Security analysis of Dutch smart metering systems

Sander Keemink and Bart Roos

July 2, 2008
1 Smart metering introduction

2 Theoretical research

3 Practical research

4 Recommendations

5 Conclusion
Smart Metering goals

- Accurate billing
- Insight in energy usage
- NTA Dutch Technical Agreement
Security analysis of Dutch smart metering systems

Smart metering introduction

NTA

![Diagram of Smart Metering System]
Your energy usage

What do you see in this image?

Hour of day

Electricity  Water  Gas
“Analyze the possible impact of the use of smart metering systems on the security of electricity metering using the CIA-triad and minimum requirements as stated in the NTA-8130 regulation. Compare the NTA and a preferred situation with the smart metering systems that are currently implemented.”
Theoretical research

- Defined the need for security using the CIA-triad
- Analyzed the NTA security requirements:

<table>
<thead>
<tr>
<th>P0</th>
<th>Not defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Read-only</td>
</tr>
<tr>
<td>P2</td>
<td>Encryption allowed if interoperable</td>
</tr>
<tr>
<td>P3</td>
<td>Grid operator should take ‘appropriate measures’</td>
</tr>
<tr>
<td>P4</td>
<td>Grid operator should take ‘appropriate measures’</td>
</tr>
<tr>
<td>P5</td>
<td>Out of scope</td>
</tr>
</tbody>
</table>
- Defined possible attack vectors based on CIA-triad
Port 0 security

- Optical interface (all meters)
- Programming buttons (some meters)
- Security measures
  - Switch behind security seal
  - Tamper detection
Port 0 security

Landis+Gyr MAP120 DLMS METER TOOL [Demo Version]
Port 2 security

- **Wired**
  - M-Bus without encryption
  - M-Bus interfaces widely available
  - Simulate gas or water meter (slave)
  - Simulate electricity meter (master)

- **Wireless**
  - Proprietary protocols
  - Wireless M-Bus not being used
Port 3 security

- Communication methods:
  - PowerLine Communication (PLC)
  - GPRS
  - Ethernet
  - Radio Frequency mesh (RF)

- Risks
  - Sniffing (Serial GPRS modem and Ethernet)
  - Disrupting communications
  - Denial of Service attacks
Security analysis of Dutch smart metering systems
Practical research

Port 3 security
Port 5 security

- Risks
  - Sniffing
  - Man-in-the-Middle attack
  - Shoulder surfing for credentials
  - The usual risks

- Basic security measures
  - SSL (HTTPS)
  - Strong authentication
Welkom bij Mijn Oxxio!

Volg en controleer uw energieverbruik via Mijn Oxxio. Deze persoonlijke en beveiligde pagina hoort bij uw slimme meter. U kunt bijvoorbeeld uw verbruik per week, per maand of zelfs per jaar bekijken. Zo weet u precies wat uw verbruik was over de verschillende periodes.

Inloggen

Klantnummer: [Namenkader]
Postcode: [Namenkader]
Huisnummer: [Namenkader] zonder toevoeging

Inloggen
Recommendations

NTA:

- Aggregate data per day, week or month
- More specific security requirements in NTA
- Port 0 should be part of NTA
  - Including minimal security requirements
Supplier and grid operators:

- Do not trust security seals
- Data availability can not be guaranteed
- Use open encryption on all links
- Do not underestimate privacy aspects
- Use SSL and strong passwords on website
- Perform data checks to verify correctness of data
Conclusion

- Privacy underestimated
- NTA not specific enough about security
- Security of meter management functions not sufficient
- No secure channel between electricity and gas or water meter
- Supplier websites should improve their security
Thanks

Thanks for your attention
Any questions before enjoying your lunches?