ Methods for data anonymisation
- ✓ Technical mechanisms to increase trustworthiness when data is shared between different providers
- ✓ Intrusion detection methods
- ✓ Authentication using trusted computing (lightweight hardware and software security)
- ✓ Dynamic security to allow systems to adapt to varying users
- ✓ Data visualisation for increasing user awareness of privacy issues
- ✓ Empowering users with risk evaluation tool for their data and contacts;
- ✓ Assistive technology/techniques to encourage more secure behaviour and awareness of users

SPIRiT: Security and Privacy foR the Internet of Things

- **Enhance trust and integrity of IoT technology**
- **Address lack of user confidence in the technology**
- **Specifically**
  - How to ensure data originates from claimed device?
  - How to ensure it has not been altered?
  - How to ensure users comply with security requirements?
  - How to ensure the solution is easy and cheap to deploy?
  - How to ensure system may evolve to changing requirement?

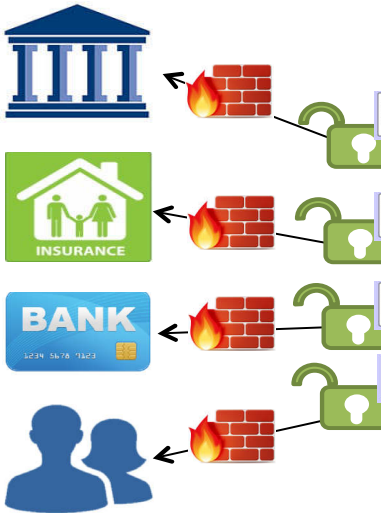
SPIRiT: Security and Privacy foR the Internet of Things



Raw

User's IoT devices
Data producer

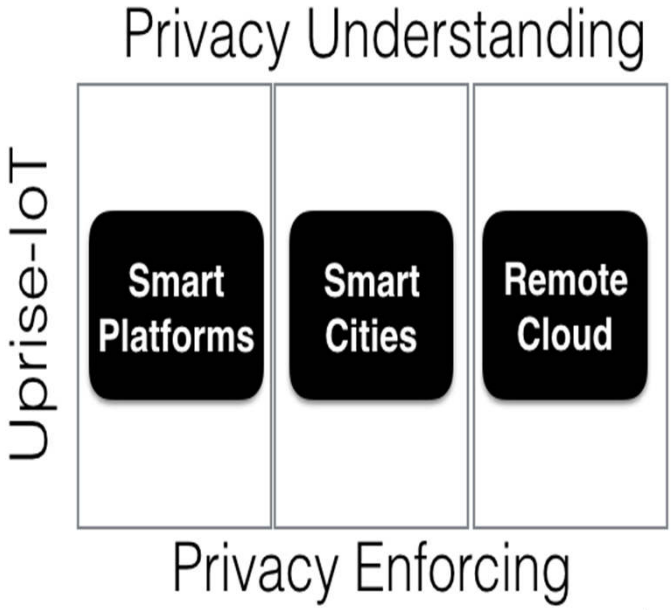
IoT Hub



Data consumers

UPRISE-IOT (SUPSI, INRIA, EURECOM, UCL)

- **Goal: UPRISE-IoT's goal is to let the users gain awareness and control over data generated and collected by the IoT devices surrounding her.**
- **Create models for describing the current context of the IoT devices**
- **Create novel strategies to secure IoT.**
- **Develop tools that will empower users in IoT.**
- **Increase the user's awareness.**



UPRISE-IOT

- **Current works:**
  - ✓ To understand how much **knowledge can be inferred** about a target user by analyzing **others' available information**.
  - ✓ Designing protocols for **secure bootstrap and data management** in IoT.
  - ✓ Study in data leakages caused by third party libraries in smart devices.
  - ✓ Implementation of a visual registry for the smart city : **Map of Things**
  - ✓ Study the changes in **perception and behavior** of different subjects when confronted with the **data leakage** on their smart devices.
  - ✓ Development of a framework for **interpretable machine learning** from personal data (in particular mobile and social media data).

