Security and Privacy in the Smart Energy Grid

Martin Erich Jobst
Supervisor: Dipl.-Inform. Andreas Müller
Autonomous Communication Networks (ACN) 2013
Chair for Network Architectures and Services
Department for Computer Science, Technische Universität München
martin.jobst@tum.de

ABSTRACT

A major part in the efforts to increase energy efficiency is the establishment of a smart energy grid. This is supposed to optimize power distribution and facilitate the delivery of fluctuating renewable energy. For these reasons, governments in the EU and US are pressing ahead with legislation for the introduction of smart meters into every household. The precise consumption measurements taken by smart meters, however, also have the potential to significantly affect consumer privacy. In addition, there are great security concerns, due to the sensitivity of the data processed by smart meters, as well as their extensive remote control capabilities. This paper gives an overview about these threats and discusses several possible solutions and countermeasures.

Keywords

Security, Privacy, Smart Grid, Smart Meter, Virtualization, VMI

1. INTRODUCTION

Smart metering devices or *smart meters* for short are able to offer many new features and services to both end-users and electric companies. They are able to provide far more detailed power readings than conventional electricity meters. Thus, smart meters are supposed to be able to assist in energy saving efforts by identifying different kinds of loads. By linking smart meters together with existing electrical power infrastructure, they create a so-called *smart energy grid* or simply *smart grid*. This enables electricity providers to remotely control and coordinate home appliances, like washing machines or dishwashers, to avoid times of peak demand. In addition, it permits small power plants to regulate their energy generation according to the current load by receiving information from the smart grid. These measures are especially important for accommodating the growing amount of fluctuating renewable energy in the power grid. All these new features, however, give rise to quite a number of privacy and security concerns.

To offer the most benefit, smart meters have to transmit very accurate and fine-grained power consumption reports. This paper shows that measurements collected by smart meters provide a deep insight into the daily life of each individual customer. There is even research showing that it is possible to discern which movies are currently being watched, based on data collected in a real-life household [3]. In response to those issues, this paper compares several possible solutions for protecting consumer privacy in the age of smart metering.

The recent uproar about compromised programmable logic controllers in industrial automation has also made it painfully obvious, that such devices are often far from perfect and secure. In light of these incidents, the security and reliability of similar devices, like metering systems, has to be questioned as well. Attacks on the smart grid could very well lead to serious damage for both customers and providers. For these reasons, this paper gives an overview of potential attacks common to smart metering systems. Additionally, various countermeasures are proposed in order to combat those threats.

In section 2 background knowledge on smart metering and smart energy grids is given, including information about current legislation. The privacy concerns and possible solutions are examined in section 3. Section 4 then continues with possible attacks on the smart grid and various countermeasures. The conclusions for future efforts in respect to smart metering are subsequently drawn in section 5.

2. SMART METERING

2.1 Smart meters

Smart meters are microprocessor-enhanced, networked metering devices. They are most commonly used for the measurement of electrical energy, but are sometimes also used by water or gas utilities. A typical *smart meter installation* on the customer's premises consists of a *metering device* and an accompanying *home gateway*, as depicted in figure 1.

The metering device is the one to actually measure the energy consumed and then report it to the home gateway. Most metering devices also offer an analog or digital display on which the cumulative consumption may be directly inspected, just as with a conventional electricity meter. The home gateway then forwards the meter readings to the energy provider and optionally also to the customer's building network.

doi: 10.2313/NET-2013-08-1_21

Most smart meters currently on the market combine the home gateway and metering device into a single unit. These devices can then simply be installed in-place instead of a conventional meter with little to no additional wiring.

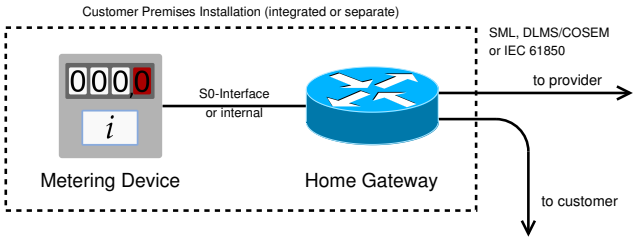

Figure 1: Smart meter installation

In case the metering device and home gateway are separated, communication between them is usually realized through very simple means. A widespread instance of this is the S0-interface (not to be confused with the S0-bus), which simply provides a fixed number of impulses per unit of energy[1]. However, in special cases, more advanced protocols might be used if the metering unit also contains a sophisticated processing unit.

