PhD-Privacy4Smart:
Privacy and Security for Smart Environments

Christian Johansen **Olaf Owe**
ConSeRNS and IoTSec

The Internet of Things (IoT) is the network of physical devices that embed sensors, electronics, software, and network connectivity that enables them to collect and exchange data about their operation and environment, and be remotely controlled. IoT as a field of study addresses the move towards a sensor-driven infrastructure for automated processes where standardized interfaces connect cheap sensors with networks, service platforms, and applications. IoT supports emerging applications such as intelligent transportation, smart homes, smart cities, and smart power grids, where this project is placed. Data created by IoT-enabled devices in the home, at work, or while moving, generates however privacy challenges. These challenges are often related to physical access such as location, communication network such as through Internet, and big data for user profiling. The privacy aspects are often of a totally new nature, especially in the smart house.

The proposed project will be central in the ongoing development of the project IoTSec towards Smart Infrastructures in e.g., Future Homes, and will complement the other efforts by the project. The current PhD topic will focus on development of privacy-aware models and measures as well as on technologies for semantic provability and ontologies for Smart environments.

Semantic Technologies proved of great use in other areas such as medicine. Semantic languages like OWL and SWRL are used for defining ontologies of specific terminology concepts and relationships between concepts, like “part of” or “relate to”, “child of”, “influences”.

1. One Objective of this project is to look at such semantic languages and logics and how they could be used to model privacy aspects in the new services coming inside the Smart Environments like Smart Home, Smart Grid, or Smart Transportation. Related semantic tools, such as Protege are used to infer and derive new relationships and concepts from the defined ontologies, e.g. on semantic privacy.
2. The second Objective will be to investigate relationships and automated tools for integrating Ontology models with programming language models and reasoning. We expect two-way interactions: both encoding an ontology into typing systems as well as requests from the type inference engines to the Ontology reasoner for powerful inferences to be used by the compilers or runtime execution engines.
3. The third Objective is to relate the semantic model with privacy-awareness, e.g. allowing users to select application related privacy levels or policies. Current research only focuses on protocols for configuration of smart infrastructures.

Sensors have been in use for a while but adding connectivity to the internet has given life to sensor and making it much more powerful. According to Gartner, IoT will include 26 billion installed units by 2020 and will transform the data centers. That means it is vital that IoT units must be manageable and information that they produce would respect user privacy.

However, there are numerous challenges on reliability of IoT devices. There have been a number of players in this market. For instance, there are several vendors for Home Automation Systems like DEFA, Honeywell, VSSafety, Zipato, Nest, HomeMatic, etc. Most of the home automation devices are controlled through gateway. Gateway sends and receive information through interconnected devices using wireless technologies like ZigBee or wifi. This project will also implement prototypes for Home Gateway and simulate them as home automation system.

Several frameworks and APIs are available enabling the devices to communicate with each other and pass information between gateway and cloud. But how secure are those activities? Are they vulnerable? Do they preserve the users' data from being misused? How confidently can we say that the IoT system does what we want? Until now we have not found any vendors who provide measurable indication saying how privacy preserving their services are. These questions need to be answered beforehand. We should be able to measure these factors, so that people from all sectors can easily understand grades of privacy of information from a given system or application. Whilst encountering with several Home Automation System vendors, we had the issues with reliability at times as gateways have shown unexpected behaviors and states.

Collaborations:

- Chalmers University
- Ecole Politechnique Paris
- IoTSec.no project members and international partners