Security and Privacy Issues in Electricity Metering

M. van Eekelen[1] B. Jacobs[2]

[1]Institute for Computing and Information Sciences, Radboud University Nijmegen
Faculty of Computer Science, Open University of the Netherlands, Heerlen

[2]Institute for Computing and Information Sciences, Radboud University Nijmegen

Govcert'09, 6/10/2009

Outline

Bart Jacobs

- Professor in computer security, at Nijmegen
- Apart from academic abstract nonsense, involved in e-government / identity managment, like biometric passports, voting, OV-chip
- Occasional role in media
- Author of online book *De Menselijke Maat in ICT*, see `www.cs.ru.nl/B.Jacobs/MM`

Marko van Eekelen

- Professor at Open University & senior lecturer at Nijmegen
- Scientific director of LaQuSo Nijmegen
  - LaQuSo = TUE/RUN cooperation for software product quality assessments
- Involved in security and privacy assessment of smart metering systems
- Invited speaker/author:
  - talk: security and privacy of AMR systems at Europe Metering 2008
  - paper: in Energie+ *Slimme Meters: Energie wordt ICT?*

see `www.cs.ru.nl/M.vanEekelen/research/pubs`

Involvement in Metering

- Smart meter evaluation projects (commercial) for Alliander (former operator part of Nuon)
  - Two meters tested (reports confidential)
  - Focus on security issues
  - Within "LaQuSo" context
- Research project on Secure Metering, financed by STW
  - three year post doc: *Flavio Garcia*
  - also involves road pricing (similar underlying issues)
  - aimed at secure, privacy-friendly, fraud-resistant protocols
  - with Alliander & RDW support/cooperation
- Now part of the metering incrowd
  (round table meetings etc)

Why smart meters?

- Basis in EC directive (2006/32/EC)
- Remote reading, to prevent expensive home visits
- Remote management (change supplier etc.)
- Remote disconnect:
  - to deal with arrears (non-payment/fraud)
  - emergency supply management ("code red")
- Intelligent grid management, for optimisation, esp. with eg.
  - electric car charging (sudden high demand)
  - clients who also produce, etc.
- Energy preservation, via better insight in own consumption
- Additional (commercial) services, based on customer profiles
  - typically by third parties

Players

1. Clients/consumers of electricity/water/gas
2. Suppliers (producers/resellers)
3. Grid operators: transport/maintenance/optimisation
4. Metering companies: input for billing
5. Commercial (additional) service providers

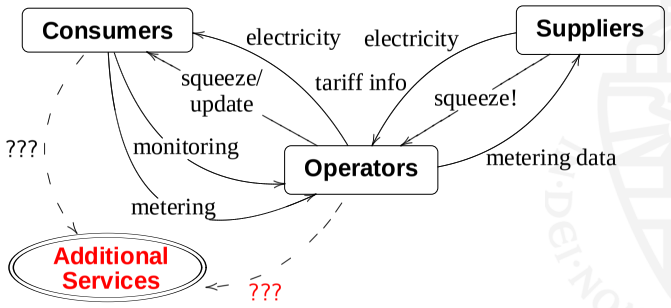
Focus here

On electricity, for simplicity

Merging of roles, with new smart meters

Grid operators will also do metering

Flow schema essentials



Sensitive issues

How much/often metering / monitoring / control / services info

Security Issues (CIA = Confidentiality, Integrity, Availability)

1. **Suppliers**
   - integrity / availability of metering info
   - availability of electricity
2. **Operators**
   - integrity / availability of metering & monitoring info
   - availability of grid
3. **Consumers**
   - confidentiality / integrity of metering & monitoring info
   - availability of electricity

Timeline

1. **Summer 2008**
   New utility law adopted by Parliament (Second Chamber)
   - making smart meters compulsory,
   - meter recording *every 15 minutes*
     (daily read-out, with opt-in for every 15 min.)
   - remote squeeze/disconnect possible
   - clients can also supply energy (solar/wind/. . .)
2. **Spring 2009**
   Senate (First Chamber) removes compulsary character
   - serious privacy/security concerns
   - positive impact: sector finally wakes-up
3. **Currently**
   Awaiting update of law (*novelle*)
   - obligation to accept meter will disappear; details pending

Lessons learned from OV-chip disaster

1. Critical attitude towards suppliers needed:
   - Sector should impose requirements/protocols
   - *Security through obscurity* does not work
     (obscurity is usually cover-up for incompetence)
2. Developments take place within privatised sector, but relevant Cabinet Minister:
   - has no real power & is not responsible
   - but is still summoned by Parliament after incidents
   - ministry now more critical/demanding
3. Consumer focus (strong role of *Consumentenbond*)

Privacy concerns: Pamphlets (in Dutch only. . .)

