Master

Datenschutzbewusste Systeme in industriellen Umgebungen

Privacy-Aware Systems in Industrial Ecosystems

Motivation

A main problem for IT service providers is to avoid data breaches and provide data protection. Article 25 of Regulation (EU) 2016/679 refers to Privacy by Design (PbD). PbD implies the design of a system must be analyzed with regard to privacy preferences and, where necessary, be improved to technically support privacy and data protection.

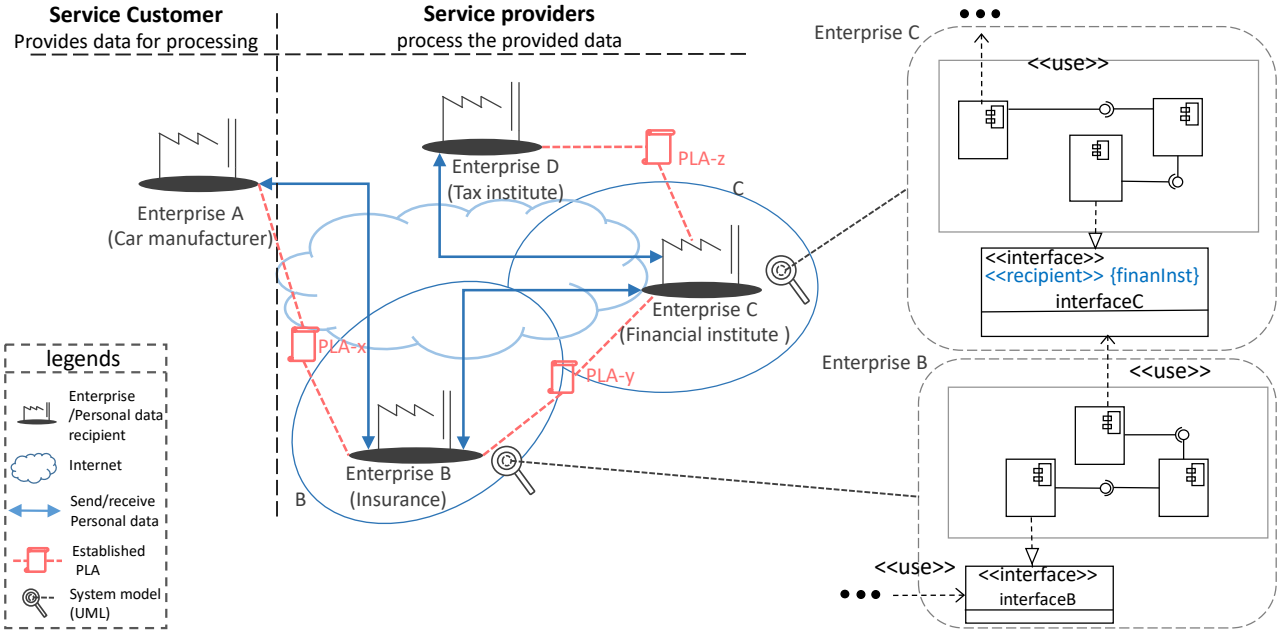

Abbildung 1: Model-based privacy analysis in Industrial Ecosystems

System-level privacy analysis is particularly challenging in today's digital society, where industrial ecosystems play a key role. Specifically, an enterprise may depend on or cooperate with other enterprises to provide an IT service to a service customer. For instance, consider Figure 1. An enterprise as a service customer of an insurance enterprise may send personal data of its employees to the insurance enterprise to issue health insurance contracts for them. The insurance enterprise must assess the solvency of the employees before issuing an insurance contract. Therefore, the personal data of each employee will be transmitted to a financial institute for the relevant assessments. Performing a privacy analysis on such a system's design requires analyzing the relevant components of the insurance enterprise, and the financial institute; and the respective interfaces between the components.

In several cases data (at least at beginning) are not consider as personal data, but later risks for the privacy of individuals or for group of discrimination based on such data became apparent. For such data, the term *privacy-relevant data* has been used. For instance, consider the sensors that are embedded in car seats (Figure 2). Such sensors are designed to increase the ergonomic aspects of a smart car. However, they may reveal physiological information of the car's driver by transmitting her/his weight average. Based on this consideration, different categories of data must be analyzed in industrial ecosystems concerning privacy.

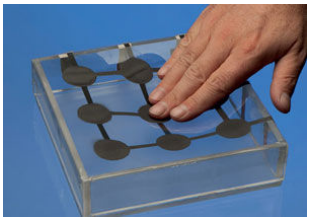

Abbildung 2: Car seat sensors

Tasks/Goals

The tasks that must be supported in this thesis are listed in what follows:

- Researching different categories of sensitive data.
- Analyzing system models to verify if privacy preferences and legal requirements are supported.
- Identifying privacy threats in industrial ecosystems.
- Identifying privacy risks in industrial ecosystems.

Remarks

The opportunity to cooperate in writing research paper after the successful submission of the thesis will be provided.

Relevant Research Projects

- IIP-Ecosphere Project: Next Level Ecosphere for Intelligent Industrial Production[1].
- DataPorts Project: A Data Platform for the Connection of Cognitive Ports[2].

Organizational

Kontakt/Contact:
Dr. Amirshayan Ahmadian (ahmadian@uni-koblenz.de)

[1] https://www.iip-ecosphere.eu
[2] https://dataports-project.eu