Privacy Threat Analysis of Smart Metering

Marek Jawurek
marek.jawurek@sap.com

Felix C. Freiling
felix.freiling@informatik.uni-erlangen.de

Abstract: Smart Grid and Smart Metering are being rolled out all over the world. However, the media, politicians and consumers are very sceptic about the potentially involved privacy loss. In this paper, we discuss the types of data the Smart Grid utilizes and what level of access the different roles of the Smart Grid need for their legitimate business. Furthermore, we provide some scenarios for how this data could be abused by stakeholders of the Smart Grid as well as external attackers.

1 Introduction

Smart Metering refers to the collection of consumption profiles and other information at customer's households with the help of so called *Smart Meters*. While the concept of Smart Metering is applicable to many other types of utilities like gas or water, it is most often discussed in the context of the electrical grid. There, Smart Metering is one part of the *Smart Grid* vision, where the electricity network is amended with a parallel communication network. The idea of the Smart Grid is to collect information along with the consumption/generation of electrical energy. This information can then be used to improve the process of energy generation, consumption and distribution. This is particularly useful in the electrical grid, since one physical limitation of the electricity grid is the inability to store electricity. Therefore, supply (generation) must match demand (consumption) at all times.

Today, predictions help to plan efficient long-term generation capabilities (like large electrical power plants) and less efficient but flexible generators are used to create the match of supply and demand. Clearly, the overall efficiency of the system critically depends on the quality of the predictions. Consumption of big energy consumers like steel plants can already be planned and controlled in a predictable way. However, the mass consumption by private households is very hard to predict. Currently, their consumption is approximated by so called standard profiles. These are calculated based on historic data and also current information like weather data and TV programs. While this method has proven to be reliable in the past, a more fine grained control of supply and demand promises more efficiency.

Smart meters allow a more fine grained control because they can act as both *sensors* and *actuators* in the private household. The vision is that every household measures its con-

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

sumption individually and makes it available in near real-time. In this case predictions could be created more precisely and at a lower level. Additional flexibility arises from using Smart Meters as actuators, because this would allow to partly control the *consumption* side, e.g., by remotely starting the washing machine at a suitable time during off-peak hours. This is in contrast to the current situation where only the generation side is controllable and relatively inflexible. Apart from the remote control of appliances the means for the control of consumption include but are not limited to time-of-use billing, load-dependent billing, real-time prices, and priority signals.

Smart Metering has been mandated by EU directive 2009/72/EC and promoted by the US Energy Independence and Security Act of 2007 and Smart Meter roll-outs have begun all over the world [sma10]. However, near real-time monitoring of energy consumption raise many privacy issues. In related work [Har92, Har89, LMW10, Sul91, BSL09] it has been shown that fine-grained measurement data of electricity consumption allows to infer many personal details like when and for how long appliances are used. In this paper we focus on the privacy risks of smart metering.

1.1 Related Work

There exists a number of overview articles on the security and privacy of Smart Metering [CPW10, GLT09, MM09, KHLF10] which we now discuss.

Cavoukian et al. [CPW10] provide an overview of what the Smart Grid is, how it will affect electricity consumers and how their privacy might be at risk by the Smart Grid and Smart Metering. Furthermore they promote the idea of building privacy into the Smart Grid from the start. Other overview articles [GLT09, MM09, KHLF10] give more information on the topics of security, privacy and trust in Smart Grids/Smart Metering and Advanced Metering Infrastructures (AMI) but do not explicitly mention roles of the Smart Grid as potential attackers on privacy.

Robinson and Stuber [RS08] perform a formal security thread analysis of Smart Metering. However, privacy of the consumers is not considered as an asset.

Individual solutions for privacy preserving operations in Smart Metering have been proposed which we now briefly discuss.

Lemay et al. [LGGG07] provide a sketch for an attested Smart Meter architecture. Using virtualization, mandatory network access control and trusted computing techniques this architecture enables multiple applications to use the Smart Meter hardware and to work in a privacy-preserving and integer manner. The article names applications for billing the customer very closely to the data origin (in the household) and applications that provide the consumer with a consumer portal. They achieve privacy-preserving Smart Metering billing by remote attestation of the billing software in the TPM of the Smart Meter.