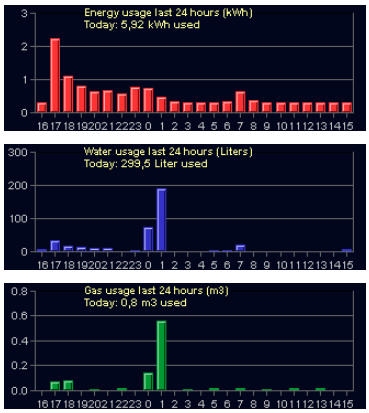
SLIMME METERS

**MIJN BROERTJE GAAT
LANGER DOUCHEN
IN DE HOOP
DAT DE CONTROLEURS
DENKEN DAT HIJ
EEN VRIENDINNETJE
HEEFT**

Loesje

Postbus 1045
6801 BA Arnhem www.loesje.nl

Privacy concerns: example readings (bwired.nl)



Privacy concerns & personal security

With 15 minute & daily meter reading . . .

- Operator/producer employees see when I'm at home or not
- Useful info for burglars
  (can use blackmail/bribery/infiltration/hacking to get such info)
- Why am I exposed to this new vulnerability?
- Privacy is important for personal security!

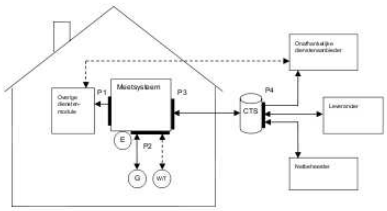
Denial of service (DOS) concerns

- Nicely illustrated in *Delta Lloyd Hackman* Video advertisement (2005)
- National security risk
  (exploitable by blackmailers/terrorists/. . .)
- Why do we introduce these vulnerabilities?

Basics/issues

- E-meters (up-to 300) connected to Data Concentrators (DCs) in geographical vicinity (block level)
- E-meter communication possible via:
  - PLC = Power Line Communication
  - GSM/GPRS
  - Internet
- Clients can also be electricity producers
- Prepaid payments, via centrally stored "coins"
- Multiple suppliers communicate cheap periods; meter can choose dynamically
- E-meter norms specified, in NTA-8130 by NNI

NTA-8130 port schematics



Detailed security requirements missing

Most sensitive/controversial

P4: Additional services connection at database. Backdoor?

Monitor protocol proposal

- Supplier S, meter M, operator O
- $\{m\}_X$ encryption with X's public key;
  $[m]_X$ signature with X's private key

Meter monitoring

$$
\begin{aligned}
O &\longrightarrow M \quad : \quad \text{monitor!} \\
M &\longrightarrow O \quad : \quad \text{nonce } n \\
O &\longrightarrow M \quad : \quad \left[\text{monitor!}, n, M, \text{timestamp}\right]_O \\
M &\longrightarrow O \quad : \quad \left\{\left[M, \text{time}_M, \text{status}\right]_M\right\}_O
\end{aligned}
$$

- Such requests must be logged and visible locally

Supplier change protocol

- Operator sets new supplier S, together with polling/readout period p, chosen by customer

Supplier & period update

$O \longrightarrow M$: new supplier!
$M \longrightarrow O$: nonce n
$O \longrightarrow M$: $\left\{ [n, M, \text{supplier}, S, \text{pubkey}_S, \text{period } p]_O \right\}_M$

Periodic meter report protocol ("power to the meter")

- Initiated by reader, with agreed frequency p
- Better name "report" (meter active) instead of "read-out" (meter passive)
- Data sent to supplier S, not visible for operator O

Meter report, periodically with frequency p

$M \longrightarrow S$: $\left\{ [M, \text{time}_M, \text{meter stand}]_M \right\}_S$

- Meter initiative/autonomy not in current business models (of operators) — O/S see themselves as "trusted"

Main points

1. Security & privacy issues can make or break ICT-projects
2. Privacy concerns wrt. suppliers handled in new law
3. Important unresolved issues
   - How much monitoring by operators? Which safeguards?
   - Additional services connections (where, if any)?
4. Important security lessons: keep it simple & open
5. Consumer focus & decentralised architecture
6. Security/privacy protection best guaranteed
   - via technical means (in protocols)
   - not via regulation (can easily be changed/circumvented)