Collaboration for a more secure Smart Grid operation

Josef Noll, Christian Johansen
UiO
IoTSec Project leader/COO
jnoll@uio.no, christi@ifi.uio.no
IoT - how will it influence us?

Think about how Internet has changed your life within the last 10 years.
IoT - how will it influence us?

Think about how Internet has changed your life within the last 10 years.

Multiply by three, and cut down to 5 years!
IoT - how will it influence us?

Think about how Internet has changed your life within the last 10 years.

- Faster
- More difficult to understand
- Autonomous
- Less secure?

Multiply by three, and cut down to 5 years!

Sustainable?
- Waste, CO2
- Energy
- Noise

2

Security through collaboration

Feb2017, Josef Noll
IoT - how will it influence us?

Think about how Internet has changed your life within the last 10 years.

- Faster
- More difficult to understand
- Autonomous
- Less secure?

Sustainable?
- Waste, CO2
- Energy
- Noise

Multiply by three, and cut down to 5 years!
National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grids

IoT in operations

IoT in operations

Admin Cloud

GSM/LTE
National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grids

IoT at home

GSM/LTE

Admin Cloud

IoT in operations

"Open World Approach" everything that is not declared closed is open
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 2013 to promote the development of a safe and secure interconnectedthings (IoT) enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) in order to be a safety information society.

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

Everything that is not declared closed is open

«Open World Approach»

Partners and Collaborations

- UoA
- UoB
- NKT
- NTNU
- IIA
- Smart Innovation District
- eSmart Systems
- Fredrikstad Energi
- Gisle Engennett
- Midatlan
- EyvindAS
- INFOSYS
- CERN
- Heros

Interest Org.

- Mondragon Unibertsitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimir
- H2020 and ECESEL projects
- Academic Collaborators

International

Academia

Admin

Cloud

GSM/LTE

IoT in operations

IoT at home

Kjeller

Oslo

Gjøvik

Halden

"Open World Approach" everything that is not declared closed is open
Future Service Requirements (in a wireless infrastructure)

- “we have no control of what is going on in Wifi”
- “only 25% of broadband customers experience the speed they got promised”
- more than 75% of all calls to ISPs is related to wireless
- over 90% of boxes sent to ISP are fully functionable
Future Service Requirements (in a wireless infrastructure)

- “we have no control of what is going on in Wifi”
- “only 25% of broadband customers experience the speed they got promised”
- more than 75% of all calls to ISPs is related to wireless
- over 90% of boxes sent to ISP are fully functional
Future Service Requirements (in a wireless infrastructure)

- “we have no control of what is going on in WiFi”
- “only 25% of broadband customers experience the speed they got promised”
- more than 75% of all calls to ISPs is related to wireless
- over 90% of boxes sent to ISP are fully functional

Access and Control

Service requirements

- readMaxProvision
- readTotalProvision
- switchOffHeatPump
- drainBattery
- chargeBattery

Token

- authenticatedPerson
- owner

Person

- Bob
- Alice, George, Carol

Semantic access control

- hasAttributes
- canOwn

Security through collaboration
Scientific focus and achievements

- Semantic system description
  - Understanding the system and describing security through security functionality
  - Measurable security - the novel security concept

- Security modelling
  - Privacy-aware models and measures
  - 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
  - Smart Grid Security Centre (SGSC)
  - (Gap Analysis of security methods for critical infrastructures)
Opportunities

- Monitoring the grid to achieve a grid stability of at least 99.96%.
- Alarm functionality, addressing:
  - failure of components in the grid,
  - alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
- Future services:
  - Monitoring of activity at home, e.g. "virtual fall sensor"
- Monitoring the grid to achieve a grid stability of at least 99.96%.
- Alarm functionality, addressing:
  - failure of components in the grid,
  - alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
- Future services
  - Monitoring of activity at home, e.g. "virtual fall sensor"

Opportunities

- Stop and reduce power consumption
- Standardised interface (API)
- Monitoring the grid to achieve a grid stability of at least 99.96%.
- Alarm functionality, addressing:
  - failure of components in the grid,
  - alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
- Future services
  - Monitoring of activity at home, e.g. "virtual fall sensor"