Garcia and Jacobs [GJ10] propose a privacy-preserving detection algorithm for leakages in electricity distribution. By aggregation across several Smart Meters the developed algorithm protects individual meter readings while allowing grid operators to detect illegiti-

ISBN 978-3-88579-286-4

mate/unknown load.

Bohli et al. [BUS10] develop a model for measuring privacy in Smart Metering and subsequently present two different solutions to privacy: A Trusted Third Party-based approach, where individual consumption profiles are aggregated at the third party and only sums are communicated to the supplier. The other approach attempts to mask consumption profiles by adding randomness to the actual profile with an expectation of the random distribution of zero.

Petrilio [Pet10] also presents a twofold approach: The first solution employs a sophisticated Trusted Platform Module (TPM) in the Smart Meter to obtain signed tariff data from the supplier and calculate a trustworthy bill. The second solution makes use of the electrical grid infrastructure as a third party to anonymize up-to-date consumption values sent out constantly by Smart Meters.

Jawurek et al. [JJK10] and Rial and Danezis [RD10] cover the aspect of private billing in Smart Metering. Using cryptographic primitives the actual electricity price is calculated in the household and provided to the supplier together with a cryptographic proof of correctness.

To the best of our knowledge, there has not been any attempt to analyze the threats to privacy in Smart Metering by both stakeholders and attackers in a systematic and structured way.

1.2 Paper Outline and Contributions

After giving some background on the electrical grid and Smart Metering in general in Section 2, we identify the different roles and stakeholders (Section 3) and the different types of data collected in Smart Metering (Section 4). We then perform a systematic threat analysis with focus on privacy using the electrical grid as an example (Section 5). Our work can be also regarded as the basis of a research agenda for security and privacy research in Smart Metering/Smart Grid environments.

2 Background

In this section we give some additional background on Smart Grids and Smart Meters in particular.

2.1 Smart Metering and Smart Grids

As explained in the introduction, the main promise of Smart Metering is improved efficiency. This can be seen in combination with the trend towards more decentral gener-

ation of electricity from renewable sources since this will lead to a stronger fluctuating supply side. The idea is that real-time information about the behavior of decentral generation/consumption can be used to control the demand side appropriately and to encourage energy consumption at times where much energy from renewable sources is available.

A better match of supply and demand and introduced ability to control demand may also provide better stability and therefore availability of the grid. Bottlenecks can be predicted and therefore easier mitigated. Using control of the demand side a higher throughput of energy can be achieved because load can be distributed more evenly.

Another aspect of the electrical grid is the envisioned introduction of electric cars that will put an additional strain on the electricity grids. Their integration can be easier if they integrate well into the Smart Grid and communicate their need and their conditions for charging. On the other hand, virtually combined they can serve as huge batteries that store energy when there is a surplus and to discharge into the grid when there is a shortfall.

Another aspect of the Smart Grid that is mainly driven by the USA is that a more flexible grid will be more resilient to cyber-attacks and offline attacks than the traditional grid. The flexibility can prevent ripple effects and be used to form self-contained grid islands in case of cyber- or offline attacks.

2.2 Smart Meters

The narrow definition of a Smart Meter is the following: Smart Meters measure electricity consumption in households and communicate their readings (via push or pull) at regular intervals to back-end system. Those would suffice for a Smart Metering architecture, where it is sufficient to collect near real-time information and to control the demand side by time-of-use or load-dependent tariffs.

If one wants to implement the full Smart Grid vision, e.g., real-time tariffs or remote control of appliances those Smart Meters will need to act as a gateway into the household to connect intelligent devices in the household to the Smart Grid. The following characterization describes the differences between traditional electricity meters and Smart Meter for Smart Metering and Smart Meters with extended functionality for the realization of the Smart Grid:

- Connectivity: Smart Meters can be remotely read. That means, they are connected, temporarily or constantly, to a communication network that allows accessing their data.
- Continuous Measurements: Smart Meters create high resolution (up to 1 reading per second or higher) energy consumption profiles. Traditional electricity meters accumulated energy consumption over the billing period and reported (via manual reading) one value.
- Complexity: Smart Meters need to cryptographically sign and potentially encrypt their readings. Therefore, they need some computing capability and additional com-

ISBN 978-3-88579-286-4

munication modules and protocol stacks to achieve mentioned connectivity.

