Security Challenges of a Changing Energy Landscape

Marek Jawurek · Martin Johns

Vincenz-Priessnitz-Straße 1, 76131 Karlsruhe, Germany SAP Research
{marek.jawurek | martin.johns}@sap.com

Abstract

The German electric energy industry is under change. The Smart Grid, Smart Metering and

electric mobility are being researched and implemented. It will have implications for the security and privacy of our every-day-lives if security and privacy are not taken into account during this

change. Therefore the identification and mitigation of security and privacy issues of prospective technologies is essential before respective systems are built. In this paper we identify the current legislative measures to induce change, derive the necessary technical changes and analyze them with respect to security and privacy challenges. We identify several security and privacy challenges: New paradigms like mobile energy consumers or bidirectional communication with electrical meters, isolated

systems like Industrial Control Systems or Home Automation Networks that will eventually be connected to public networks and huge amounts of privacy-related data that will be created by respective systems. We conclude that the energy sector is an interesting field for security and privacy research and that now is the time to ensure a secure and private future of energy supply.

1 Motivation

In ten years, we drive electric cars with renewable energy. We are now at the point in time where we, as security researchers, need to ensure that this will happen in a secure and privacy-aware manner.

Due to legal and technological changes the electric energy industry is changing rapidly at this very moment to accommodate topics like volatile renewable generation, electric mobility on a wide scale or consumer load shifting while still maintaining stability, affordable electric energy and safety for our society. For the realization of these topics IT-systems will play a crucial role and their security will in turn play a crucial role for the safety of electrical grids. Security in IT-systems for the energy industry is a very interesting topic, as these systems will unlock certain markets for the energy industry that will have impact on our every-day-life and as currently many new technologies are explored in research projects. Different constraints make this endeavour challenging: legal constraints, safety, availability and real-time requirements, the heterogeneity of involved players and the variety of potentially malicious users and their attack vectors.

In this work we list the relevant legal changes for the German energy sector and derive resulting changes for its IT-systems. Based on these prognosed changes we identify emerging security

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2010), 1-11

challenges that need to be taken into account now in order to ensure a secure and privacy-aware transformation of the energy sector.

The rest of this paper is structured as follows: Firstly, we list several legislative impulses and their affect on the energy landscape with the help of three snapshots in Section 2. Secondly, in Section 3, we analyze the potential resulting changes in IT-systems. In Section 4 we depict which security challenges can be deducted from the aforementioned changes in IT-systems and give some specific new attack vectors. Finally, after reviewing related work (Section 5), in Section 6 we conclude with a summary.

2 The Energy Landscape under Change

The energy landscape has been under major change in Germany since 1999 although first groundwork was already laid as early as 1991. These changes are mainly driven by politics which in turn realize standards set by the European union and its road map for the energy sector [EUCO06]. The following is an incomplete list of legal changes that have been mayor drivers for the change of the energy sector:

L1: Liberalization of energy markets: The goal of liberalization was to enable energy consumers to introduce competition into the energy sector and thereby foster efficiency and economic viability. What was previously considered a natural monopoly was divided into pieces where the only natural monopoly, the transport of energy, was subjected to regulation. Vertically organized corporations that owned the whole value-chain from production over transport to sales had to unbundle their operations to correspond to roles that the legislation created. See [Krisp07] for a detailed analysis of legal change.

L2: Support for the decentralized generation of renewable energy: Since 1991 several financial and legal measures were introduced by the legislative to support the decentralized production of renewable electrical energy. The implemented measures have led to an increased amount of decentrally produced renewable energy [BMUE10].

L3: Further liberalization of meter operations: In 2008 a law introduced two new roles for the area of meter installation, operation and meter reading: The metering point operator is responsible for installation, operation and maintenance of the meter while the measurement services provider is responsible for reading the data off the meter and transferring it to respective authorized receivers [GeLe08].

L4: Introduction of Smart Meters: Houses that are newly-connected to the electrical grid or that have been renovated since 2010 must be equipped with a special meter (§21b of [GeLe05]). Although, remote-reading is not mentioned as a requirement in the law, metering point operators want to upgrade directly to full Smart Meters with remote-reading capability (advanced metering).

L5: Free choice of metering point operator: According to §21b (2) of [GeLe05] house-owners have the choice of metering point operator. The metering point operator has to use a meter that fulfils the legal requirements and the technical requirements of the local grid operator.

