Privacy Enhancing Techniques for Smart Grids

PETs PhD Course
4th Session

Valentin Tudor
Chalmers University of Technology
Dept. of Computer Science and Engineering

October 18th, 2012
Karlstad
Outline

- Smart Grid general concepts
- Privacy in the Smart Grid
- Smart Grid privacy via anonymization of smart metering data
- Conclusions
The need for a “Smarter” Grid

- Electricity as the driving force
- Effects of a blackout
  - 2003 a “dark” year
  - 50 mil people left into darkness
  - Loses in billions $
Smart Energy → Smart Meters

- The traditional electrical grid is changing
- By 2020:
  - reduction in electricity consumption
  - reduction in greenhouse gas emissions
  - electricity from renewable energy

EU mandated that by 2020 all the traditional electricity metering devices should be replaced with smart meters

Source: http://ec.europa.eu/clima/policies/brief/eu/index_en.htm
A Smart Meter:
- a small embedded system
- automates (consumption) index readings
- instantaneous consumption
- in-door display
- time of use tariffs
- the base for the Advanced Metering Infrastructure
Smart Meter components

- Communication Module
- Processing Unit
- Electrical Meter

Data to/from Data Concentrator/Other Meters

Electrical Measurement from the power line
The traditional Electrical Grid

Managed and monitored by the SCADA system.

No dedicated real time monitoring system (yet).
From centralized to distributed generation

Power Island
Why privacy in Smart Grid?

- Lots of new sensitive data, gathered with a higher frequency and granularity
Using data from the Advanced Metering Infrastructure

- By the utility company
  - Billing
  - Fraud detection
  - Operational purposes – grid stability and security
  - Marketing
Using data from the Advanced Metering Infrastructure

- By 3rd parties (benign and malign)
  - Research related activities
  - Malicious activities
    - Fraud
    - Invasion of privacy
  - Attacks on critical infrastructures
Protecting Customers’ Privacy

- Smart metering data can be used to infer information about a customer’s behavior by observing energy usage patterns

- Customer’s privacy should be protected against the Utility provider and other 3rd parties
Peak = 7.18 kW
Mean = 0.49 kW
Daily load factor = 0.07
Energy consumption = 11.8 kWh

Time of day (24h)
Achieving Privacy

- Through **data manipulation**
  - Anonymization
  - Altering data (adding values from a random distribution)
  - 3rd party data aggregation and disclosure

- Through **load-shedding**
  - Changing consumption pattern using energy storage and/or production facilities at the premises (batteries, renewable energy sources, etc.)
Current Smart Grid Privacy Architectures

- Anonymous credentials – based on blind signatures
- 3rd party escrow mechanism – anonymize high-frequency metering data
- Load-signature moderation – load-shedding
- Smart energy gateway – establishing levels of privacy
- Privacy preserving authentication – using private-public key pairs to create pseudo-identities

Attacks against Privacy Architectures

Examples:

- De-pseudo-anonymization – linking by behavior
- Data-mining (see more about this later)
- Compromising the Trusted 3rd Party or the Utility Company Database

Goal: preserving customers’ privacy while having access to metering data needed for billing and metering data needed for grid operation

For one specific customer, the data needed for billing should be attributable, while the data needed for grid operation should be non-attributable.
Data generated by a Smart Meter

- ‘High-frequency’ metering data - meter readings that a smart meter transmits to the utility often enough (e.g. every few minutes) and may divulge information related with the private life of the user (e.g. usage patterns of specific electrical appliances) – **non-attributable data**
Data generated by a Smart Meter

- ‘High-frequency’ metering data - meter readings that a smart meter transmits to the utility often enough (e.g. every few minutes) and may divulge information related with the private life of the user (e.g. usage patterns of specific electrical appliances) – non-attributable data

- ‘Low-frequency’ metering data - is transmitted to the utility scarcely enough (e.g. every week or month) and is used for account management or billing purposes – attributable data
To handle the two types of data, each Smart Meter must have two separated embedded identities:
To handle the two types of data, each Smart Meter must have two separated embedded identities:

- **HFID** – High-Frequency ID – used when sending high-frequency metering data (anonymous data)
To handle the two types of data, each Smart Meter must have two separated embedded identities:

- **HFID** – High-Frequency ID – used when sending high-frequency metering data (anonymous data)
- **LFID** – Low-Frequency ID – used when sending low frequency metering data (attributable data)
Identities knowledge and data usage

- Who knows the Smart Meter’s identities?

<table>
<thead>
<tr>
<th></th>
<th>Smart Meter</th>
<th>3rd party/Manufacturer</th>
<th>Utility Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFID</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LFID</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Identities knowledge and data usage

- **Who knows** the Smart Meter’s identities?

<table>
<thead>
<tr>
<th></th>
<th>Smart Meter</th>
<th>3rd party/Manufacturer</th>
<th>Utility Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFID</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LFID</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **Who is allowed** to store and/or use the metering data?

<table>
<thead>
<tr>
<th></th>
<th>Smart Meter</th>
<th>3rd party/Manufacturer</th>
<th>Utility Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>HF-Data</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>LF-Data</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Data communication overview

Smart Meter ID profiles

- PISM - Personal Identifiable SM profile
  - PISM Certificate (LFID, PISM Public Key, PISM CA information)
  - PISM Private Key

Smart Meter ID profiles

- **PISM - Personal Identifiable SM profile**
  - PISM Certificate (LFID, PISM Public Key, PISM CA information)
  - PISM Private Key

- **ANSM - Anonymous SM profile**
  - ANSM Certificate (HFID, ANSM Public Key, ANSM CA information)
  - ANSM Private Key

Smart Meter ID profiles

- **PISM - Personal Identifiable SM profile**
  - PISM Certificate (LFID, PISM Public Key, PISM CA information)
  - PISM Private Key

- **ANSM - Anonymous SM profile**
  - ANSM Certificate (HFID, ANSM Public Key, ANSM CA information)
  - ANSM Private Key

- PISM and ANSM profiles are hardcoded into the Smart Meter and used to create the Client Data Profile (CDP) and the Anonymous Data Profile (ADP)

What are Smart Meter CDP and ADP?

