Tekna seminar “Sårbarhet i kraftsektoren”, Gardermoen, Apr2017

Hvordan ivareta sikkerhet rundt IoT enheter?

Josef Noll
josef@jnoll.net, @josefnoll, m: +47 9083 8066
Professor at University of Oslo, Department of Technology Systems
Co-Founder and Secretary General at Basic Internet Foundation
Outline

- From electricity to intelligent power
  - The Internet of Things (IoT) and the power grid
- Digitisation of the Society
  - Sensor and Data driven
  - Industry and Society
  - Your role as power provider
- Privacy and Security
  - Do we really understand the challenge?
  - Measurable security
  - Privacy labelling

Conclusions
Who is going to manage the home?
Considerations

- A variety of services
- Security and Privacy requirements
- Novel trends, flexibility
- My Home is everywhere

Securing the Internet of Things

Apr2017, Josef Noll
Digitalisation of the Society

A DIGITAL SOCIETY IS MADE OF DIGITALLY-SKILLED CITIZENS

Source: EU commission,
The Internet of Things (IoT)

- IoT =
  - Internet +
  - Semantics +
  - Things

- Tingene som snakker
  - med en datamaskin,
  - som forstår hva det dreier seg om,
  - og tar selvstendige beslutninger

How to handle security?
Traditional: Threat-based approach

- Security attribute
- Organisation
- Control/Configuration
- System of Systems
- Threat
- Vulnerability
- Severity scale

Definitions:
- Protects
- Requires
- Owns
- Implemented
- Mitigated by
- Affects
- Threatens on
- Exploited by
- Has severity

[Source: http://securityontology.sba-research.org/]

Scalability?
Future Threats?
IoT threats

• First massive attack from IoT devices
  ➡ 16Oct2016 IoT botnet attack on Dyn
  ➡ Camera (CCTV), video recorder, TV,…
  ➡ 1.2 Gbps Denial-of-Service attack

• How?
• All using Linux BusyBox for authentication
  ➡ admin - admin, root - root, admin - 1111…
  ➡ simple “test” was enough to convert IoTs into botnets

[Source: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/]
Communication & IoT for society

IoTSec.no

“Research on IoT security”
with
“The national Security Centre for Smart Grid”

http://IoTSec.no
Example: Measurable Security

- From people defined security classes
- To automated security decisions
  - through metrics assessment

- based on
  - security, privacy and dependability functionalities
Multi Metrics Assessment

- Metrics to SPD conversion
  - Parametrisation of system parameters, e.g. latency -> [ms]
  - SPD regression: «SPD value and importance for the system»
    - parameter into S,P,D value range, e.g. latency=50ms :=> (ideal, good, acceptable, critical, failure)
  - Scaling according to System Importance, e.g. latency :=> $S_{\text{max}}=30$, $P_{\text{max}}=10$, $D_{\text{max}}=20$
  - Assignment of SPD values, e.g. latency=50 ms

- Metrics combination to provide $SPD_{\text{System}}$: (60, 30, 70)
  - Mathematical combination, e.g. $S_{\text{System}}=100 - \sqrt{S_1^2+S_2^2+\ldots+S_x^2}$

Securing the Internet of Things
From System to Security Assessment

- System described through
  - Security functionality
  - Security attributes
  - Metrics converting security into [0…100]

- Automatic Meter Reader (AMR)
  - (1) remote access metric - (yes/no)
    - reading, or just controlling
  - (2) authentication metric
    - everyone, or authenticated user

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Cs</th>
<th>Cp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access ON</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Remote Access OFF</td>
<td>10</td>
<td>20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Cs</th>
<th>Cp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication ON</td>
<td>10</td>
<td>30</td>
</tr>
<tr>
<td>Authentication OFF</td>
<td>80</td>
<td>70</td>
</tr>
</tbody>
</table>
SPD$_{Goal}$ versus System-SPD$_{Level}$

- Application-based security goals
- Automated assessment

- Visualisation of “operating envelopes”
  - Security good enough?
  - Too high Security

- Critical component/sub-system assessment
Change in Business Models due to IoT

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]
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

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.
Conclusions for 2025

- Things (IoT) are driving the digital societies
- Novel services at home
  - Internet + Semantics + Things = IoT
  - Digitisation of the Society
  - Measurable Security and Privacy
  - Autonomous Decisions

- IoT Security and privacy
  - automated privacy/security through Multi-Metrics
  - Privacy label (A++, A+…D)