Measurable security and privacy for the Internet of Things (IoT)
“Our Journey of Today”

- “The last time we were connected by wire was at birth!” [Motorola]
  - Wireless is everything
  - The Internet of Things (IoT) challenges

- Smart Grid, Smart Homes, Smart Infrastructures
  - Scalability in IoT
  - Measurable Security & Privacy - IoTSec.no
  - Logic, Cloud,

- “Some meat for discussion”
  - Privacy labelling
  - Basic Internet Foundation
4G and disruptive technologies

Josef Noll
Researcher, Telenor R&D, N-1331 Fornebu
Prof. stip., Univ. graduate studies, UniK, N-2027 Kjeller
josef@unik.no

what has happened in the last 11 years?

and what is my vision for 2026?
Reality in 2016: Bad indoor coverage

- Telenor will solve challenges of indoor coverage
  - Voice over Wifi (VoWifi)
  - Voice of LTE (VoLTE)
The world of 2016

- Interference-limited Wifi
  - increased demand on customer services
  - “meaningless discussions” on “Wifi”
- Operators in the need of becoming “Digital Companies”
  - Revenue, Investors?
  - Digital Ecosystem: Identity, Federation
- 5G dilemma
  - revenue versus costs
  - network infrastructure (core vs access network costs)
- Societal challenges
  - Energy, Health, “Internet for all”
  - Security, Privacy, “Digital Societies”

Wifi at “Legevakten” Feb2011
Addressing the Threat Dimension for IoT

- Hollande (FR), Merkel (DE) had their mobile being monitored.
- «and we believe it is not happening in Norway?"
Example: Smart Grid Infrastructure

- **Smart Meter (customer home)**
  - connected via mesh or directly
  - proprietary solution (433, 800 MHz band, power line)
- **Collector**
  - collects measures
  - communicates via mobile network
- **Mobile Network**
  - as a transmission network
- **Cloud (Provider)**
  - entry point for remote access
  - Application platform
Future Smart Grid operation, § 4-2 functional requirements

1. Store measured values, registration frequency max 60 min, can configure to min 15 min.
2. **Standardised interface (API) for communication with external equipment using open standards**
3. Can connect to and communicate with other type of measurement units
4. Ensures that stored data are not lost in case of power failure
5. **Can stop and reduce power consumption in every measurement point** (exception transformator)
6. Can send and receive information on electricity prices and tariffs. Can transmit steering information and ground faults
7. Can provide security against miss-use of data and non-wished access to control-functions
8. Register flow of active and re-active power flow in both directions

---

"Forskrift om måling, avregning, fakturering av nettverk..."

AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,
b) ha et standardisert grenseinni som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,
c) kunne tilnyttes og kommunisere med andre typer målere,
d) sikre at lagrede data ikke går tapt ved spenningsavbrudd,
e) kunne bytte og begrense effektuttalet i det enkelte målepunkt, unntatt trafomtale anlegg,
f) kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordekstal,
g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og h) registrere flyt av aktiv og reaktiv effekt i begge retninger.

Norges vassdrag- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

0  Tilløyd ved forskrift 16 jan 2012 nr. 75 (i kraft 20 jan 2012).

https://lovdata.no/dokument/SF/forskrift/1999-03-11-301
Application Scenarios for Smart Meters

- 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”
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

Academia
- UiO
- UNIK
- NR
- Simula
- NTNU

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

Interest Org.
- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet
- EyeSaaS
- mnemonic

International
- Mondragon Unibertsitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo
- H2020 and ECSEL projects
Topics for potential Master Thesis?

Please be welcome to the Student Corner for Security and Privacy in the Internet of Things (IoT).
Feel free to have a look at UNIK4750 course related to the project.

Ongoing Master Thesis related to IoTSec

- Smart Meter Security Analysis (Editor: Christian Resell, Hans Jørgen Furre Nygårdshaug, Mehdi Noroozi)
- The human aspect in Smart grids (from Security and Privacy point of view) (Editor: Linn Eirin Paulsen)
- Pervasive computing in smart electricity grid (Editor: Kaniz Fatema Tuly)
Upcoming Infrastructure

- **Smart Meter**
  - read and control
  - logic?

- **Smart Home**
  - intelligent devices
  - on-demand regulation

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

from criticality

<table>
<thead>
<tr>
<th>SPD level</th>
<th>SPD vs SPD_{Goal}</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>
Towards Measurable Privacy - Privacy Labelling

- “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

---

Appfail Report - Threats to Consumers in Mobile Apps

The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.
Addressing the challenges of IoT connectivity

**Device ownership**
- who owns the device
- which data are going to whom
  - maintenance

**Easyness Setup**
- 1. step ownership
- take control

**Scalability**
- business model for SIM/device not scalable
- free wireless for IoT data
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
Motivation
“Need to close the digital gap”

- The Global Goals: Norway is the secretariat for Quality Education
- Internet history
  - 1973 Europe through Kjeller
  - 1994 Opera Software
  - 2014 Basic Internet Foundation

“I'm currently learning Python and HTML, so I can make a website for my parents’ business”
The vision of 2026

- “Digital and Inclusive Society”
- Networks adopting to service needs
  - Security, privacy, dependability
- “the Road Network Infrastructure”
- Low-capacity Internet
  - free and open access
- Broadband services
  - authenticated access

WWRF vision for 2017; “7 trillion wireless devices serving 7 billion people by 2017”,
Conclusions

- Internet of Things (IoT) is a game changer
  - Everything is wireless: Smart Infrastructures
  - Autonomous systems, Critical Infrastructure
- Collaborative approach for a (more) secure society
  - Trust is not enough, need for measurable
  - Partnership for security: threats, measures, counter activities
- Measurable Security and Privacy for IoT
  - IoTSec.no - Security for Smart Grid
  - Industrial impact: Security Centre for Smart Grid
  - Privacy labelling for apps and devices
- Innovation ecosystem for the IoT
  - Reducing the digital gap
  - Providing Basic Internet to everyone