Protocols for privacy-aware Smart Metering

Enabling the Smart Grid without sacrificing privacy
Overview

Benefits and costs of Smart Metering and what has privacy to do with it

Problems in Smart Metering concerning privacy

Solving the (some) problems – an overview

Are we there yet? Open problems and questions
- Need accurate per-customer data according to tariff for billing
- Have interest in load profiles of their respective customers

- Has interest in accurate metering data of customers within its grid
Balancing costs and benefits of Smart Metering

Infrastructure costs

More efficient power generation

Improved Grid stability

New services for customers

Decentralization

...
Balancing costs and benefits of Smart Metering

Infrastructure costs

Loss of privacy

More efficient power generation

Improved Grid stability

New services for customers

Decentralization

Austria reverted laws for the introduction of Smart Meters in 2013 due to privacy concerns.
What exactly is privacy?

“I recommend that legal restrictions be enacted or clarified so that electric power usage is considered as private as any phone conversation.”
George W. Hart, 1989
More advanced applications with higher sampling rate:

- Recognition of watched TV program
- Fine-tuned house-automation
Once collected, it’s not over yet…

Problem:
Storage of private, sensitive and potentially very valuable information

Penetration test of an energy provider in southern Germany performed in 2014:
Within a few days, testers achieved full access to the operations control center.
Solution: prevent interesting data at the source

Use local energy storage to compensate features in energy consumption profile
- Infrastructure and operational costs
- Limited by size of energy storage
Solution: Only collect what’s actually needed

Why do we meter energy?

Metering for billing
- More accurate bills
- More timely billing (not real-time)
- Better transparency

Metering for operations
- Monitoring energy flow in network
- Managing real-time energy production
- Information source for demand side management

Two problems, that can be solved separately.
Solving the metering for billing problem

Accurate
High-frequency

Semi-accurate
Low-frequency

Aggregated over time

March 1.342kWh
April 1.146kWh
May 1.042kWh
Solving the metering for billing problem

Simple time-based aggregation may be too simple for future flexible tariffs.

Using cryptographic commitments is one possibility.
Solving the metering for operations problem

- For billing
  - Aggregate over time
  - For each household

- For operations
  - Aggregate over households
  - For each measurement

- Different sets of households necessary
  - Segments of the power network for grid operators
  - Possibly geographically scattered customers of a specific energy provider
Using a trusted third party

A trusted third party aggregates incoming measurements and provides an aggregate
- Infrastructure costs
- Who can still be trusted nowadays?
Separating aggregation and storage

A trusted third party only maintains keys and enforces policies on data access to one or many storage providers
  • Reduced infrastructure costs
Without a trusted third party: peer privacy

Households cooperate with each other to “defuse” their measurements
- Smart Meters must be able to communicate with each other
- Trust is “spread out” over peers
Basic concept behind SMART-ER: SMART

Slice measurements

Mix slices

Aggregate slices
Basic concept of SMART-ER
Characteristics of SMART-ER

- Small communication overhead
  - Exchange of masking data with peers
  - Linear in number of cooperating peers

- Small computational overhead
  - Simple arithmetic
  - Linear in number of cooperating peers

- Strong privacy guarantees
  - No information leak as long as data sink is not compromised
  - Exact measurement revealed if data sink and all cooperating peers are compromised
Problems of peer privacy

- Unreliability of Smart Meters and their communication infrastructure
  - Failure of one peer to submit → measurements of cooperating peers are lost

Solution: make small groups
Problem of smaller groups

- Attacks on the trust “spread out” over peers get easier
  - If data sink is already compromised only remaining group members need to be compromised
  - Efficiency of attack depends on grouping algorithm

Solution: decentralized, randomized grouping
Implementation on constrained hardware

- Smart Meters have to be
  - Cheap
  - Energy-efficient
  - Robust
  - ...

- Complex software/algorithms/protocols are difficult in this setting

- Working prototype: Smart Meter Speeddating for sensor networks
  - Measurement aggregation over households and randomized peer-to-peer group building
  - TinyOS
  - 7.37MHz, 8-bit CPU
  - 4kByte RAM
Open questions and problems

- How to measure (achieved or guaranteed) privacy?
  - Aggregation over how many households / which time frame is enough?

- What kind of capabilities do we need in our attack models?
  - Compromised data sink? Compromised Smart Meters?

- What are the capabilities of Smart Meters?
  - Complex cryptographic operations or simple arithmetic?

- How reliable are Smart Meters and their communication infrastructure?
  - How often is a Smart Meter “disconnected” or out of service?

- What needs to be done to get privacy-aware Smart Metering deployed?
  - What needs to be first, demand or product?
Conclusion

- Privacy-aware Smart Metering can be done!
  - With or without a trusted third party
  - With or without complex cryptography

- Privacy-aware Smart Metering can be done efficiently
  - Small communication and computational overhead
  - Smart Metering performance (almost) as good as privacy-violating Smart Metering

- Privacy-aware Smart Metering is not wide-spread (yet!)
  - If there is demand, there will be a product
  - If there is a product, there will be demand
Image credits

- Brass scales by Toby Hudson: http://commons.wikimedia.org/wiki/File:Brass_scales_with_cupped_trays.png
- Sphere by Geek3: http://commons.wikimedia.org/wiki/File:Sphere_wireframe_15deg_4r.svg