L6: Tariffs to encourage energy saving: From end of 2010 energy suppliers must offer at least one tariff that supports the saving of energy. This might either be a load-dependent or a time-dependent tariff (§ 40 (3) of [GeLe05]). This might support L4 in the wide-scale distribution of Smart Meters as load/time-dependent metering requires this hardware.

L7: Legislative support for the introduction of electric mobility: Following their development plan for electric mobility [GeGo09] the German government created a research framework program for electric mobility [BMWi09]. The idea is to foster research programs that deal with electric cars and the necessary infrastructures.

After having depicted the legal measures introduced to make change happen the following three sections 2.1, 2.2 and 2.3 describe different stages, before, in the mid of and after the introduced change. They will help us to identify (Section 3) the emerging changes in technology that might have security implications (Section 4).

2.1 Yesterday: Few Players, Strong Ties

We consider the year 1990 for our 'Yesterday'-scenario. Energy markets were considered natural monopolies. That means, it was taken for granted that one corporation owned the local distribution grid and had a monopoly on the energy supply to the residents and industries of that area.

Back then energy was produced, transported, distributed and sold by few big integrated corporations. As they held the whole value chain this had mayor consequences for the structure of the market, the customers and the internal processes. Only few actors were active in the market with clearly defined areas of influence.

As energy suppliers were integrated corporations and produced for own use their power plants did not need interaction and were controlled by isolated computer systems with manual interaction: Industrial control systems (ICS). Demand control of major consumers of energy was performed via telephone.

Metering was performed with Ferraris meters and meters were read manually either by a representative of the supplier or by the customer himself. Customers had usually one fixed price for energy that did not change over the course of the day or year and had no way of knowing the current demand.

Decentralized generation of energy from renewable sources was effectively non-existent with only 3.1% of Germany's total demand fulfilled by renewable energy [BMUE10] (Table 5).

Electric mobility, as in electric cars, scooters or buses was nearly non-existent.

2.2 Today: Totally Liberalized ...

We consider the year 2010 for our 'Today'-scenario. Energy markets are liberalized and unbundled where possible. Liberalization led to the emergence of more suppliers who procure energy either directly over-the-counter from producers or at energy stock markets like the EEX. Customers have the choice of supplier independent of the customer's/supplier's location.

The control of demand still works like in the 'Yesterday'-scenario with one important addition. Consumers of large amounts of energy participate directly in the trade of energy and control their demand in response to market prices.

From 2010 on, owners can choose to equip newly built or renovated houses with Smart Meters (see [WoCP09] for a short definition). Different research and commercial projects are deploying Smart Meters [SMPM10] and allow residents to view real-time energy consumption data [Yello10]. Some research projects also try to figure out how volatile prices induce changed customer behaviour [PrIn10] or how controllable devices on the consumer side can be leveraged by suppliers to shift loads [PMRe10].

Decentralized generation of energy from renewable sources is currently emerging. Energy generated from renewable sources in Germany amounts to 16.1% of Germany's total demand in 2010 [BMUE10].

Electric mobility is being supported by the government with a research program framework [BMWi09] Car manufacturers and energy corporations are researching the integration of electric mobility into the Smart Grid (see [WoCP09] for a short definition) of the future in [PMRM10].

2.3 Tomorrow: Smart Grid Utopia

We consider the year 2020 for our 'Tomorrow'-scenario. For this scenario we base our predictions conclusions on the legal changes being introduced as laid out in Section 2 and experience from research programs where we actively participate. Expected developments are marked with H1.. HN standing for hypothesis 1 to N to be referenced later:

H1: The proportion of renewably generated energy will increase further. The volatile nature of renewable generation will put a significant strain on the grid. Therefore controllable generators will be tied to the smart meter and can be part of a controllable virtual power plant (see H2).

H2: The market will feature more market roles, those that have been realized so far in the 'Today'-scenario, those that are being introduced in L4 and those that probably will be introduced by electric mobility. Electric mobility might necessitate roles for the provisioning of mobility services across electric grid boundaries with support of roaming similar to roaming in the mobile telephony market, e.g. electric mobility provider. Roaming across different electric grids and national borders might also necessitate independent third parties that facilitate this roaming by transparently providing services for international billing and other bookkeeping tasks, e.g. clearing houses. The installation and operation of charging points could be handled by charging point operators. With an increasing amount of devices participating in demand response an aggregation role could simplify communication: the demand side manager. The demand side manager has a number of controllable appliances under his command and sells this potential in load change to customers like suppliers or grid operators. On the other hand, a virtual power plant (run by an aggregator company) [FENI10] role will do this for decentral producers of generators.

