High level view on IoTSec

Christian Johansen
Ifi & ITS, UiO
christi@ifi.uio.no

Josef Noll
ITS, UiO
josef@unik.no
National initiative for a more secure future in IoT
IoTSec.no - Security for IoT for Smart Grids

The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

«Open World Approach» everything that is not declared closed is open

Partners and Collaborations

- UiO
- UNIK
- NR
- Simula
- NTNU

Academia

- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

Industry

- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet

Interest Org.

- EyeSaas
- mnemonic

Industry

- Mondragon Unibertsitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo

International

- H2020 and ECSEL projects
Security in IoT - our promises

- Semantic system description
  - Understanding the system and describing security through security functionality
  - Measurable security - the novel security concept
- Security modelling
  - Development of privacy-aware models and measures
  - Adopting and enhancing adaptive security for system of systems
  - Formal languages for semantically proving signalling
- System versus Goal analysis
  - Application-specific security/privacy, e.g. billing vs
  - Human/technical interface, security usability
- Operational security for IoT-based critical infrastructure
  - IoTSec ecosystem -> extended network
  - Roadmap for Smart Grid Security Centre (SGSC)
  - (Gap Analysis of security methods for critical infrastructures)
High level view of Security in IoT

- **Goal**
  - Provide the means for IoT security
    - from todays attack to tomorrows design
    - security thinking in organisations
- **Trust in Things**
  - Privacy label
- **Smart Grid Security Centre**

facilitated through:

- **Accountable security:**
  - Assessment
  - Modelling
  - Framework
  - Meas. Security

our basis:

- **Security and Privacy Functionality**

Smart Grid Security Centre

Privacy Label

Security classes & System design

- **Security** classes & System design

- **Privacy** Label

- **Trust in Things**
  - Privacy label

- **Elahe**
- **Manish**
- **Adam**
- **Christian**
- **Heidi**
- **Olaf**
- **Toktam**
- **Habtamu**
- **Seraj**
- **Elahe**
- **Josef**
- **Håkon Øivind**
Security and Privacy Functionality

- Security Technology
- Operations Security
- Human Resource Security
- Development, Maintenance, and Audit
- Physical and Environmental Security
- Decommissioning
- Access Control
- Privacy Protections

References:
- Future-proofing the Connected World - Cloud Security Alliance, 2016
Security Classes and System design

- **Security Class in IoT**
  - Consequence
  - Exposure

- **Consequence**
  - as in risk map

- **Exposure**
  - Physical exposure
    - people, building, physical ports,…
  - IT exposure
    - ports, firewall, connectivity

- **Used to assess the security class of Systems, sub-systems and components**

---

### New postulate of security class

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
<th>Class 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Class 5</td>
<td>Class 5</td>
<td>Class 4</td>
<td>Class 4</td>
<td>Class 5</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
<td>Class 2</td>
<td>Class 2</td>
<td>Class 2</td>
<td>Class 2</td>
</tr>
<tr>
<td>2</td>
<td>Class 2</td>
<td>Class 2</td>
<td>Class 2</td>
<td>Class 2</td>
<td>Class 2</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 1</td>
</tr>
</tbody>
</table>

**Security Class**

**Exposure**
Semantic attribute based access control (S-ABAC)

- Lifting the security class through S-ABAC
- Access to information
  - who (sensor, person, service)
  - what kind of information
  - from where
- Attribute-based access
  - role (in organisation, home)
  - device, network
  - security tokens
- Rules inferring access rights

Attributes: roles, access, device, reputation, behaviour, ...
Methodology: From System description to SPD level

- **System**: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- **Sub-systems**: AMR consists of power monitor, processing unit, communication unit
- **Component**: AMR communication contains of a baseband processing, antenna, wireless link
- **Configuration Parameter**: Wireless link: \( f = 868 \text{ MHz} \), output power=? , Encryption=?