- Gateway functionality: The Smart Meter acts as gateway into the household. The user either shifts load directly himself as reaction to price changes or incentives or enters preferences into an appropriate household controller (e.g., the gateway) to let the gateway take control of load shifting. Therefore, the gateway delivers appropriate information to respective displays or appliances or provides means of interaction itself.
- Remote actuation: The gateway functionality is extended, by control of household appliances. Appliances are registered with the gateway and their control is forwarded to external entities. In accordance with the households preferences and restriction those external entities now have a combined load-shifting potential of many households at their hands and can shift overall demand considerably.

3 Smart Metering roles

As basis for a threat analysis, it is necessary to identify the different stakeholders. The following is based on the German energy industry roles as already described by law, predicted by research projects or already being implemented by companies. Some of these roles have already existed in the traditional grid:

- consumer,
- grid operator,
- supplier,
- generator,
- metering point operator (new),
- measurement services provider (new),
- demand side manager (DSM) (new) and
- virtual power plant operator (VPPO) (new).

Consumers are physically connected to the electrical grid and have a Smart Meter installed in their households. After fixed time intervals they pay their bill for energy consumed in that interval to suppliers.

The Smart Meter is installed in households and maintained by metering point operators, a job previously covered by the grid operator role. Metering point operators can be chosen by consumers (or default to the local grid operator's contractor) and are paid by consumers either directly or through the grid operator.

ISBN 978-3-88579-286-4

Measurement services provider collect consumption data from Smart Meters and deliver it to the respective grid operator. The grid operator sorts the data according to supplier affiliation and reports all consumption data of the supplier's customer base to this supplier.

Suppliers estimate the future energy needs of their customer base and order respective future amounts from generators. Discrepancies between the actual consumption of the customer base and the previous estimate can be reduced to some extend in real time by buying generation potential at energy stocks. For remaining discrepancies the supplier either pays or receives money to/from the grid operator, depending on the discrepancy's sign and the discrepancies of all other suppliers. In order to even better control the consumption (to match the estimate) supplier may instruct virtual power plant operators or demand side managers to control the supply/demand side respectively.

Virtual power plant operators logically combine small decentralized generation into big, centrally controlled virtual power plants. (De-)Activiation of single generators allow virtual power plants to control their output with high resolution. Demand side managers control the demand side by giving consumers short-term incentives to reduce/increase power consumption or by directly controlling consumer appliances remotely. Both provide logical load-shifting potential to suppliers for achieving predictions and physical load-shifting potential for the prevention of physical bottlenecks in transmission. Small generators profit from lowered control effort and from better marketing opportunities as part of a big virtual power plant. Consumers benefit from participation in demand side manager plans either by more appealing supply tariffs or from concrete rewards for changed consumption behavior. Households can be consumers and generators at the same time.

With respect to data, consumers and generators are producers while grid operators, suppliers and measurement service providers are consumers of data.

4 Data types in Smart Metering

In the traditional metering scenario the following different data items are created by the data producers:

- *Contact details* are used for identifying the customer and for sending the invoices. The customers neighborhood also indicates the income level and social class.
- *Billing details* are used for directly collecting the invoice from the customers bank account. The way the customer pays his bills also indicates the income level and social class and perhaps also the employment status.
- *Annual measurements* are collected manually from meters and reported to the grid operator and subsequently to the supplier.
- *Payment history* records the timeliness and reliability of payments of a customer to his supplier. This data item is automatically and implicitly created by the consumer paying his bills.