There are several high-level protocols for the communication between the home gateway, data aggregator and provider backend. On the physical layer, communication may occur over a large variety of channels. Those include telephone lines, wireless links or the power line itself. While smart metering protocols in the past were often based directly on the physical or data-link layer, most modern protocols actually support the use of TCP/IP and related technologies. Most protocols for smart metering are standardized by the International Electrotechnical Commission and some additionally by the European Committee for Standardization. The exact kind of data exchanged between the meter and the provider is, sadly, both protocol and device specific.

The most commonly used protocols for smart metering are SML and DLMS/COSEM, both specified in IEC 62056, as well as another protocol simply referred to by its specification name IEC 61850 [2]. SML and DLMS/COSEM are widely used in the European Union, including Germany. All of these protocols already support communication encryption, either natively or via an underlying SSL/TLS implementation.

2.2 Smart energy grids

Smart energy grids or *smart grids* are most of all intended to facilitate the delivery of energy from the growing number of small to middle-sized power plants, like photovoltaic installations or wind parks. To that end, information is collected on the individual energy consumption and the overall generation capacity in the grid. This information is then used to both anticipate and regulate the energy demand, as well as the power generation. An example smart energy grid is shown in figure 2.

[1]The voltage, number and duration of impulses is device-specific and must be obtained by consulting the respective data sheet.

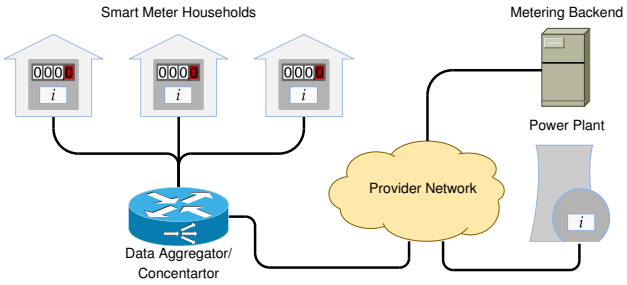

Figure 2: Smart energy grid

In the future, every household is supposed to be equipped with a smart meter, which reports the current power consumption to the smart grid and forwards control commands back to specially-enabled home appliances. These so-called *smart appliances* are then started at times of low demand or high capacity and stopped when there is a power shortage in the grid. This is mostly intended for non-time-critical appliances, such as washing machines or dishwashers.

Some grid architectures additionally employ intermediary *data aggregators* or *concentrators* between the home gateway and the provider, thus forming a hierarchical network. In case the smart meters communicate their readings over a wireless link, the data aggregators are also often used to act as intermediaries between the wireless protocol and the provider network.

2.3 Smart metering regulations in the EU

The European Union regulates the usage of intelligent metering devices in the directives 2006/32/EC and 2009/72/EC. Member states are thereby instructed to take measures so "at least 80 % of consumers shall be equipped with intelligent metering systems by 2020." In Germany, the adoption of smart metering is additionally regulated by §21d EnWG and the MessZV, which mandate the use of smart meters for new installations.

The general requirements for metering devices in the European Union are set forth by the Measurement Instruments Directive or MID from 2004. However, those are mostly abstract requirements for accuracy and tamper-resistance not particularly directed at smart meters. However, there is also a large and growing number of international standards for smart meters and the smart grid in general, including those on communication protocols mentioned in subsection 2.1.

3. PRIVACY

As smart meters are able to provide very accurate power consumption profiles, they pose a serious threat to consumer privacy. The smart meters that are currently in use or available on the market report measurements with an interval of as low as 2 seconds [3]. The identification of different power signatures in those reports may thus even be accomplished with the bare eye. By additionally using sophisticated data mining techniques, this data could be used to very accurately identify the behavioral patterns for individual household members.

