A Holistic View of Security and Privacy Issues in Smart Grids

Muhammad Rizwan Asghar and Daniele Miorandi

CREATE-NET
International Research Centre
Via alla Cascata 56/D
38123 Povo, Trento (Italy)
{asghar,daniele.miorandi}@create-net.org

Abstract. The energy system is undergoing a radical transformation. The coupling of the energy system with advanced information and communication technologies is making it possible to monitor and control in real-time generation, transport, distribution and consumption of energy. In this context, a key enabler is represented by smart meters, devices able to monitor in near real-time the consumption of energy by consumers. If, on one hand, smart meters automate the process of information flow from endpoints to energy suppliers, on the other hand, they may leak sensitive information about consumers. In this paper, we review the issues at stake and the research challenges that characterise smart grids from a privacy and security standpoint.

Keywords: Privacy, Data Security, Smart Meters, Smart Grids, Prosumers

1 Introduction

The umbrella term 'smart grids' is used to broadly identify the next generation of energy transmission and distribution infrastructures. These will be characterised, from the technical standpoint, by a deep integration with Information and Communication Technology (ICT). Such a coupling with ICT will enable new functions and features, which will transform what is now, to a large extent, a uni-directional static infrastructure to a highly dynamic network able to support bi-directional electricity flows. This, in turn, will enable the full integration at scale of distributed generation (be it coming from renewable energy sources or distributed co-generation) and of energy storage (coming, e.g., from the widespread adoption of electric vehicles).

Smart grids will generate huge amounts of data. This smart grid data will be used for the real-time acquisition of various parameters of interest (including generation and consumption at end points; and grid state parameters) as well as for transmitting control messages (for example, for controlling from remote the behaviour of smart appliances). This is giving rise to a number of issues and challenges concerning the management of such data, issues and challenges which represent novelties for the energy sector.

In this paper, we focus on the security and privacy aspects of data generated by smart meters. Smart meters are one of the key technological enablers of smart grids. By measuring in near real-time consumption data of consumers (both industrial and householders), they enable distribution grid operators to control and optimise the supply and distribution. Further, in the presence of distributed generation, their role is vital in enabling local load balancing, a key aspect for improving the efficiency of the overall energy system. At the same time, data from smart meters rise privacy concerns and confidentiality issues. This fact, and its perception within the public, is slowing the roll-out of such technology in a number of countries. Developing ICT solutions able to successfully tackle such issues is instrumental in ensuring smart meters can be extensively deployed. What makes this different from standard data security issues is the combination of three factors: the legacy of energy technologies; the interweaving with legal and regulatory aspects; and, the complex structure of the energy sector, with a variety of players and different issues at stake.

The main contribution of this paper lies in the presentation of the key privacy and security issues of smart meter data, as well as in the identification of the most pressing research challenges to be tackled in order to devise ICT solutions capable of enabling the full scale deployment of smart meters and smart grid technology.

The remainder of this paper is organised as follows. In Section 2, we introduce some background on smart grids, its main stakeholders and key components. In Section 3, we discuss the most relevant research challenges to be tackled. In Section 4, we survey and comment related work on privacy and security issues of smart grids. Section 5 concludes the paper, pointing out directions for enlarging the scope of the current work.

2 Smart Grid Technology: An Overview

The vision of a smart grid builds on the development of intelligent, reliable, secure and cost effective technology able to provide full-fledged infrastructure for the complete life-cycle management of energy resources. A smart grid supports natively bidirectional energy flows and integrates two-way communication and control capabilities, thereby enabling a whole new array of functionalities and applications [1].

In the following, we first describe main stakeholders and then list key components of a smart grid. We then discuss enabling technologies, regulatory and legal aspects.