ISBN 978-3-88579-286-4

Smart Metering introduces new data items:

- *High-resolution measurements* or even real-time consumption measurements are recorded by Smart Meters. This data item replaces the obsolete annual measurements.
- *Load/Generation-shifting preferences* are configured by the consumer/generator into the gateway component of the Smart Meter. They are used by the Smart Meter to determine how to control appliances/generators to comply with the inhabitants' preferences. E.g. when to start the dryer or when to start the combined heat and power (CHP) generator.
- *Smart Appliance information* are seen by the Smart Meter while in interaction with the appliances. This includes types of appliances and usage times/patterns.
- *Demand side reaction history* record how the customer reacts to load-shifting request by demand side managers. This data item is automatically and implicitly created by the consumer participating in demand response schemes.

In order to judge the actual privacy loss associated with the different data items we identify two dimensions. The first dimension is whether data items are *static* vs *dynamic*. Static data items leak information very seldomly (at most once a month) while dynamic data items change often (e.g. hourly) over time and therefore reflect changes in the household or in inhabitants' behavior. The other dimension is the degree of concreteness of the data items, *explicit behavior data items* vs *implicit behavior data items*. Explicit behavior data items directly express what goes on in the household, e.g. washing machine started at 10am, or what inhabitants like/dislike/prefer, e.g. washing machine must not run at night or on vacation. Implicit behavior data items only give an indication about what might be going on in the household. From implicit behavior data items one could try to infer what is going on in the household, e.g. increased energy consumption might indicate the washing machine but might also indicate cooking.

Table 1 illustrates how the aforementioned data items can be categorized according to the aforementioned dimensions.

We do not attempt to order the different data items w.r.t. their privacy impact. In this abstract observation of the Smart Grid this is not feasible, a specific description of the data items, the sampling frequency and more information would be required to even attempt something like this. However, regarding each dimension individually, one can generally claim that dynamic data items leak more privacy than static data items and that explicit behavior data items leak more privacy than implicit behavior data items.

We can therefore conclude, that smart appliance information (dynamic, explicit behavior) and load/generation-shifting preferences (explicit behavior) are among the most privacy invasive data items of that list.

ISBN 978-3-88579-286-4

	Static	Dynamic
Implicit behavior data items	Contact details, Billing details, Annual Measurements, Payment history	Demand side reaction history, High-resolution measurements
Explicit behavior data items	Load/Generation-shifting preferences	Smart Appliance information

Table 1: Traditional/Smart Grid data item characterization

5 Privacy Threat Analysis

5.1 Legitimate uses of Smart Grid consumers' data

For the analysis of legitimate uses of Smart Grid data items we restrict ourselves to the data consuming roles identified in 3. Legitimate access is when a service provider requires that data item in order to provide the service to the service consumer.

Table 2 displays in what form the different types of Smart Grid consumer data items are required by the different roles of the Smart Grid in order to provide their services. For the virtual power plant operator the data producer is the electricity generating household, for the rest the data producer is represented by the electricity consuming household. The entries of the table are explained in the following:

N : Necessary for legal and legitimate purpose. These data items are legitimately used by the respective user in order to do business. All honest roles that do business with consumers need their contact details for contractual reasons, while only those need billing details that actually receive their fees directly from the customer.

A : Only necessary in aggregated form for legal and legitimate purpose. That means, the full amount of data is not necessary for doing business. For different purposes different aggregation techniques can be used to increase privacy for the consumer while maintaining utility. Consumption measurements, for instance, are needed in aggregated form for billing by the supplier but in real-time form by the demand side manager to perform their business.

Anon : Only necessary in anonymized form. The exact origin of this data item is not required, users could be grouped by topological proximity with respect to the grid. The grid operator,for instance, does not need to know which consumer produces which part of the bottleneck he is merely interested in the sum of load at a specific grid segment.

Most requirements by Smart Grid roles for data items are self-explanatory, almost every-

ISBN 978-3-88579-286-4

	Contact details	Billing details	High resolution measurements		Demand side reaction history	Load/Generation-shifting preferences	Smart Appliance information
			real-time	delayed			
Grid operator	N		Anon	A			
Supplier	N	N	Anon	A			
Metering point operator	N						
Measurement services provider			Anon	A			
Demand Side Manager	N	N	N		N	N	N
Virtual power plant operator	N	N	N			N	

Table 2: Use/Abuse matrix of Smart Grid consumer data items

one needs to know the consumers contact details for communication with the consumer. The measurement services provider does not need to know the consumer, it merely access the consumer's anonymous Smart Meter.

