

SUCCESS: Secure Accessibility for the IoT

Middlesex University London
Inria Rennes Inria / ESTASYS and PARKAS
Université Grenoble / Verimag
University of Twente, Netherlands

<http://www.iot-success.eu>

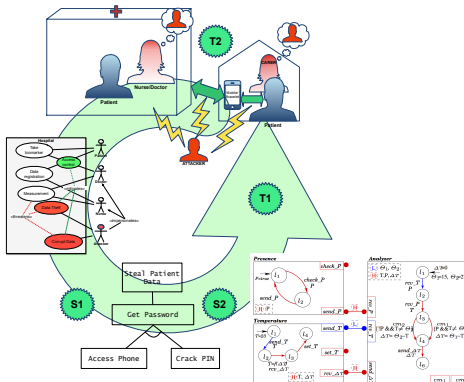


CHIST-ERA Seminar Paris, 11. April 2018

Current Project for Security and Privacy for IoT

CHIST-ERA (EU) project SUCCESS:

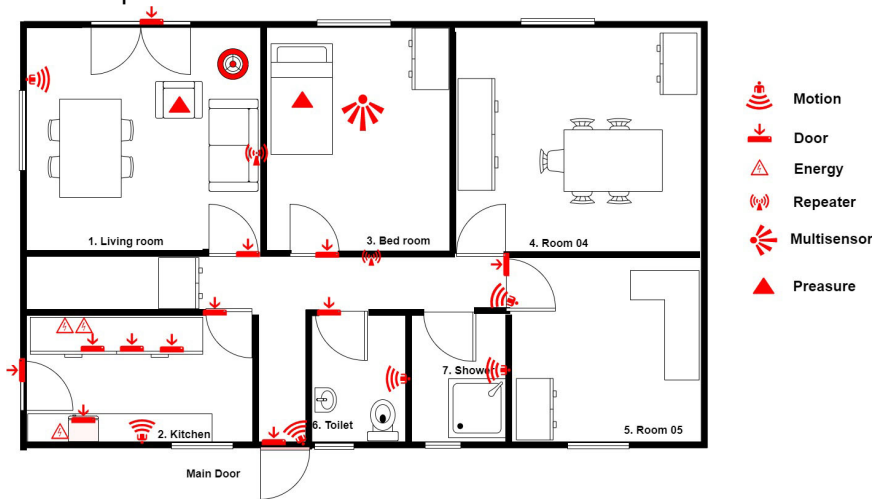
SecUre aCCESSibility for the internet of things



- Formal design of privacy-critical IoT scenarios
- Risk visualisation by **attack tree analysis**
- Certified implementation for IoT component architectures
- IoT Pilot scenario: sensor based monitoring for Alzheimer's patients

Pilot Infrastructure (MU)

Plant map of FarmSide : authentic house at MU

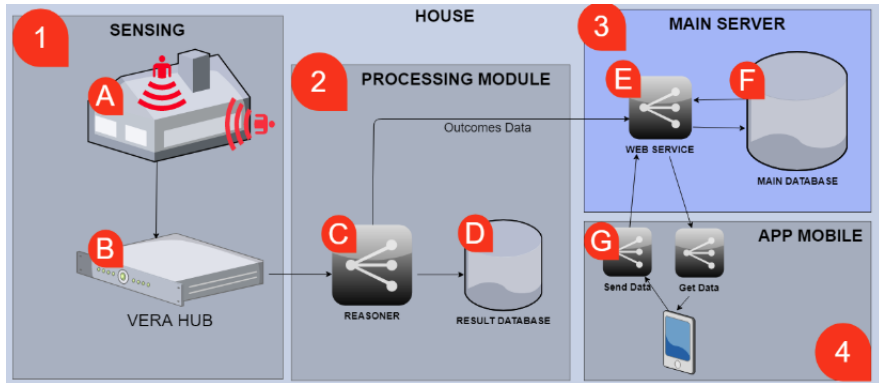


Sensor Hub (MU)