H3: Demand response for big consumers will probably be entirely controlled by the market price and direct procurement of energy by the big consumer. However, demand response (the response of the demand side to loads on the grid) could be a beneficial endeavour for small/medium enterprises and even for consumers. Alternatively it could be made a requirement as the strain on the grids will increase due to H7 and H1. That means, that appliances can be scheduled to run at

a specific time or be delayed during times of high demand. At consumer level dishwashers, refrigerators or washing machines could be scheduled / delayed by a demand side manager inside the parameters given by the owner (e.g. wash dishes until 8 pm).

H4: It can be expected that every household will be equipped with a Smart Meter and that this Smart Meter will be remotely-readable, manageable and upgradeable (L4). This will enable energy prices for end-users that are either load-dependent or time-dependent (L6). The Smart Meter will be act as a gateway for receiving and forwarding price/control signals from demand side managers/aggregators/grid operators to appliances in Home Automation Networks (HANs).

H5: An integration of the Smart Meter with the HAN will enable residents to get direct feedback regarding the current energy usage of their appliances and the current energy price. In addition to that, residents of houses equipped in this manner will be able to 'program' their appliances and plan their usage patterns either in compliance with their supply contract or in expectation of future market prices.

H6: Electric mobility will be deployed one a wide scale [GeGo09]. Advances in technology will make up for low range/long charging times. For instance, travel schedules derived from commuting habits and personal/professional calendars could help to plan charging along the day's route and respective charging points could be reserved. Charge points will be distributed on a wide scale and most of them will also offer cars to introduce energy back into the grid to provide service to the grid as a storage system, bundled together by aggregators.

H7: Due to a large amount of new, potentially autonomous, devices connected to the grid that will allow controlled generation, storage and demand the current management of the grid will not be feasible anymore. Old power plant management systems, 'old' grid control devices and new devices must become inter-connected to allow shifts in demand and supply in order to ensure stability, economic viability and environmental sustainability.

3 Emerging Technological Changes

In this Section we attempt to analyze the intermediate impact the legal changes and the changes we observe between today and the predicted 'Tomorrow'-scenario will likely have on IT systems.

3.1 More Communication Relationships with Heterogeneous Partners

Due to L1 already in the 'Today'-scenario we see more roles in the energy market than we had in the 'Yesterday'-scenario. From L3 and some predictions in H2 we can see that the market of the future will feature even more different roles with potentially many companies fulfilling these roles. That means, that some roles will communicate with a number of different (w.r.t. role) partners which implicates different communication protocols/interfaces and therefore more involved IT-systems.

3.2 Interfaces where No Interfaces Existed Before

Newly introduced interfaces between different systems always involve a significant amount of work and coordination (w.r.t. standardization). However, these interfaces could be of utmost importance to a successful realization of the Smart Grid and surrounding technologies:

- Old legacy ICS systems (Section 2.1), were never meant to be connected to the outside of the power plant [RIPT01]. Despite that, [RIPT01] states that ICS in fact are already connected to corporate networks as management habits change and engineers monitor their systems remotely.
- Suppliers used to enter customer's consumption data into their billing systems manually. But indirection of meter data reading by measurement service providers (L3) and the change in type of data (from kWh to energy usage profiles L6 in high resolution) implicate that supplier's billing systems must offer automatic interfaces for measurement services provider to transmit these profiles.
- HANs will form an important basis for the Smart Grid as the network of controllable appliances with a Smart Meter as gateway to the Smart Grid. The necessary connections between HANs and Smart Meters for this purpose have to be analyzed and standardized.

3.3 New Communication Paradigms

New communication paradigms will dramatically change the way IT-systems operate in the energy sector:

- Communication will not be unidirectional anymore (H3), but control/price signals will be send back to the consumer.
- With emerging electric mobility (see H6) a great number of energy consumers will not be bound to a specific location anymore. As a plug-in hybrid electric vehicle (PHEV) moves around and charges at different charging points the communication endpoint for its mobility provider or other necessary communication partners moves around as well. A clearinghouse might mitigate the number of involved communication parties (see H2) but the location will still implicate the local communication partners (charging point operators, grid operators). These systems must accommodate for international roaming and differently structured energy markets in different countries.