Billing details are required by everyone directly billing or paying the consumer/generator. The grid operator and the metering point operator usually bill the consumer through the supplier. The measurement services provider is payed by the grid operator. The demand side manager and the virtual power plant operator may pay the consumer/generator for providing load-shifting/generating capacity.

High resolution, real-time consumption measurements are required by the demand side manager and the virtual power plant operator to know their load-shifting potential. The grid operator could use anonymized real-time consumption measurements for physical optimization of its grid. The supplier could use anonymized real-time measurements for minimizing the discrepancy between prediction and actual consumption in real time through the services of a demand side manager.

The high resolution consumption measurements can be collected with delay and in aggregated form by the measurement services provider. They are then subsequently transported to the grid operator and further along to the respective supplier.

Demand side manager need to know quite a lot about their bundled consumer' households in order to provide a meaningful service to grid operators or suppliers. On one hand, they need as much information about consumers as possible to estimate the individual household's potential for load-shifting at any point in time. On the other hand, they need real-time information about the current consumption to judge how successful their efforts to control the demand side have been. The same applies to virtual power plant operators, although they usually do not require a reaction history because generators are usually remotely controlled.

We observe, that demand side manager and virtual power plant operator require most data items and also require the most privacy relevant data items: Dynamic and explicit behavior data items like the Load/Generation-shifting preferences and Smart Appliance information.

5.2 Privacy Concerns

The informational invasion into households that comes with the technologies of the Smart Grid faces resistance from data privacy experts, the media and the public. However, although technologies like remote actuation or real-time metering are very invasive with respect to privacy they also provide the biggest benefit to the Smart Grid. Furthermore, this benefit is measurable when investments into the grid for the mitigation of peak load can be avoided because of effective load-shifting. On the other hand, depending on the current state of distribution/transmission grids, new concepts like the massive introduction of renewable energy sources or electric cars necessitate an evolution of the grid. With a revolution of traditional metering into Smart Metering, those new concepts can be introduced without a massive extension of the grid's transmission/generation hardware.

ISBN 978-3-88579-286-4

For those reasons it is important to find techniques to mitigate the privacy problem without impeding on progress and innovation. In the following we give exemplary attack vectors that we foresee for different roles of the Smart Grid as well as external entities like Cracker or government agencies and even the consumer himself.

5.2.1 Smart Grid roles as attackers

The variety of opportunities for legitimate participants of the Smart Grid to abuse collected consumer data items is limited. We can safely assume, that the market is a good control instance that limits Smart Grid roles to attacks which either will not be detected or will not significantly harm their main business. Otherwise, they risk to lose their clients very quickly. This leaves them with only with one option, the trade with data items:

Depending on the data item in question this can be done quite stealthy, e.g. selling contact details to mass marketers. The trade of billing details would harm the consumers very directly and is therefore unlikely. High-resolution consumption measurements might be well worth trading. In anonymized form this data would, for instance, allow TV advertisement agencies to optimize their advertisement timing. In non-anonymized form this data could be used to directly market consumers with special offers that make use of information contained in the consumption data. However, as identified in Section 4, the most privacy-invasive data items are smart appliance information (dynamic, explicit behavior) and load-shifting preferences (explicit behavior). They can be directly used to send consumers individual advertisement based on existing appliances or on their explicitly phrased preferences.

Depending on the actual jurisdiction those uses of Smart Metering data items could even be legal. However, it should be noted that neither security nor privacy are a zero sum game which means that such abuse of privacy must not necessarily result in an negative impact for the 'victim' apart from the virtual loss of privacy.

