Hvilke muligheter kan skapes i norsk og global sammenheng med basis i IoT?

Josef Noll
Department of Technology Systems, University of Oslo
m: +47 9083 8066, e: josef.noll@its.uio.no

IoTSec.no - SCOTT.IoTSec.no
"The last time I was connected by wire was at birth" - our when Internet of Things (IoT) meets people

- Internet has changed, IoT will accelerate
  - the ecosystem of making business
  - automated processes
- The Nordic Model - Opportunities

- Security in IoT
  - “teach our sensors to talk Norwegian”
  - The changing role of security in HMS -> HMSS
  - new paradigm: measurable security
  - security classes “design”
- related to projects:
  - Security in IoT for Smart Grids: IoTSec.no
  - Secure Trusted IoT: SCOTT.IoTSec.no
The change of Business Models

- Car industry: Liability in IoT driven business models
- Energy: Cost of providing of Energy -> Cost of Reliable Network
- Telecom: uO (MicroOperator), Partnership
Digital share of GDP (2015 - 2020)

- Today: USA, 33% GDP due to digital
- Financial Services 57% digital, Business Services 54%, Communications 47%
- 22% of global retail from digital, 28% in health, 20% in consumer goods
- Digital achievements: technology, skills, accelerators

[Source: Accenture, “Digital Disruption Growth” 2016]
Volvo to 'accept full liability' for crashes with its driverless cars

But decide on rules so we can make the dang vehicles

To secure the Internet of Things and to build trust with customers, the way that vendors approach manufacturing, distributing and supporting devices and solutions must change, a panel of security pros said Monday at the National Cyber Security Alliance's (NCSA's) Cybersecurity Summit held at Nasdaq.

"Business models will have to change. We used to build them [products], ship them and forget about them until we had to service them," said John Ellis, founder and managing director of Ellis & Associates. "We've moved to a new world where we have to ship and remember."
The “sharing economy” for energy companies?

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

Prosumer bidding and scheduling in electricity markets

[Source: eSmartSystems.com]

[Source: aftenposten.no]
Automated processes

- Work force demand
- Blockchain, IOTA
- The state business model
The challenge from automation

USA work force time spent [%]

- Predictable physical work: 18%
- Data processing: 7%
- Data collection: 14%
- Stakeholder interactions: 16%
- Applying Expertise: 17%
- Managing others: 12%

Technical automation potential 2016 [%]

- Predictable physical work: 78%
- Data processing: 69%
- Data collection: 64%
- Unpredictable physical work: 25%
- Stakeholder interaction: 20%
- Applying expertise: 18%
- Managing others: 9%
A digital society is made of digitally-skilled citizens.

Digital Agenda Scoreboard 2015: Strengthening... 40% of Europeans don't even have basic digital skills.

Source: EU commission (2015)
Blockchain, IOTA, and automated money

- Increased security in micro-data handling
- Trust enabler for IoT data

- No trustworthy organisation backing crypto currencies
- US$ covered by U.S. Department of Justice, U.S. Treasury, the Federal Reserve
  - centralized digital currencies
Summary of discussion [Kåkå festival 2017]

- Skattesystem:
  - data kontrolle forsvinner -> penger forsvinner
  - digital kompetanse: “Internet light for all”?
  - styreforhold: industri vs politikk

- Framtidens fordeling av inntekter
  - god lønn til toppene, luselønn til arbeidere

- Tidligere: 50% av jobber for ufaglærte, nå bare 10% av jobber
  - re-industrialisere Norge
  - god utdannelse viktig

- “5 største teknologiselskaper hadde 950 milliard USD økning i verdi i 2016/2017 (siste 10 mnd), mer enn BNP av NO, DK, FI sammen
Addressing the Threat Dimension for IoT

- Hollande (FR), Merkel (DE) had their mobile being monitored
- «and we believe it is not happening in Norway?»

[source: Süddeutsche Zeitung, 18Dec2014]
Health, Security and Environment
Helse, Miljø og Sikkerhet

- Security affects safety
  - IoT attack -> car crashes
- Security affects core business
  - Company confidential information
  - Customer information
    - Privacy regulative (GDPR May2018): 4% of revenue

IoT is corporate governance
IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- **Answer the IoT need for a new and more advanced security paradigm through security classes**
- **Create a Convincing privacy assessment through privacy labelling**
- **Establish a clear link between security and safety**
There will be no peace until all men learn to understand each other.