3.1 Privacy problems

It has been shown on various accounts [11, 12, 13], that it is possible to identify individual home appliances by their power signatures and the time of day. An example of this is illustrated in figure 3.

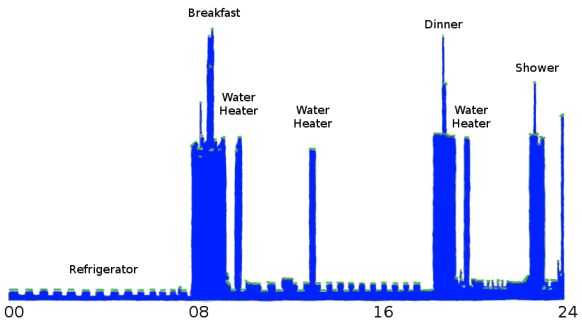

Figure 3: Example smart meter measurement data, redrawn from [11]

In the example at hand, spikes in the morning and evening indicate the making of breakfast and dinner, respectively. The lack of power consumption during the day might also hint that there is no one home during that time. Based on such data, detailed behavioral profiles may be compiled. By collecting usage patterns over an extended period of time, it is also possible to reason based on changes in the power traces. This could answer questions about sick leaves, holidays or how well a person sleeps at night. Such insights could then, for example, be used by insurances, criminals, as well as for marketing or law enforcement. These and other implications are also laid out in more detail in [11] and [12].

If the smart meter transmits its usage data on an interval of a few seconds, it is even possible to identify the television program or movies being watched [3]. This is possible, because the power consumption of a typical backlit flatscreen television changes significantly between bright and dark scenes. It has been shown that by comparing these fluctuations with those predicted based on individual movies, it it possible to identify the content being watched even while other appliances are in use. This opens up a whole new level of possibilities for the invasion of customer privacy.

3.2 Solutions

The obvious approach ...
is to increase the interval between measurement reports to the provider. Depending on the increase, more and more details are kept private and the identification of behavioral patterns is hampered. The customer would retain full access to all measurements by directly connecting to the smart meter, in order to still be able to identify possible ways to save energy.

However, as this also goes against the provider's interest to get as accurate real-time power measurements as possible, quick adoption of this concept is very unlikely. The obtained data could then merely be used for coarse-grained statistics, in addition to general accounting.

A more sophisticated approach described in [1] uses a combination of infrequent attributable reports for accounting and frequent anonymized reports for grid management. This has the potential of both preserving the customer's privacy and the provider's interests.

The pseudo-approach ...
is to pseudonymize the measurement data by a trusted intermediary, either a data aggregator or a trusted third party, before forwarding it to the provider. This would allow the provider to still receive accurate and detailed meter readings, however, they would not be attributable to a single household. For accounting, this approach could be combined with less frequent readings reported directly to the provider.

However, it has been shown [4] that by collecting external consumption-related information on a household, pseudonymized readings may still be linked to individual households. Therefore, this approach offers no real protection against more resourceful attackers. It would also require a central point that both customer and provider trust. If this central point would be compromised or disabled, the confidentiality of measurements could not be guaranteed anymore and the operation of the smart grid could also be seriously impaired.

The statistical approach ...
is to anonymize or aggregate measurement reports either in an intermediary data aggregator or by a trusted third party [1]. The provider would then only receive data not attributable to individual households. If the number of aggregated households is large enough, each customer's consumption would thus be obscured. For accounting, this approach could be combined with less frequent readings reported directly to the provider or with a protocol based on zero-knowledge proofs [14, 11].

The drawback of this approach is, that it again requires a central trusted point. If the trustworthiness of the provider is already in question, then customers are also unlikely to accept a different company to protect their data. Besides, it would take a very large number of aggregated households to actually make it impossible to extract individual usage information based on changes in the total consumption.

The mathematical approach ...
is to add random distortions to the measurement data directly in the smart meters prior to sending them to the provider or intermediate data aggregator. This is done in a way, so that all of these distortions cancel each other out if the individual values are combined. Several possible implementations for smart meters are presented in [9]. The basic outline of the solution is repeated here.