For preventing abuse by Smart Grid roles research needs to find measures that allow companies to fulfill their roles but limit the potential for abuse. With [JJK10] such a solution for billing has been presented. It describes a Smart Metering architecture and protocol to bill consumers of electricity with time-of-use or even real-time tariffs without leaking consumption measurements outside the household. That means, that even the billing supplier just receives verifiable, aggregated price information that do not disclose much.

5.2.2 Government agencies, Crackers and others

Table 3 shows how government agencies, crackers or others might abuse data items collected and stored by Smart Metering. The following list describes the table's entries:

M : Abuse for marketing. Knowledge of this data could enable someone to expand their business. Semi-honest suppliers or demand side manager could abuse this data to identify interesting customers that either have a huge demand of energy or have huge load-shifting potential respectively.

	Contact details	Billing details	High resolution measurements: real-time	High resolution measurements: delayed	Demand side reaction history	Load-shifting preferences	Smart Appliance information
Government Agencies			D	D		D	
Cracker		F					C
Other	M	F	E	D			

Table 3: Use/Abuse matrix of Smart Grid consumer data items

F : Banking fraud. This data could be used in banking fraud/credit card fraud or could be sold on respective black markets for credit card/bank contact data.

E : Energy fraud. This data could be used to manipulate the energy stock markets.

D : Data mining. This data could enable someone to learn private information about consumers. This information could subsequently be sold to marketing companies, directly used for internal marketing or used for blackmail/monitoring of citizens.

C : Information gathering for cyber-attacks. This data could enable someone to stage further attacks.

While government agencies are mostly interested in collecting information about citizens crackers are interested in remote massive manipulation of Smart Meters by viruses/Trojan horses or denial of service attacks. Those could disturb the grids' ability to operate at peak efficiency. This can be used by attackers for at least two purposes:

Availability: Disturbing load-shifting on a massive scale could bring the grid down if the resulting peak loads can no longer be accommodated by the grid's infrastructure. The more the grid relies on its 'smart' techniques instead of brute hardware power the more receptive it becomes to these kinds of attacks. Attacker can target Smart Meters themselves or merely the communication infrastructure that connects them with the Smart Grids backbone. Those kinds of attacks could be used to severely disturb whole countries and could therefore be interesting for malicious governments or malicious interest groups.

Integrity: By manipulating the grid's load-shifting capability in this way, an attacker could try to monetize his efforts on energy stock markets. As he foresees the inability in load-shifting he can bet on higher loads that he produces himself. Whether the jurisdiction would put one and one together and link the non-availability of parts of the grid and the trades on energy stock markets together is doubtful. If executed carefully, i.e. not too greedy, the attacker could benefit a lot over a longer period of time.

Physical attacks: Data items of the Smart Grid could also be used to identify households whose inhabitants are on vacation or simply wealthy. Potentially also the existence of alarm systems could be identified in consumption profiles.

Wherever massive amounts of interesting data are stored this attracts attackers. The Smart Grid gathers or even stores huge amounts of consumption profiles, household load-shifting preferences or incentive-reactions. Attackers will try to get to this information and they will try to identify the weakest link. All IT-systems of legitimate Smart Grid participants are potential entry points for attacks. It is definitely easier to attack those systems instead of gathering the data in the Smart Grid by oneself.

5.2.3 Owner as attacker

In Smart Metering introduction debate the household's inhabitants are always portrayed as the victims of privacy invasions. However, one must also consider that an important piece of the Smart Grid will be situated in the household, the Smart Meter/Smart Grid Gateway. Meter tampering has always been a problem for energy companies, as people tried to 'steal' energy by manipulating the meter. Eventually, meters were made at least tamper-proof if not even tamper-resistant to allow meter reading personnel to spot manipulations. With Smart Meters, however, that perform most of their work in software, tampering becomes harder to detect. Techniques to prevent this are being considered at the moment: Trusted Platform Modules, remote attestation or virtualization of the actual metering program to separate it from the actual operating system [LGGG07]. Manipulation of the Smart Meter might not only result in energy theft but also in disruption of Smart Grid operations. If, due to tampering, real-time information or load-shifting requests cannot be transmitted from/to the household the overall load-shifting capability of the grid suffers.