True...

How are we going to get everybody to speak Norwegian?

Teach our sensors to talk Norwegian.
IoT impact for Scandinavia

- Demand
  - mobile
  - distances

- Adaptation
  - infrastructure
  - business environment
  - Trust relation

- Challenges
  - sensor industry
  - distance to Brussels
  - economy of scale
The Internet and Scandinavia

• The first connection of Arpanet outside of the USA (and Hawaii) was to Scandinavia (Kjeller, June 1973)
• List_of_Internet_pioneers [Wikipedia]
  - Yngvar Lundh, Paal Spilling
• Application development
  - .php, OpenSource, Linux, Skype, Spotify
  - OperaSoftware, FAST Search
  - Nokia, Ericsson
  - Telenor, TeliaSonera
• Mobile Internet:
  - GSM
  - Service adaptation
Conclusions

๏ Things (IoT) are driving the digital societies
๏ IoT: Business merger
  ➡ Internet + Semantics + Things = IoT
  ➡ Digitisation of the Society
๏ IoT ecosystem
  ➡ Promote the Nordic system
  ➡ Security classes, accountable security
๏ competitive advantage e.g.:
  ➡ Privacy label (A++, A+…D)
  ➡ business advantage for SMEs
Further information
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
Learn from Industrial Automation and Mobile Networks

- “What to secure?”

- Network segregation
  - Network slicing

- From Confidentiality, Integrity, Availability (CIA)

- to Availability, Integrity, Confidentiality (AIC)
Security and Privacy Functionality

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

Hardware-based Security Controls
- Use of Memory Protection Units (MPUs)
- The Microcontroller (MCU)
- Considering a Trusted Platform Module (TPM) into IoT
- Secure Physical Interfaces
- Guard the Supply Chain
- Use of Cryptographic Modules
- Use of Specialized Security Chips/Coprocessors
- Device Physical Protections
- Incorporate Physically Unclonable Functions (PUFs)
- Tamper Protections
- Self-Tests
- Trusted Platform Modules

References:


Future-proofing the Connected World - Cloud Security Alliance, 2016
The trust matrix

- trust as a positive user attitude
  - engaging voluntarily
- security based trust issues
  - building trusted systems
- technological factors
  - data storage, distribution
  - insight
- human/societal factors
  - government
  - family, friends

Trust factors:
- Security
- Privacy (social)
- Acceptability
- Usability
- Reliability
- Availability
- Maintainability
- Safety
- Integrity
- Confidentiality
- Predictability
- Reputability (social)
- Configurability (social)
- Consistency
- Functionality

http://SCOTT.IoTSec.no
http://SCOTT-project.eu
Security Classes and System design

- Security Classes 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

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 4</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 5</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 3</td>
<td>Class 4</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>

Impact/Exposure: 1, 2, 3, 4+

Increase weak security:
- watchdog
- Attribute based access control (S-ABAC)
The economic perspective

- The big 5 IT companies have a GDP as big as that of France
- Amazon largest sector in terms of revenue is selling of data
  ➡ 20% of revenue

- How can SMEs compete?
  ➡ Each service and device gets a privacy label

- Four areas for Privacy Label
  ➡ which data are collected
  ➡ sharing to my phone, my cloud, public cloud,...
  ➡ data communication integrity and storage
  ➡ further distribution of data, ownership of data, further processing

Privacy Label (A-F)
- easy visibility
- customer focus
- transparent

Privacy Label (A-F)

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

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.
Facilitator for economic growth and partnership

- We need more long-term investments
  - build infrastructure
  - enable digital services
- Long-term revenue
  - value creation
  - inclusion creates novel services
  - peer-to-peer enabler
  - supporting the low income segment
- “Creating roads” for digital services
  - free access to non-profit content: education, health, agriculture, eGov
  - mobile and Wifi hot-spots
- Done by: Jio, Amazon, Google, Alibaba

The example from India

- 1 GB per day for € ~2.1 per month
- free voice, Zero-rated cloud content
- Schools, railway stations,…
- “Revenue is not an issue. Services will come”
  [source: Jio Press Release, Jan 2018, India]