All smart meters in a reasonably-sized group agree on random values p_i, so that

$$\sum_{i=0}^{n} p_i = 0$$

is true, given n as the number of meters in the group. Each smart meter then transmits its measurement data m_i as the distorted value $c_i = m_i + p_i$.

doi: 10.2313/NET-2013-08-1_21

If the provider or data aggregator then combines all values, the formula

$$\sum_{i=0}^{n} c_i = \sum_{i=0}^{n} m_i + p_i = \sum_{i=0}^{n} m_i + \underbrace{\sum_{i=0}^{n} p_i}_{=0} = \sum_{i=0}^{n} m_i$$

yields the correct sum of all individual measurements. A different way of distorting the values, also presented in [9], uses Diffie-Hellman exponents instead of simple summation. The underlying principle, however, stays the same. They also present different ways for the meters to agree on the p_i for the distortion, from selecting some meters to act as moderators to a cryptographic group key-exchange protocol.

The main advantage of this approach is, that it requires no trusted third party or any trust in the provider by the customer. Since all privacy-related operations are performed inside the smart meter or home gateway at the user's premises, no private data may be leaked. The drawback of this approach is, that it is significantly more complex than just sending the plain data and most likely also less fault-tolerant.

The analog approach . . .
is to store the energy from the provider in a buffer or battery at home for later use, as described in [6, 7]. Since the smart meter only measures the charging of the energy buffer, the concrete power usage patterns remain hidden. This would also enable sophisticated smart grid load balancing and protect the customer in case of short power outages.

However, the high cost and sheer complexity of this approach currently makes it the least likely solution to be implemented. On the other hand, if, in the future, customers have access to high capacity batteries in their electric cars anyway, this approach is expected to become more and more realistic.

4. SECURITY

The ongoing introduction of smart meters into every household also raises great concerns about their security and the security of the smart grid as a whole. As shown above, devices in the smart grid handle quite sensitive information, especially for customers. Additionally, as more and more systems operate based on information from the smart grid, manipulations could have very serious consequences for both customers and suppliers. This includes, but is not limited to, cascade failures causing extensive power outages, as well as possibly life-threatening malfunctions in the power grid and connected devices. An overview of attacks on the smart grid and related countermeasures is given in table 1.

Smart meters are supposed to stay in service for long periods of time without supervision. This causes additional problems, because security vulnerabilities present in the meter's firmware could easily be exploited by an attacker even years after they are first discovered. It is therefore imperative to have a secure method for regular fully-automated updates in place, which also cannot be misused by an attacker to inject malicious code.

The following analysis does not specifically cover attacks requiring direct physical access to the smart meter installation. As metering installations are usually specifically sealed and protected, this kind of tampering would pose a high risk of detection for external attackers and malicious customers alike. Nonetheless, even though smart meters do not need to be read out in person anymore, they should be inspected in regular intervals in order to discover manipulations.

Since there is a large number of different standards concerning smart metering, some of which are currently in development, this analysis provides only an abstract view on security in the smart grid.

4.1 Attacks on the smart grid infrastructure

The following is an overview of different kinds of attacks on parts of the smart grid infrastructure. The attacks range from simple eavesdropping to potentially, albeit unlikely, catastrophic failures in the grid infrastructure.

Eavesdropping on metering reports
This attack is aimed at undermining the confidentiality of metering reports by a third party. In case communication takes place over a wireless link or the power line, transmissions could be intercepted with very cheap equipment and little-to-no risk of detection. Possible kinds of attackers range from intrusive neighbors to professional burglars trying to find out when their prospective victims are not at home. In any case, this would mark a serious intrusion into the customer's privacy.

Denial of service
As for every kind of public network, denial-of-service attacks will most certainly also be applicable to the smart grid. The most likely target in this case would be the metering server of the provider, where measurement reports are gathered. Since most modern metering protocols are based on common protocols also used in the Internet, all well-known denial-of-service strategies apply here as well. The most promising attacks are likely going to be SYN flooding and SSL/TLS-based attacks. A more rudimentary approach is to simply cause interference on the physical medium, for example, the wireless link or the power-line.