http://uprise-iot.supsi.ch/

IDentification for the Internet of Things

CHIST-ERA call 2015
project 651.002.003
Starting date February 2017

Boris Skoric (TU Eindhoven)
Daan Leermakers

Teddy Furon (INRIA)
Laurent Amsaleg
Marzieh Gheisari

Slava Voloshynovskiy (Univ. Geneva)
Behrooz Razeghi

IoT problem areas:

- identification/authentication of constrained IoT devices
- scalability problems

Technologies:

- (optical) PUFs, quantum readout
- approximate nearest neighbor search
- scalable signal processing

Technische Universiteit Eindhoven University of Technology

inventeurs du monde numérique

UNIVERSITÉ DE GENÈVE

Chist-era seminar, April 2018

IDentification for the Internet Of Things: Results so far

- Privacy preserving protocols based on random projections with sparse vector representation and ambiguisation [1,2].
- Similarity search in high-dimensional spaces [3].
- Security analysis of QSA-related protocols [4,5].

Publications

[1] *Privacy Preserving Identification Using Sparse Approximation with Ambiguization*.
B. Razeghi, S. Voloshynovskiy, D. Kostadinov, O. Taran.
IEEE Workshop on Information Forensics and Security (WIFS) 2017. pp.1-6.

[2] *Privacy-preserving outsourced media search using secure sparse ternary codes*.
B. Razeghi, S. Voloshynovskiy.
International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2018.

[3] *Memory vectors for similarity search in high-dimensional spaces*.
A. Iscen, T. Furon, V. Gripon, M. Rabbat, H. Jégou.
IEEE Transactions on Big Data 4(1), pp. 65-77, 2018.

[4] *Optimal attacks on qubit-based Quantum Key Recycling*.
D. Leermakers, B. Škorić.
Quantum Information Processing 17(3), pp. 57, 2018.

[5] *Security proof for Round Robin Differential Phase Shift QKD*.
D. Leermakers, B. Škorić.
https://eprint.iacr.org/2017/830

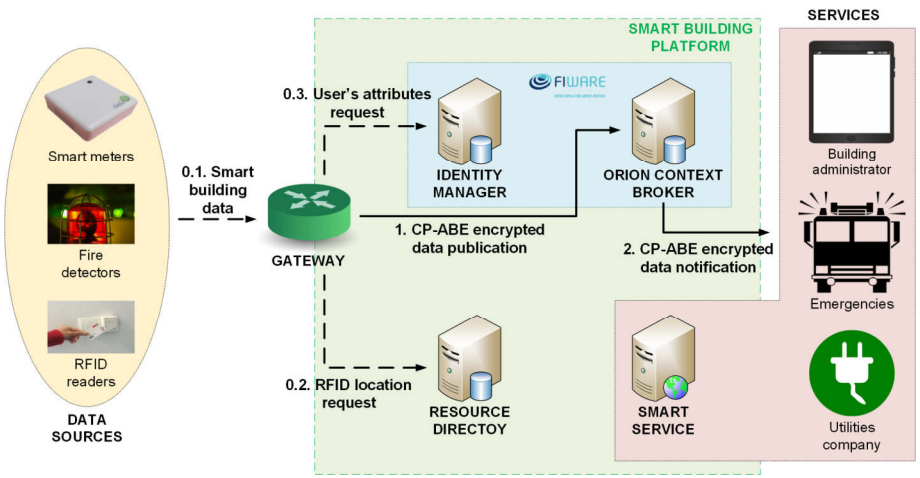
USE-IT

- **USE-IT: U**ser empowerment for **SE**curity and privacy in **I**nternet of **T**hings (http://useit.eu.org)
- **Objective:**
  To let users and devices easily and tightly control who has access to which data in which context, without leaking collateral information such as location or behaviour data.
- **Partners:**
  - ✓ IBM Research – Zurich, CH
  - ✓ University of Murcia, ES
  - ✓ Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA), FR
  - ✓ Technical University Eindhoven (TUE), NL:

USE-IT Technology

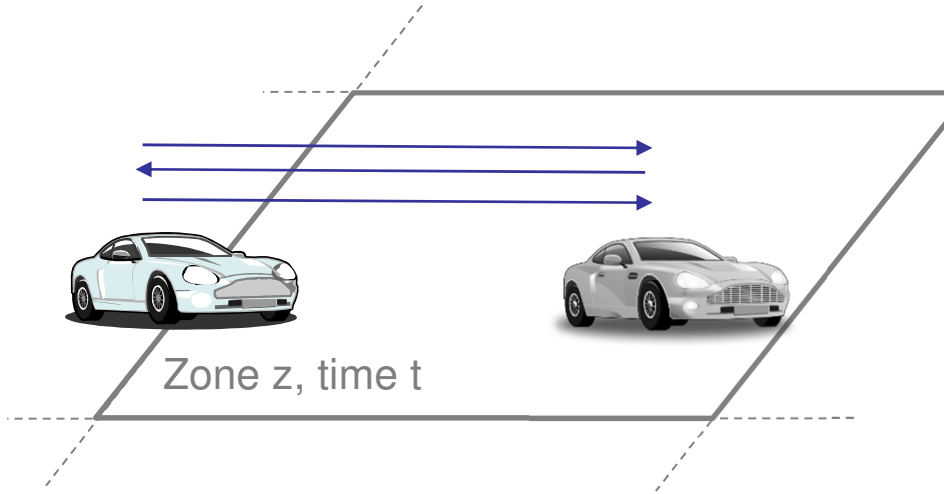
Smart buildings

- Combine symmetric crypto with CP-ABE for scalability, efficiency and flexibility
- Bridge incident response (reactive) and CP-ABE (preventive) by integrating IDS