3.4 High Amounts of Privacy Related Data

Due to the ability of Smart Meters to record fine grained profiles of energy consumption (see L4) and the necessity to do so (see L6) huge amounts of data will arrive at suppliers' IT-systems eventually. Legally imposed data retention times will only worsen the situation.

Electric mobility also creates additional data tuples: Data about when and where someone charged a certain car and where he plans to go (reservations of charging points).

3.5 Overarching Architecture

The idea of the Smart Grid implicates some form of intelligence in the grid. Because central intelligence is just not feasible for a grid of this size a way must be found to decentrally control the whole either directly with control messages or indirectly with incentives and market prices.

4 Security Challenges

In this Section we derive the security challenges that are implicated by the emerging changes for IT-systems from Section 3. For every area of changes as laid out in Section 3 a corresponding subsection provides the respective security implications.

4.1 More Communication Relationships with Heterogeneous Partners

Automated communication relationships with heterogeneous partners implicate several severe IT-security challenges. Due to the high numbers of (potentially changing) partners ensuring authenticity of a communication partner is not trivial. This relates to the actual technology used (e.g. PKI, shared secrets) to protect against attacks aimed at the technology and it also relates to keeping respective connection details up-to-date (e.g. contact persons, telephone numbers) to protect from social engineering attacks. Authorization for data/system access has to be crafted to every specific role/company and has to be managed over the lifetime of the communication relationship. Special care has to be given privacy related data which is, at least in German, subject to data privacy law w.r.t. creation, transport and alteration.

4.2 Interfaces where No Interfaces Existed Before

As already mentioned in Section 3.2 ICS were not designed to be connected to public networks but in fact are connected to corporate networks which in turn have connection to public networks. They have not been designed and implemented with a remote attacker model in mind and therefore contain blatant vulnerabilities [WeFS06]. Changing the systems appropriately might face a severe problem: There are few control system security experts available [Weis09]. The point which makes this security challenge so significant is that these systems control important real-life systems like coal plants but also critical systems like nuclear power plants or hydro power stations. Failure of these facilities might result in loss of money, infrastructure or even lives. The software interfaces constitute another attack vector which could be used for mischief, extortion or terrorism.

The fact that billing systems (and other systems) need to be interfaced opens up attack vectors similar to those in Web Security: Data that is transmitted must not be trusted and handled as potentially malicious data to protect from injection attacks. These attacks must not necessarily originate from the transmitting system but could come from transitively connected IT-systems.

The connection of Home Automation Networks (HANs) and Smart Meter (H5) also implicates several challenges: Apart from the obvious challenges like standards for their communication and the correct implementations of these standards the linking of HAN and Smart Meter connects the HAN to other networks. This is a similar situation as with ICS systems (HAN and ICS systems are similar in the way that both control physical devices). The HAN was probably not designed to be connected in such a way and furthermore it now also has several masters - the home owner via his legacy interaction methods and the party that would like to control appliances inside the HAN. Authentication, authorization, trust and privacy issues emerge.

4.3 New Communication Paradigms

The new communication direction of the emerging bidirectional communication, from demand side managers/suppliers to customers brings interesting challenges: The Smart Meter (or the HAN controller) must be able to authenticate and authorize the commands that enter the HAN from outside (w.r.t. the view of the customer). The Smart Meter might play the role of a firewall for the HAN.

With respect to control/price signals the sender of these signals must employ measures to ensure safe transport and to prevent repudiation of receipt. Otherwise, the customer could try to commit fraud by intercepting the signals and pretending that they never arrived. Fallback handling has to be developed for times of accidental loss of communication connection. Confidentiality of (existence of) these signals should also be preserved. By intercepting control signals attacker might either deduct appliances in use at the receiver's house or, even worse, deduct times of absence: When the residents are on vacation their washing machines will not require scheduling and therefore will not receive signals.

The mobility of energy consumers opens up a whole new field for IT although solutions could be heavily borrowed from the mobile phone industry: The mobility requires an authorization and billing infrastructure that features high-availability and confidentiality and potentially spans several countries or whole continents. Here it is crucial to keep costs of such infrastructures low (without sacrificing security) as the profits from mobile charging will also be significantly lower than with conventional refueling. The actual charging procedures and systems must ensure that neither involved parties can commit fraud (charging point operator by simulating a charging procedure, the customer by repudiation, supplier by claiming false charging records) nor that outsiders threaten the acceptance of electric vehicles by attacking the availability/credibility of the system.