**Students Corner of IoTSec.no**

**Topics for Master Thesis related to IoTSec**
- *Integrating Energy Devices through BasicIoT (Editor: Svein Norsk Hau)*
- *Privacy labels for IoT consumer products (Editor: Linn Einna Paulsen)*
- *Security challenges of low-capacity access will be editor: (Naj Ahmed Kadah)*
- *Measurable Security for Sensor Communication in the Internet of Things (Editor: Zayid Shah)*

**Finished Master Thesis related to IoTSec**
- *Pervasive computing in smart electricity grid (Supervisor(s): Christian Johansen, Josef Noll, Trend Aalberg)*

---

**Monitoring the grid to achieve a grid stability of at least 99.96%**

**Alarm functionality**
- Failure of components in the grid
- Alarms related to the Smart Home, e.g., burglary, fire, or water leakage

**Intrusion detection**
- Monitoring both hacking attempts to the home as well as the control center and any entity in between

**Billing functionality**
- Providing at least the total consumption every hour, or even providing information such as max usage

**Remote home control**
- Interacting with the heating system

**Fault tolerance and failure recovery**
- Providing a quick recovery from a failure

**Future services**
- Monitoring activity at home, e.g., "virtual fall sensor"
“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 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
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 issued a report "Potential threats to consumer protection hidden in the end user terms and privacy policies of apps"
Collaborate to answer the questions

- Smart Meter
  - read and control
    - soft switch, remote switch off
  - logic?

- Challenges
  - Logic: Centralised ↔ Fog
  - Smart Meter: Information ↔ Control
  - Smart Grid Information ↔ Internet Info

from criticality

to measurable: security, privacy and dependability

<table>
<thead>
<tr>
<th>SPD level</th>
<th>SPD vs SPD$_{ideal}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 61.47)</td>
<td>(0, 0.0)</td>
</tr>
<tr>
<td>(0, 61.47)</td>
<td>(0, 0.0)</td>
</tr>
<tr>
<td>(31, 33.63)</td>
<td>(0, 0.0)</td>
</tr>
</tbody>
</table>
Collaborate to answer the questions

- **Smart Meter**
  - read and control
    - soft switch, remote switch off
  - logic?

- **Access control**
  - access to read, control, configure
  - based on attributes (network, position, ...)

- **Rules and policies**

- **Challenges**
  - Logic: Centralised ↔ Fog
  - Smart Meter: Information ↔ Control
  - Smart Grid Information ↔ Internet Info

### Challenges

- Logic: Centralised ↔ Fog
- Smart Meter: Information ↔ Control
- Smart Grid Information ↔ Internet Info

---

**Criticality**

- Ideal
- Good
- Acceptable
- Critical
- Failure

---

**Access control**

- read, control, configure
- based on attributes (network, position, ...)

**Rules and policies**

**Measurability**

**.to measurable: security, privacy, and dependability**

- SPD level
- SPD vs SPD

- (0-61.47) (0.6, 0.0)
- (67.0, 61.47) (0.0, 0.0)
- (31.33, 63.3) (0.0, 0.0)
Collaborate to answer the questions

- Smart Meter
  - read and control
    - soft switch, remote switch off
  - logic?

- Challenges
  - Logic: Centralised
  - Smart Meter: Information
  - Smart Grid Information
  - Fog
  - Control
  - Internet Info

- Access control
  - access to read, control, configure
  - based on attributes (network, position, ....)

- Rules and policies

- Measurability

IoT security challenges

- Mirai attack
  - “security by obscurity”
  - different security viewpoint
  - “it is just the beginning”

Challenges

- Logic: Centralised
- Fog
- Smart Meter: Information
- Control
- Smart Grid Information
- Internet Info

from criticality

to measurable: security, privacy and dependability

<table>
<thead>
<tr>
<th>SPD level</th>
<th>SPD ± SPD_trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,01/4,47</td>
<td>0,0 ± 0,4</td>
</tr>
<tr>
<td>0,01/4,47</td>
<td>0,0 ± 0,4</td>
</tr>
<tr>
<td>0,01/4,63</td>
<td>0,0 ± 0,6</td>
</tr>
</tbody>
</table>

21 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack on Dyn, an Internet infrastructure company that provides critical technology service to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Vonage.