On another level, household inhabitants might try to abuse those schemes that should bring efficiency by load-shifting to the grid. Complicated incentive schemes always bear the risks of being conned. Therefore we find it important always to try new schemes on a small population in order to keep potentially negative effects small.

6 Conclusions and Further Research

We already mentioned how attacks on the Smart Grid could result in decreased availability of the grid itself or privacy loss of its users. While the problems of availability and integrity

can mostly be countered with careful design and robustness in mind the privacy aspect requires special attention as it forms a trade-off with utility of the Smart Grid technologies as mentioned in the introduction of Section 5.2.

In order to reduce the amount of data and the potential of abuse techniques like on-site calculation of bills [JJK10], aggregation of data destined for particular purposes or anonymization could be applied. Calculation on encrypted data could also mitigate the risks associated with large quantities of clear text data in badly protected IT-systems. While those approaches are technological regulatory approaches exist as well. However, they can only punish misbehavior retrospectively while technological approaches can prevent it in the first place.

We are confident that a satisfying trade-off between the utility of data and its privacy can be found on a per-application basis.

References

[BSL09] Gerald Bauer, Karl Stockinger, and Paul Lukowicz. Recognizing the Use-Mode of Kitchen Appliances from Their Current Consumption. In *EuroSSC*, pages 163–176, 2009.

[BUS10] Jens-Matthias Bohli, Osman Ugus, and Christoph Sorge. A Privacy Model for Smart Metering. In *Proceedings of the First IEEE International Workshop on Smart Grid Communications (in conjunction with IEEE ICC 2010)*, 2010.

[CPW10] Ann Cavoukian, Jules Polonetskyand, and Christopher Wolf. Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, 3(2):275–294, August 2010.

[GJ10] F. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Proceedings of the 6th International Workshop on Security and Trust Management*, 2010.

[GLT09] M. Oostdijk G. Lenzini and W. Teeuw. Trust, Security, and Privacy for the Advanced Metering Infrastructure. Technical report, July 2009.

[Har89] George W. Hart. Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows. *IEEE Technology and Society Magazine*, June 1989.

[Har92] G.W. Hart. Nonintrusive appliance load monitoring. *Proceedings of the IEEE*, 80(12):1870 –1891, dec 1992.

[JJK10] Marek Jawurek, Martin Johns, and Florian Kerschbaum. Plug-in privacy for Smart Metering billing. *CoRR*, abs/1012.2248, 2010.

[KHLF10] Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A. Frincke. Smart-Grid Security Issues. *IEEE Security and Privacy*, 8:81–85, 2010.

[LGGG07] Michael Lemay, George Gross, Carl A. Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *in Hawaii International Conference on System Sciences. Big Island*. ACM, 2007.

ISBN 978-3-88579-286-4

[LMW10] Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker. Inferring Personal Information from Demand-Response Systems. *IEEE Security and Privacy*, 8(1):11–20, 2010.

[MM09] Patrick McDaniel and Stephen McLaughlin. Security and Privacy Challenges in the Smart Grid. *IEEE Security and Privacy*, 7:75–77, 2009.

[Pet10] Ronald Petrlic. A privacy-preserving Concept for Smart Grids. In *Sicherheit in vernetzten Systemen: 18. DFN Workshop*, pages B1–B14. Books on Demand GmbH, 2010.

[RD10] Alfredo Rial and George Danezis. Privacy-Preserving Smart Metering. Technical report, Microsoft Research, November 2010.

[RS08] R. Eric Robinson and Michael Garrison Stuber. Advanced Metering Infrastructure Risk Analysis for Advanced Metering. Technical report, 2008.

[sma10] Smart Metering Projects Map. `http://maps.google.com/maps/ms?ie=UTF8\&oe=UTF8\&msa=0\&msid=115519311058367534348.0000011362ac6d7d21187`, 2010.

[Sul91] F. Sultanem. Using appliance signatures for monitoring residential loads at meter panel level. *Power Delivery, IEEE Transactions on*, 6(4):1380 –1385, oct 1991.