



WP1

Semantic System Description

by Olaf Owe (UiO)

- **Olaf Owe** (PMA group leader, leader Conserns)
- **Christian Johansen** (50% IoTSec), senior researcher (UNIK + UIO)

Postdocs/researchers hired at UiO

- **Ming-Chang Lee “Leo”** (hired 6 month until 1.7.16, then at Simula)
- **Toktam Ramezani** (hired from 1.8.16)

PhD students hired at UiO

- **Elahe Fazel** (hired from 1.1.17)

Other members from PMA and ConSeRNS are associated.

Major Achievements



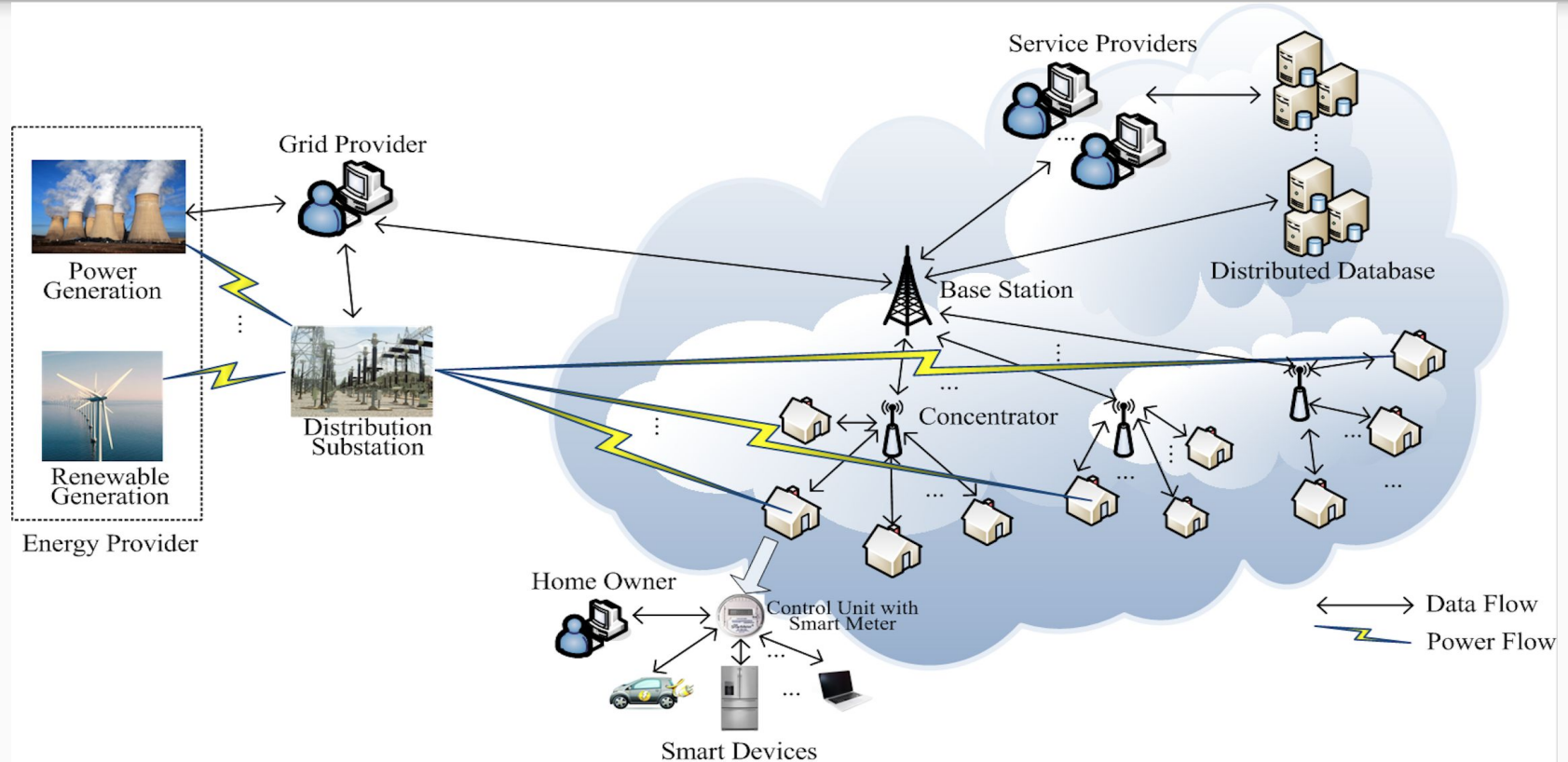
- T.1.1 Semantic description of infrastructure, attack detection, system view
 - **Semantic Modeling** of Smart Homes and Smart Grids: *Formal, executable* modeling
 - i. (Full) *Maude* model. Purpose: adaptability, abstraction mechanisms, intrusion detect.
 - Owe: Maude prototype of smart grids/homes + analysis of undesired attacks
 - ii. ABS modeling. Purpose: Compare different cloud solutions at an abstract level
 - Lee&Owe: Smart home modelling + ABS prototype
 - “Semantic Modeling of Smart Homes in the ABS Real-time modeling language”. IFI res. report 457
 - iii. Language-based security: Secrecy policies in “**SeCreol**”. Enforcement of secrecy.
 - Ramezani&Owe: NWPT’16 + paper in progress
 - [A Secrecy-Preserving Language for Programming of Object-Oriented and Distributed Systems](#) ^{NWPT}
 - **Static detection** of attacks and system weaknesses.
 - i. McDowell&Owe: Flooding detection NWPT’15 + invited journal paper (in review)
 - ii. Ramezani&Owe: Information flow analysis, attack detection and information leakage