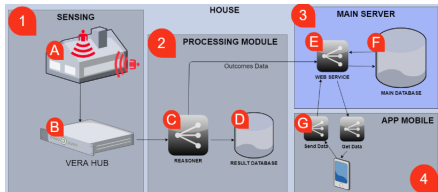
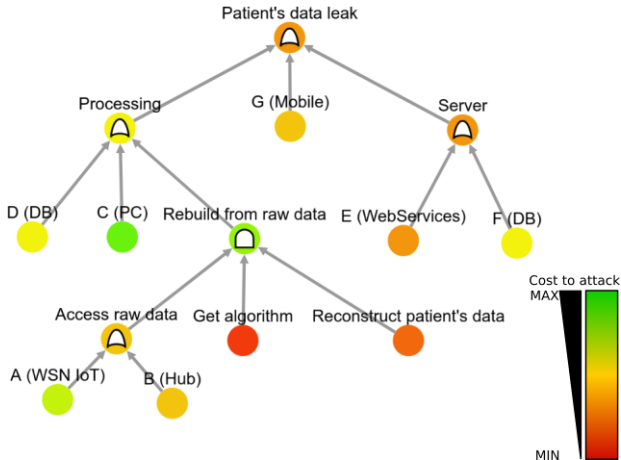
Vera Sensor Hub in Farmside



Pilot Architecture



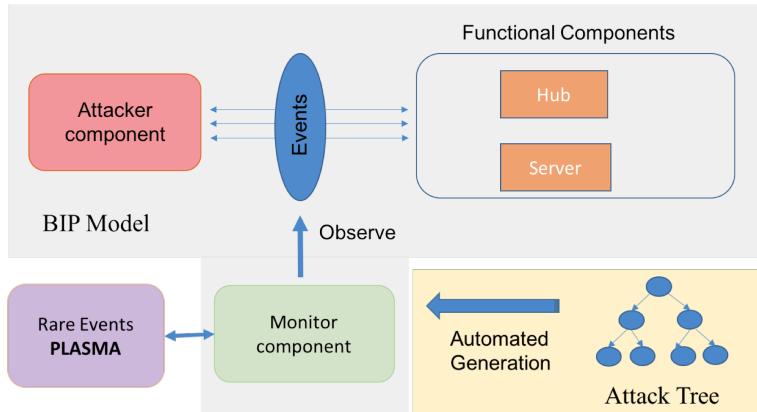
Attack Tree Analysis (UT)



BIP Extension (Inria/UGA)

New Tools for BIP methodology

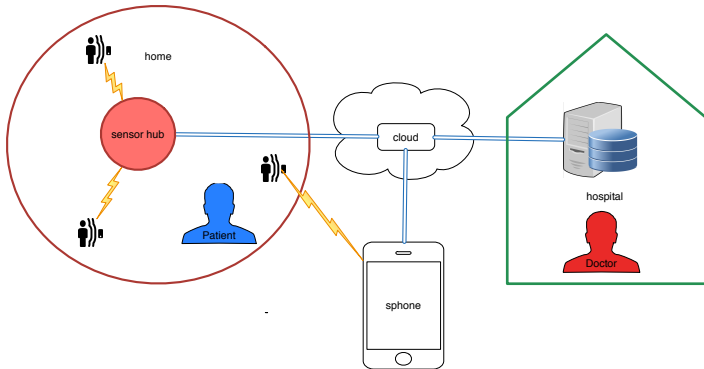
- Compiler IoT language $\mapsto$ BIP
- Attack trees to monitor generator
- BIP plugin for Plasma (Statistical MC)



GDPR compliance (MU)

Data protection by design

- User must always be able to see, change, and delete personal data
- Data protection at level of global architecture necessary



SUCCESS: Achievements, Challenges, Roadmap

- Achievements
 - Pilot infrastructure
 - Pilot architecture
 - Attack tree analysis
- Roadmap/Vision:
 - S&P-certified IoT Healthcare monitoring system
 - Reproducible 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