- Are attached to each message which contains metering data information, send by the Smart Meter:
  - Each message containing **Low-Frequency** metering data has **CDP** (Client Data Profile) attached to it.
  - Each message containing **High-Frequency** metering data has **ADP** (Anonymous Data Profile) attached to it.
Client Data Profile (CDP) Setup

- Is initiated by the Smart Meter or the Utility Company

1. CL- >U: CL. CLI
2. U- >AGG: CL. CLI + PI SM CERT + U. CERT
3. AGG- >U: AGG. CERT
4. U- >PDNet: AGG. CERT + PI SM CERT + U. CERT
5. PDNet- >U: PDN. CERT

\[ \text{CDP} = \text{CLI} + \text{PI SM CERT} + \text{AGG. CERT} + \text{U. CERT} + \text{PDN. CERT} \]

6. U- >SM: CDP + U. code
7. SM- >U: CDP + $S_{\text{PI SM PRIV}}(\text{CDP})$

\[ \text{SM- >U: CDP} + \text{Data. LF} + S_{\text{PI SM PRIV}}(\text{CDP} + \text{Data. LF}) \]
Client Data Profile (CDP) Setup

Is initiated by the Smart Meter or the Utility Company

HFID – High-Frequency ID – used when sending high-frequency metering data (anonymous data)

LFID – Low-Frequency ID – used when sending low-frequency metering data (attributable data)
Anonymous Data Profile (ADP) Setup

- Is initiated by the Utility Company and the Smart Meter after CDP setup has finished

1. U→ESC: CDP + U.CERT
2. ESC→U: OK
3. U→SM: ADP setup request

   \[ \text{ADP} = \text{ANSM.CERT} + \text{AGG.CERT} + \text{U.CERT} + \text{PDN.CERT} \]
   SM waits a random time

4. SM→ESC: \( E_K(\text{CDP} + \text{ADP}) + S_{\text{ANSM.PRIV}}(E_K(\text{CDP} + \text{ADP})) \)
5. ESC→AGG: ADP + ESC.CERT
6. AGG→ESC: OK
7. ESC→SM: OK

   SM→AGG: ADP + Data.HF + \( S_{\text{ANSM.PRIV}}(\text{ADP} + \text{Data.HF}) \)
Anonymous Data Profile (ADP) Setup

- Initiated by the Smart Meter or the Utility Company
- HFID – High-Frequency ID – used when sending high-frequency metering data (anonymous data)
- LFID – Low-Frequency ID – used when sending low-frequency metering data (attributable data)
Security analysis of CDP and ADP setup

- **CDP setup security analysis:**
  - to verify if a genuine Smart Meter has been installed to a genuine location
    - The client is verified by the utility engineer
    - The Smart Meter authenticity can be verified by checking U. code
  - The utility engineer must be trusted at all times

(see http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/)
Security analysis of CDP and ADP setup

- ADP setup security analysis:
  - Depends on the security of the CDP process
  - Depends on the trustworthiness of the 3rd party escrow entity
  - Depends on the level of anonymity achieved through the setup and use of the ADP
    - The anonymity set depends on the number of ADP finalization responses received by the utility between the CDP finalization response (ADP setup request) and the ADP finalization response of the same meter
Security analysis of CDP and ADP setup

- ADP setup security analysis:
  - Depends on the security of the CDP process
  - Depends on the trustworthiness of the 3rd party escrow entity
  - Depends on the level of anonymity achieved through the setup and use of the ADP
    - The anonymity set depends on the number of ADP finalization responses received by the utility between the CDP finalization response (ADP setup request) and the ADP finalization response of the same meter
Security analysis of CDP and ADP setup

- ADP setup security analysis:
  - Depends on the security of the CDP process
  - Depends on the trustworthiness of the 3rd party escrow entity
  - Depends on the level of anonymity achieved through the setup and use of the ADP
    - The anonymity set depends on the number of ADP finalization responses received by the utility between the CDP finalization response (ADP setup request) and the ADP finalization response of the same meter

..CDP_{1ADPr}, CDP_{77ADPr}, CDP_{33ADPr}, CDP_{2ADPr}, CDP_{7ADPr}, CDP_{5ADPr}, CDP_{49ADPr}, ADP_{77}, ADP_{1}, [ADP_{33}]...
Security analysis of CDP and ADP setup

- ADP setup security analysis:
  - Depends on the security of the CDP process
  - Depends on the trustworthiness of the 3rd party escrow entity
  - Depends on the level of anonymity achieved through the setup and use of the ADP
    - The anonymity set depends on the number of ADP finalization responses received by the utility between the CDP finalization response (ADP setup request) and the ADP finalization response of the same meter
  - The random time interval between receiving the ADP setup request and the ADP finalization responses must be chosen in such a way that a large anonymity set can be created
What to remember?

- Splitting data depending on the usage purpose and privacy sensitivity

- Setting up public and anonymous pseudonyms must be done such that a large anonymity set is maintained
Conclusion

- Privacy in the Smart Grid is important – data can expose behavior patterns of inhabitants.

- Laws and regulations not very well defined or applicable only to a defined region, state, city, country.

- Not a very clear understanding of the privacy issues in the Smart Grid (no public privacy violation cases so far…).
Thank you!

Questions?