Major Achievements



- T.1.2 Measurable security, privacy and dependability, metrics
 - Work by UNIK led by Seraj Fayyad and Josef Noll
 - i. The multi-metrics methodology from IoTSec is included as one of the technological building blocks in the SCOTT project (ECSEL JU), involving 56 partners from 12 countries.
 - ii. Multi-Metrics Framework for measurable security (concept established)
 - Publications:
 - i. Principles of Multi-Metrics approach in Journal paper [1]
 - ii. Critical dependencies of components addressed through novel method [2]

Illustration from case study: ABS model



- **Project Applications based on IoTSec :**
 - Cooperation with the energy group at UiO (Vitenberg/Eliassen). CPS Lab.
 - Safety of IoT systems (by PMA)
 - Cooperation with Chalmers U., Liverpool U., and ITU Copenhagen among others.
 - Coordinated by IoTSec members (Owe), with international collaborators from UK, DK, SE.
- **Cooperations:**
 - **Papers** with coauthors from U. of Darmstadt, U. Braunschweig, ITU. Copenhagen, Chalmers U., U. Torino, and SIRIUS centre at UiO
 - **Guest lectures** from Chalmers, Copenhagen, Bristol, INRIA-Paris industry
 - Cooperations with groups: ConSeRNS (IFI strategic initiative), Shukun Tokas
 - And with other Norwegian Institutions: HiØ via Dang Ha The Hien and Roland Olsson
 - Plans for H2020 application, including industries from the networks of the collaborators.

Ongoing work



- Defining a **framework** for modeling and analysis of secrecy and privacy in distributed OO systems, suitable for IoTSec (and smart grids/homes).
 - Based on the Creol language, adding features for secrecy
 - Developing **static** and **dynamic detection** of attacks
 - Planned **implementation** in the K framework (G.Rosu group at UIUC)
 - Persons: Ramezani, Fazel, Tokas, Johansen, Owe, Noll, Fayyad, et al.
+ MSc students (ca. 5)
- Continue cooperation with Chalmers U., U. Copenhagen, U. Bristol, industry

Research challenges:

- **Language-based security** frameworks for IoT systems
 - Formal semantics
 - Adaptivity
 - Security analysis, formal and tool-oriented methods
- **Cloud solutions** for storage of user data & **privacy** issues
 - Openness and access for 3rd party companies
 - Subscription, information Filters and encryption
- **Virtual machines** and Operating system level security issues
 - IoT applications

Industry challenge: make use of modeling and analysis tool on prototypes

Suggestions to funding agencies



- Modeling of IoT and smart infrastructures
 - Executable modeling and tool-based analysis
 - Useful at an early phase
 - Gives better foundation for services
 - Existing frameworks can be improved (and specialized to IoT and privacy)
 - Use of embedded models in IoT systems -- better flexibility
- Topics related to smart infrastructures.
 - International standardized of security-related case studies
 - [Common Weakness Enumeration and National Institute of Standards Technologies](#)
 - Further investigations on:
 - Vulnerabilities
 - Weaknesses
 - Attacts

List of Publications related to WP1



[1] J. Noll, I. Garitano, S. Fayyad, E. Åsberg, H. Abie, "Measurable Security, Privacy and Dependability in Smart Grids", Journal of Cyber Security, 3_4, (2015)

[2] S.Fayyad and J.Noll. "Components Interconnection Consideration In Multi-Metrics Approach", CENTRIC 2015