2.1 Main Stakeholders of a Smart Grid Scenario

In this section, we describe the most relevant stakeholders of a smart grid. This includes:

• *Consumers* are users (householders or companies) who consume energy, mostly accessing it in the form of electricity.
•*Energy Suppliers* provide consumers with access to energy; they are responsible for ensuring quality of service and for billing. Most pricing schemes adopted by energy suppliers (e.g., time-of-use, real-time prices) foresee the need to access aggregated energy consumption data.
•*Energy Service Companies (ESCOs)* provide advanced energy-related services. Within the scope of this paper, we refer only to that subset of ESCOs services that focus on consumers. This includes the design and implementation of energy savings project and of "rent-a-roof" schemes, whereby ESCOs install and manage solar panels on households' roofs.
•*Transmission System Operator (TSO)* operates the transmission (high-voltage) electricity infrastructure.
•*Distribution System Operator (DSO)* operates the distribution(low- and medium-voltage) electricity infrastructure.
•*Generation Company (GenCo)* produces energy that can be delivered in the form of electric power.
•*Network Providers* are responsible for offering services related to the data communication network.
•*Network Operators* operate the data communication network. Network providers and network operators may be the same but not necessarily.
•*Data Users* are those entities (including, but not limited to, data analytics companies and research centers) that can use data of smart grids publicly.
• *Prosumers* refer to individuals and companies that consume, as well as produce, energy.

2.2 Key Components of a Smart Grid

A smart grid includes the following key components:
• *Energy Transmission Infrastructure* is used for transmitting energy from energy sources to energy stations. For instance, energy transmission infrastructure for electricity includes a set big towers and high voltage cables deployed between electricity sources (such as solar panels, dams and wind farms) and electricity stations.
• *Energy Distribution Infrastructure* for electricity consists of a set of medium to small towers and medium to low voltage cables deployed between electricity stations and consumers' premises.
• *Data Communication Network* enables two-way communication between consumers and energy suppliers and between the latter one and TSOs/DSOs. A data communication network can make use of a variety of transmission technologies, be them wired (e.g., xDSL and FFTH) or wireless (e.g., LTE/4G and WiFi). In the energy sector, the energy distribution infrastructure can be used as a data communication network by making use of Power Line Communications (PLC) technology.
• *Smart Meters* are devices that record energy consumption of appliances within a home and communicate this information to energy suppliers and ESCOs.

• *Home Gateways* are devices that can access a data communication network (typically a public IP network) from the consumers' premises. In smart grids settings, home gateways can be used for transmitting information gathered by smart meters.
• *Network Gateways* are bridge between home gateways within a specific area and other smart grid components, such as energy suppliers and ESCOs or DSOs.
• *Monitoring Modules* provide usage and statistical information. For consumers and energy suppliers, monitoring modules can provide information about billing, energy consumption by a smart device and average daily energy consumption. For energy suppliers, monitoring modules provide information energy consumption in a particular area. For GenCo, TSOs and DSOs, monitoring modules provide information about how much energy is generated, transmitted and distributed, respectively. Both smart meters and Phasor Measurement Units (PMUs) include monitoring modules.
• *Smart Appliances* are appliances that can be remotely monitored and controlled; as such, they natively include appropriate monitoring modules.
• *Decision Making Modules* play an important role by taking decisions and controlling one or more of the aforementioned components. Examples of tasks performed include balancing supply/demand to maintain the energy transmission and distribution, as well as scheduling smart appliances to minimise the electricity bill.
• *Energy Generators* are sources that produce energy. They can be of large (e.g., a nuclear reactor) or small scale (e.g., rooftop solar PV plants).
• *Energy Stores* store energy generated by energy generators. This includes devices such as batteries, electric cars and flywheels.
• *Data Stores* store data generated and transmitted by different components in smart grids, such as home gateways and network gateways.
• *Electricity Market* allows the relevant actors to sell, buy and trade energy (in form of electricity).

2.3 Technology Aspects

Traditionally, energy systems were engineered around a rather small set of principles. First, generation was focused on a (rather) limited number of large power plants, which were under full control. The installed capacity was dimensioned base on peak loads (i.e., worst-case dimensioning). As the demand was not controllable, the supply had (basically) to follow the demand.