4.4 High Amounts of Privacy Related Data

The problem about this data is that it can be used to create personal profiles of residents and can be subject to national data privacy laws which can differ from country to country. The energy usage profiles indicate when people wake up/go to bed, when and if they cook and whether they stay at home or go out at nights [Sulta91]. The data might also indicate how appliances are used [BaSL09].

Electric mobility creates even more privacy related data. Information about the position of past and future charges could be used for extortion (husband at unambiguous location) or industrial espionage (employee of company Y at headquarters of company X).

It is crucial that architectures (or organizational measures) that are developed for the handling of this data account for its importance and prevent leakage of data to unauthorized parties or retention times longer than necessary.

4.5 Overarching Architecture

Security challenges related to the overarching architecture are very hard to predict. It is safe to say that it will face the same challenges that all distributed systems face w.r.t. security. One point that

should be stressed here is the following: When the Smart Grid is fully realized it will probably be the largest logical network of embedded devices (charging cars H6 and Smart Meters H4), control systems (ICS) (H7) and traditional IT-systems with a real impact on our everyday-life [CISC09]. That means, that a failure of such a system, however it was produced, would lead to a complete standstill of our society, unlike with similar networks (mobile phones, the Internet). Containment strategies of the implemented controls have to be devised in order to limit the impact range of attacks/failures. The idea to support decentralized generation (L2) will already facilitate this.

5 Related Work

We could identify several areas of related work: Firstly, there are several articles that identify risks for the Advanced Metering Infrastructure (AMI)/Smart Grid superficially [GaRo08] and [CISC09], in more depth [Anton09], [KHLF10], [ASAP10] and [OoLT09] and for specific systems (Dutch Smart Metering) [RoKe08]. [ASAP09] identifies very detailed relevant components of AMI systems and provides guidance on how to secure them. However, we did not find any work on the integration of an infrastructure for electric mobility into the Smart Grid.

Secondly, the area of ICS security is covered by [WeFS06] which describes the vulnerabilities that were found in different ICS systems under analysis, by a NIST recommendation/guide [ScSF08] on how to secure ICS systems and by a short blog post in [DaBo10] at 2009/12/16 indicating the differences between traditional IT-systems and ICS systems.

Thirdly, privacy of Smart Grids in particular is discussed shortly in [McMc09], [ASAP10] and very detailed in [WoCP09]. The 'Smart Grid Security Blog' [DaBo10] is also a wealthy source of information regarding the security of the Smart Grid.

However, we could not find related work that deals with the integration of electric mobility into Smart Grids and with privacy and security issues of electric mobility.

6 Conclusion

From legislative measures implemented by the German government to fulfill a European/German agenda for technical/organizational evolution in the energy sector and from data regarding the future of electric mobility [WWFD09] and data about the proportion of renewable energies [BMUE10] we derive emerging changes in relevant technical systems. Based on these changes we identify implications for the security of these and of new technical systems.

In particular we identify the need for communication protocols and a corresponding infrastructure that allows secure and privacy-aware roaming of electricity consumers (electric vehicles) and their integration into the Smart Grid. Ideas for this infrastructure could be borrowed from mobile telecommunication solutions but must account for the differences between the domains and for differences in energy industries of different countries. Furthermore, we identify two fields where legacy technological systems will be connected to public networks although they have not been designed for this. Industrial Control Systems and Home Automation Networks were designed to work isolated from other networks but will be connected to the Smart Grid to fully unlock its potential. The problem of data privacy spans all identified new problem areas. As IT-systems will operate the energy industry of the future, the collection, transport and processing of

huge amounts of data will become feasible and interested parties might either experiment carelessly with this data or even try to capitalize on it.

Finally, we point out that the Smart Grid will form one of the largest networks with every-day-life physical implications in case of failure or successful attack. Interestingly enough, we are at a point in time where things are still in development and where research and development of security and privacy solutions for the respective areas will have an impact.

7 Acknowledgment

Martin Johns' work in this paper was partly funded by the German Federal Ministry of Economics and Technology (BMWi) as part of the e-mobility project with reference number 01ME09012.

Marek Jawurek's work in this paper was partly funded by the German Federal Ministry of Economics and Technology (BMWi) as part of the MEREGIOmobil project with reference number 01ME09007.

