SUCCESS
SecUre aCCESSibility for the IoT

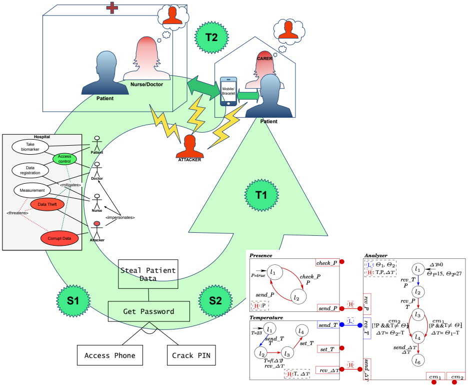
Florian Kammüller

Middlesex University London

October 24, 2016

CHIST-ERA (EU) project SUCCESS

SUCCESS SecUre aCCESSibility for the internet of things (IoT)



- Formal design of privacy-critical IoT scenarios
- Risk visualisation by attack trees
- Certified implementation for IoT component architectures
- IoT Pilot scenario: sensor based monitoring for dementia patients

SUCCESS: Fact Sheet

- Budget **700 K** Euro, Duration **36 months**
- Middlesex University London (**300 K**)
  - **PI and co-ordinator** F. Kammüller,
  - Co-PIs: Juan Augusto, Richard Bayford, Simon Jones
  - Team member: Taolue Chen
- Netherlands, (**200 K**)
  - University of Twente, Marielle Stoelinga
- France (**200 K**)
  - Inria Rennes, Axel Legay
  - Inria/ENS Paris, Albert Cohen
  - Verimag Grenoble/Université GRA, Saddek Bensalem

SUCCESS: Abstract

The IoT enables using smart devices, like smart-watches, smart wristbands, and smartphones, to provide cost-effective services for humans, for example, for low-cost monitoring schemes in the health-care sector to provide early diagnosis of diseases. From a security and privacy perspective, the IoT could be described as a hopeless case since all prevention aspects of security (confidentiality, integrity, and availability) are inherently weak and unwanted tracking and monitoring throws the doors wide open to privacy attacks. To provide secure IoT solutions, modeling and analysis needs to be integrated in the planning and validation of application scenarios and smart-device architectures to address burning security issues like unintentional or intentional insider attacks. The more so, we need to look at how to represent humans and the ways they interact with systems, and make security risks understandable for humans and secure IoT solutions accessible.

SUCCESS: Goals

- To provide logical specification and analysis methods for organisational security and integrate them with risk and fault tree analysis,
- To extend quantitative attack tree analysis and decentralized access control for IoT component systems by generalizing security models to include smart devices,
- To design and prototypically implement certification methodology for IoT component frameworks,
- To build and test user-aware security of an IoT pilot scenario from the healthcare sector of a sensor based monitoring architecture for dementia patients with security critical data and actions.