A number of innovations and disruptive technologies have radically changed that picture. First, we are witnessing the arising of distributed generation, whereby large power plants are replaced by a number of smaller generating units (down to the order of one kW) sparsely distributed on the territory. These generators are usually not under the full control of grid operators, as they are owned by third parties, be it companies or single householders (in the latter case we speak of prosumers, i.e., users that both produce and consume energy). Second, an ever increasing part of energy production comes from renewable sources. Most of them (in particular, those related to solar and wind energy) are rather unpredictable, with power supply varying heavily over even short time intervals. This makes it challenging for grid operators to ensure balance between supply and demand. On the other side, the deep integration with ICT makes it possible to have some degrees of control over demand. In other words, the execution of an energy-consuming activity (e.g., a dishwater cycle) can be controlled and, if deemed appropriate, delayed and re-scheduled. Technology enabling such processes goes under the name of 'demand-response'. Various solutions are currently under study, be them centralised (whereby a central unit schedules the work of remote appliances) or distributed (where a set of smart appliances is under the control of a local agent which takes decisions based on, e.g., real-time price plans). Another potential game changer is energy storage. Energy is difficult to store (in particular, at small scale); albeit different technological solutions have been proposed, none of them has made its way successfully into the market. The widespread adoption of electric vehicles with vehicle-to-grid (V2G) capabilities could provide, for the first time, the ability to store energy at an economically attractive price, providing a further degree of freedom (but also bringing additional constraints and challenges) in the management and control of smart grids.

In the context of smart grids, a smart meter is a device able to (i) measure consumption of electric energy with a variable time granularity (ii) communicate via some networking technologies to the distributed system operator. A typical smart meter is shown in Figure 1.

Fig. 1: A typical smart meter layout (image borrowed from [2])

Concerning the time granularity, the technology rolled out in European countries can typically record and transmit at intervals of about 15 minutes. Concerning the communication technology used, current technology makes use of PLC technology to send data to the LV/MV gateways, where data is processed and moved over an IP connection to the distribution operator's enterprise network and servers. One possibility is to use ZigBee as a communication technology [3]. In the future, it is envisioned that data can be sent directly from the consumer's premises using 'open' (i.e., not dedicated) IP networks.

2.4 Regulatory and Policy Aspects

Given its vital role for the development of society and economy, energy is a strongly regulated sector. The energy system is indeed, together with finance, transport and telecommunications, recognised as a pillar on which Europe depends for its progress.

From the service chain standpoint, traditionally energy was run as a monopoly, with one incumbent company (typically state-owned) covering the whole service chain, from generation to transmission to distribution and to service provisioning. Driven by the belief that competition and less regulation could improve the economic efficiency of the energy sector, the EU mandated a number of regulations to open the energy market.

The key rules were set in EU directive 96/92/EC. According to such a directive, electricity consumers should be provided with the option to choose their electricity supplier. Management unbundling and accounting separation were foreseen as necessary means to ensure true competition in the service provisioning. Electricity networks, at the contrary, were still considered as natural monopolies and hence subject to regulations in provisioning fair access to the various electricity suppliers.

As generation is not strongly characterised as a natural monopoly, with various actors being active, opening up the electricity supply side led to the need of putting in place mechanism for ensuring efficiency and security of supply. This, in turn, led to the development of open electricity markets, which are currently in place in most EU-27 countries, and are run under principles of neutrality, transparency, objectivity and competition between producers, as well as of economically managing an adequate availability of reserve capacity. The creation of an electricity market responds to two specific requirements: (i) encouraging competition in the potentially competitive activities of electricity generation and sale, through the creation of a marketplace; (ii) favouring maximum efficiency in the management of electricity dispatching, through the creation of a market for the purchase of resources for the dispatching service.

In the last few years, the energy sector has been subject to a number of interventions by policy makers, all going in the direction of turning Europe into a low–carbon, sustainable economy and society. The European energy policy adopted by the European Council on 9 March 2007 on the basis of the Commission's Energy Package defines a comprehensive strategy aimed at achieving the three core energy objectives for Europe: sustainability, competitiveness, and security of supply. This was elicited in the European 20-20-20 Plan that targets a 20% cut on greenhouse gas emission, a 20% of energy consumption level covered by renewable energy sources and a 20% increase in energy efficiency, all this to be achieved by 2020 [4]. The trend was further reinforced by the adoption by the EC, on 15 December 2011, of the Communication "Energy Roadmap 2050" [5]. In such document, the EU commits to reducing greenhouse gas emissions to 80-95% below 1990 levels by 2050. Such Communication will play a pivotal role in developing a long-term pan-European framework for ensuring the growth of a sustainable, low-carbon European society.