Geo-zone encryption for location privacy in C-ITS

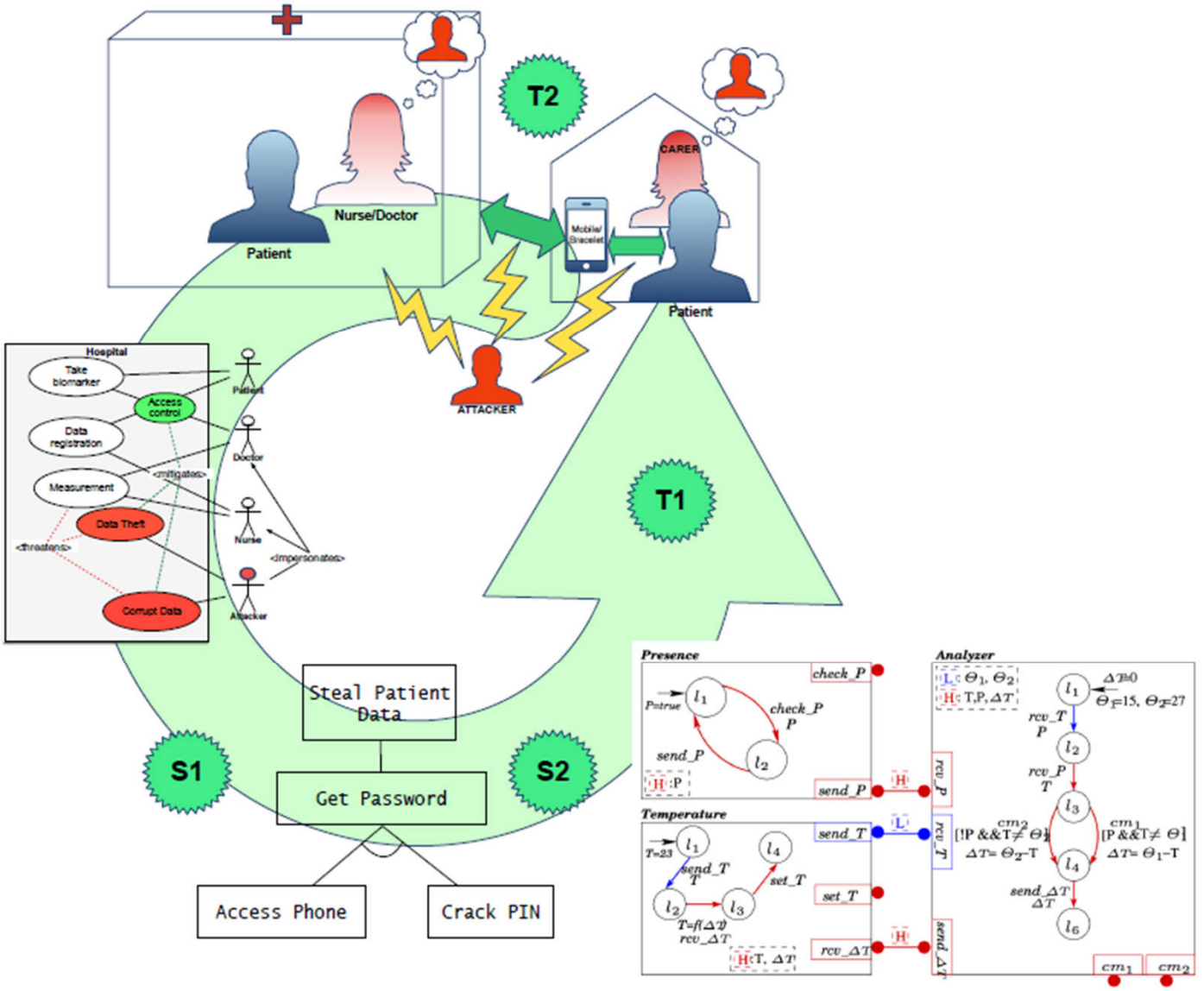
- unlimited pseudonyms by Privacy-ABCs
- security against passive eavesdropping by encryption



SUCCESS

- Overview/Main Goals: SUCCESS, Secure Accessibility for the IoT
  - ✓ Formal design of privacy-critical IoT scenario
  - ✓ Risk visualisation by attack tree analysis
  - ✓ Certified implementation for IoT component architectures
  - ✓ IoT Pilot scenario: sensor based monitoring for Alzheimer's patient

SUCCESS


T2
Nurse/Doctor
Patient
CARER
Patient
ATTACKER
T1
Hospital
Take biomarker
Access control
Data registration
Measurement
Data Theft
Corrupt Data
<mitigates>
<threatens>
<impersonates>
Patient
Doctor
Nurse
Attacker
Steal Patient Data
S1
S2
Get Password
Access Phone
Crack PIN
Presence
Temperature
Analyzer

SUCCESS

- Achievements
  - ✓ Pilot infrastructure
  - ✓ Pilot architecture
  - ✓ Attack tree analysis
- Roadmap/Vision:
  - ✓ S&P-certified IoT Healthcare monitoring system
  - ✓ Reproducable process to instantiate similar certified systems for use in healthcare (Knowledge Transfer)
  - ✓ User Transparency: Visualisation of Attack Trees
- Challenges:
  - ✓ Reach out to stakeholders to validate vision
  - ✓ IoT devices (sensors) are off-the shelf, not open-source, not suitable for code generation

Upcoming challenges and Roadmap

- **How to exploit complementarities of each project**
- **Availability of solutions**
- **What should we integrate?**
- **Common dissemination?**
  - ✓Special session in conference?

Role of the CHIST-ERA support

- Smaller and more focus within the projects
- Annual meetings allow better collaboration
- More direct contact with support staff
- Allows incorporation of more diverse set of researchers
- Integrates partners from each country because of fixed funding per country
- Focus on international project on basic research

Questions

Questions ?