### Methodology Diagram

<table>
<thead>
<tr>
<th>System/Sub-system</th>
<th>Components and functionalities</th>
<th>Could be</th>
<th>SPD Components, SPD functionalities</th>
<th>Metrics description (SPD functionality)</th>
<th>define config. parameters and SPD values in Metrics</th>
<th>Run SPD Multi-metrics analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is made by</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Could be</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Components and functionalities</td>
<td>SPD Components, SPD functionalities</td>
<td>Metrics description (SPD functionality)</td>
<td>define config. parameters and SPD values in Metrics</td>
<td>Run SPD Multi-metrics analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

IoTSec.no  #IoTSecNO

High level view on Security for IoT  Nov 2017, Chr. Johansen, J. Noll
Accountable security

- **Assessment**
  - Comparison desired Class vs Calculated class
  - PROSA modelling

- **Modelling**
  - SPD Metrics, from criticality to SPD value

- **Framework**
  - Examples of applicability

- **Measurable Security**
  - Security is not 0/1

Measurable criticality

<table>
<thead>
<tr>
<th>SPD level</th>
<th>SPD vs SPDGoal</th>
</tr>
</thead>
<tbody>
<tr>
<td>(67,61,47)</td>
<td>(○,○,○)</td>
</tr>
<tr>
<td>(67,61,47)</td>
<td>(○,○,○)</td>
</tr>
<tr>
<td>(31,33,63)</td>
<td>(○,○,○)</td>
</tr>
</tbody>
</table>
Mission Statement

We help the Utility Companies achieve their smart grid goals with higher resiliency and quicker response times against security threats.
Privacy Labelling
http://PrivacyLabel.IoTSec.no

- “Measure, what you can measure
  - Make measurable, what you can’t measure” - Galileo
- Privacy today
  - based on lawyer terminology
  - 250.000 words on app terms and conditions
- Privacy tomorrow
  - A++: sharing with no others
  - A: …
  - C: sharing with ….
- The Privacy label for apps and devices

In collaboration with Consumer Services (Forbrukerrådet)
- Paul Chaffey (Statssekretær) support
- Finn Myrstad (Forbrukerrådet) -> EU

Appfail Report - Threats to Consumers in Mobile Apps

The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to discover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.
DIGITALEUROPE’s views on Cybersecurity Certification and Labelling Schemes

Brussels, 23 March 2017

RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security certification framework for ICT products and 2) a “Trusted IoT label” giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

2. Trusted IoT Label

In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.
IoTSec - Conclusions

- **IoTSec from a helicopter perspective**
  - overall vision broken down into activities
  - measurable achievements

- **Example Smart Home**
  - positive surveillance
  - privacy-aware
  - including neighbours, family, friends

- **Impact**
  - more secure IoT
    - security classes
    - security and privacy ontology
  - competitive advantage e.g.:
    - privacy label

<table>
<thead>
<tr>
<th>Impact/Exposure</th>
<th>Class 1</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 2</td>
<td>Class 2</td>
</tr>
<tr>
<td>2</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
</tr>
<tr>
<td>3</td>
<td>Class 4</td>
<td>Class 4</td>
<td>Class 4</td>
<td>Class 4</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
<td>Class 4</td>
<td>Class 5</td>
<td>Class 5</td>
</tr>
<tr>
<td>5</td>
<td>Class 5</td>
<td>Class 5</td>
<td>Class 5</td>
<td>Class 5</td>
</tr>
</tbody>
</table>

New postulate of security class

- Development and Implementation
- Security Technology
- Operation
- Update
- End-of-life
- Monitoring
- Physical Access
- People

14 New postulate of security class
The “sharing economy” for energy companies?

IKT er den nye oljen! | Sigve Brekke
[Source: aftenposten.no]

Sharing Economy: “Telenor will create a digital ecosystem in Pakistan”

Prosumer bidding and scheduling in electricity markets
[Source: eSmartSystems.com]