2.5 Legal Aspects

Smart meters are currently subject to vibrant public debates in a number of EU countries, where the roll-out of smart meters is still on its way. Examples include the Netherlands and Germany. One of the key issues at stake in the debate is the possibility of identifying activities of consumers by applying advanced data mining techniques to smart meter data. It is interesting to remark that in countries where the roll-out has already been achieved (in particular, Italy and Sweden) such issues were never considered an obstacle for the deployment of the technology. There is, however, general consensus that smart meter data should be managed according to the provisions foreseen for "personal data". Recently, the European Data Protection Supervisor issued an opinion on the usage of smart meters' data [1], stating *"Stakeholders must be aware that processing of personal data in the context of smart grids/smart metering will have to fully comply with the national legislation transposing the relevant EU legislation, including Directive 95/46/EC, and – to the extent applicable – the e-Privacy Directive"*[2]

According to the EU directive 95/46/EC, personal data is defined as "any information relating to an identified or identifiable natural person('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Data subjects' rights are determined by a data controller (determines the purpose and means of processing) or a data processor (processes personal data on the behalf of a data controller) [6]. Collection of personal data is forbidden unless selectively allowed by law. This includes the case of explicit, specific legitimation, whereby, in our case, a DSO can state that smart metering data is necessary for preserving a societal interest (in this case, the overall stability of the power grid). However, even when allowed, the collection of personal data

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, p 37), as amended by Directives 2006/24/EC and 2009/136/EC.

is subject to limitation of purpose. Personal data collected for one specific purpose cannot be used for a different one. Additional purposes require a separate legitimation. Also, the entity collecting personal data should demonstrate that the collection of aforementioned data is necessary for achieving the specific purpose. Data subjects have, further, the right to access information on what data is stored and for what purpose. The data controller, at the same time, has the duty to inform the data subject about the information being collected and its intended use.

In time of big data and cloud computing, one important issue to address relates to the use of third-party services for storing/processing/analysing personal data (i.e., smart meter data in our case). EU directives distinguish between two roles. The first one, the data controller, is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determine the purposes and means of the processing of personal data". The second one, the data processor, is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". According to current legislation, the data controller is responsible for ensuring that data processor complies with the laws.

3 Research Challenges

In this section, we provide a short description of the main security and privacy challenges associated with smart grids.

3.1 Data Confidentiality

In the context of data confidentiality, the data exchanged and stored in the smart grids must be protected. In a smart grid, the major component that generates data is a smart meter. The smart meter collects data from smart appliances, providing information about energy consumption within a home. Generally, an energy supplier provides the usage tariff information, which is public information. The billing information, which is calculated as a function of energy consumption and usage tariff information, is also considered as confidential. In this regard, the research challenge is how to make energy consumption data confidential.

Furthermore, smart meter data can be used to devise forecast information of energy consumption. Such forecasts may be relevant for all actors in the delivery chain (GenCos, TSOs, DSOs) for the purpose of putting in place anticipatory control actions aimed at achieving load balancing. ESCOs can make use of such data, coupled with forecasts on market prices' evolution, to schedule smart appliances and optimise energy consumption. Forecasting services can be provided by third party companies, which shall be granted access to smart meter data. The forecast information must be protected since it may expose quite sensitive information about consumers and energy distributors. Here, the research challenge is how to make the forecast information of energy consumption confidential.

3.2 Privacy

Privacy can be defined as *the quality or condition of being secluded from the presence or view of others*[3]. In the context of smart grids, privacy of consumers means not to disclose their private data to anyone other than consented entities. Such private data may include consumer identification, address and energy usage information. In a smart grid, an energy supplier requires aggregated data within its region to calculate usage per region at a particular time. Such information can be shared with energy distributors. A load balancing module of an energy distributor considers this information for distributing energy as needed. The aggregated data should include data from sufficient number of consumers to ensure minimum privacy level. Here, we are referring to k-anonymity [7]. The larger k, the better is the privacy level; unfortunately, a smaller value of k might reveal significant information about consumption. The research challenge here is how to ensure privacy of consumers without relying on any (trusted) aggregator.

3.3 Trust

In a smart grid, the trust level can vary from fully trusted to untrusted entities [8]. Typically, a smart meter is considered fully trusted because it is equipped with a Trusted Platform Module (TPM) [9], where the cryptographic key is embedded in; while, the energy supplier is considered honest-but-curious (see e.g., [10–12]). The open research challenge is to construct a secure system even under the assumption that all entities are untrusted, thus guaranteeing the stronger level of trust. On the contrary, if we consider all entities trusted, any misbehaving entity may reveal private information.