References

[Anton09] Antoniadis, Denise: Identify Inherent Security Risks: Advanced Metering Infrastructure and Smart Meters. 2009.

[ASAP09] The Advanced Security Acceleration Project (ASAP-SG): Security Profile for Advanced Metering Infrastructure. Technical report, December 2009.

[ASAP10] Advanced Security Acceleration Project (ASAP) – Smart Grid The Cyber Security Coordination Task Group: Smart Grid Cyber Security Strategy and Requirements. February 2010.

[BaSL09] Bauer, Gerald, Stockinger, Karl, Lukowicz, Paul: Recognizing the Use-Mode of Kitchen Appliances from Their Current Consumption. In EuroSSC, 2009, pages 163–176.

[BMUE10] Naturschutz und Reaktorsicherheit (BMU) Bundesministerium für Umwelt: Entwicklung der erneuerbaren Energien in Deutschland 1990-2009. 2010.

[BMWi09] BMWi. IKT für Elektromobilität. http://www.ikt-em.de/de, 2009.

[CISC09] CISCO: Securing the Smart Grid. Technical report, 2009.

[DaBo10] Danahy, Jack, Bochman, Andy: The Smart Grid Security Blog. http://smartgridsecurity.blogspot.com/, 2010.

[EUCO06] EU Commission: European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future. Technical report, 2006.

[FENI10] The FENIX Project. Flexible Electricity Network to Integrate the eXpected 'energy revolution'. http://www.fenix-project.org/, 2010.

[GaRo08] Garrison Stuber, Michael, Robinson, R. Eric: Advanced Metering Infrastructure Risk Analysis for Advanced Metering. Technical report, 2008.

[GeGo09] German Government: Nationaler Entwicklungsplan Elektromobilität der Bundesregierung. August 2009.

[GeLe05] German Legislation: Energiewirtschaftsgesetz. 2005.

[GeLe08] German Legislation: Gesetz zur Offnung des Messwesens bei Strom und Gas für Wettbewerb. September 2008.

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

[Krisp07] Krisp, Annika: Der deutsche Strommarkt in Europa : Zwischen Wettbewerb und Klimaschutz. PhD thesis, 2007.

[McMc09] McDaniel, Patrick, McLaughlin, Stephen: Security and Privacy Challenges in the Smart Grid. In: IEEE Security and Privacy, pages 7:75–77, 2009.

[OoLT09] M. Oostdijk G. Lenzini, W. Teeuw: Trust, Security, and Privacy for the Adanced Metering Infrastructure. Technical report, July 2009.

[PrIn10] Project Intelliekon: http://intelliekon.de/intelliekon, 2010.

[PMRe10] Project MeRegio. http://meregio.forschung.kit.edu/, 2010.

[PMRM10] Project MeRegioMobil. http://meregiomobil.forschung.kit.edu/, 2010.

[RIPT01] Riptech Inc.: Understanding SCADA System Security Vulnerabilities. http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf, January 2001.

[RoKe08] Roos, Bart, Keeming, Sander: Security analysis of Dutch smart metering systems. Technical report, July 2008.

[ScSF08] Scarfone, Karen, Stouffer, Keith, Falco, Joe: Guide to Industrial Control Systems (ICS) Security. Technical report, September 2008.

[SMPM10] Smart Metering Projects Map http://maps.google.com/maps/ms?ie=UTF8\&oe=UTF8\&msa=0\&msid=115519311058367534348.0000011362ac6d7d21187, 2010.

[Sulta91] F. Sultanem: Using appliance signatures for monitoring residential loads at meter panel level. In: Power Delivery, IEEE Transactions on, 6(4):1380 –1385, October 1991.

[WeFS06] Wells, Rita A., Fink, Raymend K., Spencer, David F.: Lessons learned from Cyber Security Assessments of SCADA and Energy Management Systems. Technical report, September 2006.

[Weis09] Weiss, Joe: Cyber Security of Industrial Control Systems for Air Force and other Military Bases. June 2009.

[WoCP09] Wolf, Christopher, Cavoukian, Ann, Polenetsky, Jules: SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. November 2009.

[WWFD09] WWF Deutschland. Auswirkungen von Elektroautos auf den Kraftwerkspark und die CO2-Emissionen in Deutschland. March 2009.

[Yello10] Yellow Strom GmbH: Seeing and controlling electricity. http://google.yellostrom.de/index_en.php, 2010.