3.4 Data Usage

By default, a consumer agrees to provide information about billing and aggregated energy consumption to energy suppliers. However, the legislation, such as EU Data Protection Directive [13], requires explicit consumers consent prior to processing data for purposes other than billing and aggregated energy consumption. In a smart grid system, both ESCOs and data users can get access to data only for the purpose for which consumers have given explicit consent, where consent can be withdrawn at any time [14]. Without explicit consent, data collection and usage may raise serious security concerns. Even if a consent is given (as considered in [15,16]), it is an open problem to ensure if the data is processed according to the given consent. This open problem is inherently present in the smart grid.

3.5 Fine-grained Access Controls

An authorised entity should be able to access only the requested data, thus following the principle of least privilege [17]. This problem becomes more challenging as we move from coarse-grained to fine-grained access controls, in particular

[3] `http://www.thefreedictionary.com/privacy`

access controls that are enforceable efficiently. The other problem is that access controls might reveal sensitive information about private data considering the enforcing entity (such as ESCOs) is semi-trusted (say honest-but-curious). It becomes an issue how access controls can be enforced without revealing information they are protecting [10, 18].

3.6 Tamper Resistance and Non-repudiation

In a smart grid, entities, such as energy suppliers and ESCOs, need assurance that the data coming over the communication network, say sent by smart meters, is not tampered. Furthermore, the data sender should not be able to repudiate. For instance, the billing information sent by smart meters or consumers must be neither tampered nor repudiable. Also, the data stored in data stores must be tamper resistance and non-repudiable. Ensuring both tamper resistance and non-repudation is not an issue if considered in isolation; however, it is a challenging problem if we consider it together with, in particular, privacy (as well as access controls and data confidentiality).

3.7 Availability

The server side components of the smart grid, such as energy suppliers and ESCOs, can made unavailable by mounting Denial-of-Service (DoS) attack, where an adversary sends a large number of requests. The attack could be more severe if a large number of machines generate bogus requests (also known as Distributed DoS attack - DDoS attack in short). Generally, the server side components of the smart grid perform tamper resistance and non-repudiation checks before they process the requests. Similarly, smart meters, home gateways and network gateways can also be made unavailable by mounting DoS/DDoS attack (by replaying legitimate traffic coming from the server side components of the smart grid). The open issue is how to withstand against DoS/DDoS attacks in order to ensure availability of all components within a smart grid.

3.8 Transparent Auditing and Verifiability

In a smart grid, consumers should be able to verify that they are charged according to what (duration) and when (peak or off-peak) they consume energy; and they are not overpaying. On the one hand, energy suppliers should be able to ensure that consumers are paying according to what and when they consume energy. The monetary incentive for consumers is to show lower consumption than actual and to replace consumption during peak hours with off-peak hours. On the other hand, the monetary incentive for energy suppliers could be to do exactly the other way around i.e., to show higher consumption than actual and to replace consumption during off-peak hours with peak hours. The solution to this challenging problem requires an efficient scheme that can offer transparent auditing mechanism which should allow both consumers and energy suppliers to do the verification. Generally, the auditing problem, whether the received data in response of a request is correct or not, holds for communication between any two entities in the smart grid. The verification process should require limited and fine-grained access to the data to be verified. Before and after the verification or auditing, the data should still be protected without compromising privacy of consumers.

There is a lot of research (as discussed in the following section) on addressing the individual challenges; however, there is no work for holistically targeting main security and privacy challenges related to smart grids. In short, the open problem is to address all above research challenges holistically, instead of in isolation, thus leading to the development of a secure data management framework able to cover the whole life-cycle of energy data.

4 Related Work

There is already a lot of research on how privacy of households can be violated from their energy consumption profile [19–21]. In order to preserve privacy, there are solutions both with and without trusted third party for data aggregation [22]. Efthymiou and Kalogridis [23] describe a secure mechanism for anonymising metering data sent by a smart meter. Unfortunately, their security mechanism assumes a trusted escrow services to aggregate the data to be anonymised. Moreover, they leave open the problem of forensic analysis, where a faulty smart meter needs to be replaced or when a new meter is installed. Molina-Markham *et al.* [21] propose an architecture assuming the smart meter as a prover, the energy (or power such as electricity, gas or water) trace as a secret. Their proposed protocol lets the smart meter report its billing without under-reporting its usage. The protocol provides aggregated information including neighbouring consumption information to the energy supplier. The energy supplier needs such information for predicting the future demand. Like [23], they merely transfer the trust to the neighbouring gateways. Moreover, it is not clear how to perform forensic analysis in case of investigations. Acs and Castelluccia [8] propose DREAM, a light-weight privacy-preserving smart metering system for data collection and aggregation. The main idea behind DREAM is to add noise to the data. DREAM does not rely on a third-party to aggregate the data. They assume that smart meters in an area communicate not only with the energy suppliers but also with each other and they send the metering data. The main issue with this scheme is that a single malfunctioning or malicious smart meter can make the metering data irrecoverable. In other words, smart meters rely on each other for successful data recovery at the energy supplier end.

Jawurek *et al.* [9] list requirements of the smart energy system and propose a scheme to protect privacy leakage through the smart metering billing. In their scheme, an additional privacy component is plugged with the smart meter to protect privacy of the metering data. The privacy component sends only the billing information with the signed commitment to the energy supplier. The commitments are signed by the smart meter and can be verified by the energy supplier. This scheme can calculate billing with linear tariff consumption. Rial and Danezis [24] extend the idea for calculating non-linear tariff consumption with further optimisations. However, in both schemes [9, 24], the energy supplier does not get any information about how much energy was consumed at any time, the information necessary for load balancing at distributor ends.

In terms of data collection and usage, Sundramoorthy *et al.* [25] describe design concerns of domestic energy-monitoring systems. They address how a piece of data is collected, stored and analysed and who are the data processors or data controllers. Anderson and Fuloria [26] provide an analysis based on security economy of electricity metering. They describe historical background and provide some recommendations. One main recommendation is that smart meters data should send data only to energy supplier and only be for billing purpose. For sending smart meter data to any other entity or for any other purpose, the consumer's consent should be captured. There are some approaches that can capture consent in an automated manner [15, 16].

Smart grid security requires a holistic solution [27]. There are partial solutions proposed in the state of the art; however, the area still requires great attention of researchers for proposing a holistic solution not only from security and privacy aspects but also from regulatory aspects (e.g., NIST regulations [28] and EU regulations [29]). Both [30] and [31] broadly describe the trust, security and privacy issues in smart grid systems. McDaniel and Smith [32] emphasise the importance of hacking and exploiting vulnerabilities in smart meters for monetary purposes and briefly explain the privacy concerns. Kostyk and Herker [33] provide a brief overview of emerging smart grids. Baumeister [34] reviews and categories literature on smart grid security.

In summary, there are in principle solutions proposed to each single research challenge described in Section 3. However, their integration into a holistic secure energy data management framework is far from trivial, and is considered to require considerable research efforts by the relevant scientific communities.

5 Conclusions

In this paper, we outlined and surveyed the most relevant data security and privacy issues arising in a smart grid scenario. While solutions able to (at least partially) tackle each of the identified issues have been proposed in the literature, we are still far from devising a coherent and integrated framework capable of ensuring security and privacy of smart grid energy data.

This paper represents a call to action to the scientific communities active on data security and privacy, presenting them with an analysis of the most relevant challenges ahead and urging them to lay the scientific foundations for enabling the development of novel solutions able to tackle the identified issues in a holistic fashion.

Acknowledgements

This work was partially supported by EIT ICT Labs (http://www.eitictlabs.eu/) within the Action Line on Smart Energy Systems.

References

1. NIST, "Smart grid: A beginner's guide." http://www.nist.gov/smartgrid/beginnersguide.cfm. Last accessed: 28 October 2012.
2. Wiki, "Smart meter." http://en.wikipedia.org/wiki/File:Intelligenter_zaehler-_Smart_meter.jpg. Last accessed: 18 February 2013.
3. D.-M. Han and J.-H. Lim, "Design and implementation of smart home energy management systems based on zigbee," *Consumer Electronics, IEEE Transactions on*, vol. 56, pp. 1417 –1425, aug. 2010.
4. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010)639, "Energy 2020 a strategy for competitive, sustainable and secure energy," Oct. 2010.
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011)885, "Energy roadmap 2050," Dec. 2011.
6. R. Massey and M. Russo, "Clarification of data controller and data processor under eu privacy directive new opinion of article 29 data protection working party." http://www.mwe.com/publications/uniEntity.aspx?xpST=PublicationDetail&pub=4959. Last accessed: 18 February 2013.
7. L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.
8. G. Ács and C. Castelluccia, "Dream: Differentially private smart metering," *CoRR*, vol. abs/1201.2531, 2012.
9. M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-in privacy for smart metering billing," in *Privacy Enhancing Technologies* (S. Fischer-Hbner and N. Hopper, eds.), vol. 6794 of *Lecture Notes in Computer Science*, pp. 192–210, Springer Berlin / Heidelberg, 2011.
10. M. R. Asghar, M. Ion, G. Russello, and B. Crispo, "ESPOON: Enforcing Encrypted Security Policies in Outsourced Environments," in *The Sixth International Conference on Availability, Reliability and Security*, ARES'11, pp. 99–108, August 2011.
11. M. R. Asghar, G. Russello, and B. Crispo, "Poster: ESPOON$_{ERBAC}$: Enforcing security policies in outsourced environments with encrypted RBAC," in *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pp. 841–844, ACM, 2011.
12. M. Asghar, M. Ion, G. Russello, and B. Crispo, "Securing data provenance in the cloud," in *Open Problems in Network Security* (J. Camenisch and D. Kesdogan, eds.), vol. 7039 of *Lecture Notes in Computer Science*, pp. 145–160, Springer Berlin / Heidelberg, 2012.
13. E. Communities, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, November 1995. Last accessed: 27 October 2012.

14. "Personal data protection act." http://www.dutchdpa.nl/Pages/en_wetten_wbp.aspx, November 1999. Last accessed: 29 October 2012.
15. M. Asghar and G. Russello, "Flexible and dynamic consent-capturing," in *Open Problems in Network Security* (J. Camenisch and D. Kesdogan, eds.), vol. 7039 of *Lecture Notes in Computer Science*, pp. 119–131, Springer Berlin / Heidelberg, 2012.
16. M. Asghar and G. Russello, "Actors: A goal-driven approach for capturing and managing consent in e-health systems," in *IEEE International Symposium on Policies for Distributed Systems and Networks*, POLICY'12, pp. 61–69, July 2012.
17. J. Saltzer and M. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975.
18. M. R. Asghar, M. Ion, G. Russello, and B. Crispo, "ESPOON$_{ERBAC}$: Enforcing security policies in outsourced environments," *Computers & Security*, 2012.
19. G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design," *Energy and Buildings*, vol. 35, no. 8, pp. 821–841, 2003.
20. E. Quinn, "Privacy and the new energy infrastructure," *Available at SSRN 1370731*, 2009.
21. A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, BuildSys '10, (New York, NY, USA), pp. 61–66, ACM, 2010.
22. J. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, pp. 1–5, IEEE, 2010.
23. C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *First IEEE International Conference on Smart Grid Communications*, SmartGridComm'10, pp. 238–243, October 2010.
24. A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, WPES '11, (New York, NY, USA), pp. 49–60, ACM, 2011.
25. V. Sundramoorthy, G. Cooper, N. Linge, and Q. Liu, "Domesticating energy-monitoring systems: Challenges and design concerns," *IEEE Pervasive Computing*, vol. 10, pp. 20–27, 2011.
26. R. Anderson and S. Fuloria, "On the security economics of electricity metering," in *WEIS*, 2010.
27. A. Metke and R. Ekl, "Security technology for smart grid networks," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 99–107, 2010.
28. A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements." http://www.meits.us/MEITS-SECURE/MS-EAP/Download/Cyber_Security_Coordination_Task_Group.pdf, September 2009. Last accessed on: 28 August 2012.
29. V. Annex, "Smart grid security." http://www.thecre.com/fisma/wp-content/uploads/2012/07/ENISA_Annex-V-Smart-grid-Security-Related-Initiatives.pdf, March 2012. Last accessed: 25 October 2012.
30. H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, pp. 81–85, 2010.
31. A. Cavoukian, J. Polonetsky, and C. Wolf, "Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, 2010.

32. P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *Security & Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.
33. T. Kostyk and J. Herkert, “Societal implications of the emerging smart grid,” *Commun. ACM*, vol. 55, pp. 34–36, Nov. 2012.
34. T. Baumeister, “Literature review on smart grid cyber security,” tech. rep., Collaborative Software Development Laboratory, Department of Information and Computer Sciences, University of Hawaii, December 2010. Last accessed: 28 October 2012.