A subsequent denial-of-service situation could then be used to interfere with provider accounting systems and possibly cut control systems off from accurate load measurements. In the worst case, such an attack could disrupt the smart grid completely, with unforeseeable effects for the power grid as a whole. Additionally, if smart meters have to listen for remote commands, they become vulnerable to these kinds of attacks as well. Since they have only very limited processing capabilities, they would be even more receptive to denial-of-service attacks than the provider's systems.

Forgery of metering reports
The goal of this attack is to compromise the data integrity or authenticity of metering reports sent by the smart meter to the provider. This could, for example, be achieved by performing a man-in-the-middle attack to modify consumption data between the home gateway and the provider. Further information on this attack can also be found in [10].

doi: 10.2313/NET-2013-08-1_21

Attack	Consequence(s)	Countermeasure(s)
Eavesdropping on metering reports	Invasion of privacy	Communications encryption
Denial of service	Suboptimal energy distribution, power outages, grid malfunctions	none
Forgery of metering reports	Energy theft, financial damage to providers or individual customers	Communications encryption
Injection of false remote commands	Cutoff of individual households, large-scale power fluctuations	Communications encryption
Compromisation of smart meter integrity	Manipulate meter readings, remotely control connected appliances, infect the customer network	Verification of system integrity, Virtual machine sandboxing, Intrusion detection systems
Attacks on the provider infrastructure	Manipulate metering data, remotely control smart meters, infect the power grid	Verification of system integrity, Virtual machine sandboxing, Intrusion detection systems

Table 1: Overview of Attacks and Countermeasures for the Smart Energy Grid

The attacker is most likely the customer himself attempting to reduce his power bill by committing energy theft. Another possibility, however, is an external attacker intent on inflicting financial damage on specific customers by increasing their reports or crashing the provider's accounting system altogether.

Injection of false remote commands

A different type of attack is to inject false remote commands addressed to certain or all smart meters in the network. Again, the data integrity and authenticity of messages is affected. One way to accomplish this could be to replay previous remote commands from the provider. Another way could be to again perform a man-in-the-middle attack and manipulate commands as they are sent to the smart meter. Given the extensive remote management possibilities of smart meters, an attacker could use this to cut power to specific households or even cause large-scale power fluctuations on the grid. If, in the future, home appliances may be remote controlled to run at off-peak times, those could quite possibly be affected as well.

Compromisation of smart meter integrity

A very tempting target is the smart meter itself, that is, compromising the integrity of the smart meter directly. By exploiting a weakness in the metering software or the operating system itself, an attacker could gain access to the entire metering device. This would enable him to freely manipulate metering reports, send false information to connected home appliances or go even further and compromise the entire building network.

Attacks on the provider infrastructure

Last but not least, malicious entities could try to use the new possibilities of the smart grid in order to attack the energy provider's infrastructure itself. The attack vector is very similar to an attack on the integrity of the smart meter. In case the metering infrastructure and the control systems for the power grid are not separated, attackers who manage to compromise the metering system may also be able to gain control of the power grid as a whole. This would enable them to cause serious harm to the entire grid, for example, by overloading one or more transformer stations. While such an attack is rather unlikely, when considering the significant damage which could ensue, it is still important to keep this kind of worst-case scenario in mind.

4.2 Countermeasures

In the following several countermeasures are presented for the attacks above. Some of them are already available for use in current smart metering devices, like encryption and trusted platform support, while others still require further research.

Communications encryption

The most obvious countermeasure is certainly the consequent encryption of all communication in the smart grid. Most modern communication protocols for smart metering hence support encryption either natively or through the use of SSL/TLS. However, a problem common to all kinds of autonomous machine-to-machine communication is the secure distribution and storage of key material. Often a Trusted Platform Module (TPM) is used to serve as a secure key storage. In this case, the keys would be pre-programmed into the TPM before the device is installed. Another possibility is to use a pre-programmed smart card, which could be inserted into the device at a later time and also exchanged if required. For smart meters, this could also provide a secure and convenient way for customers to change contracts, simply by replacing their smart card with another one.

Verification of system integrity

Another important countermeasure is the verification of system integrity in smart metering devices, to prevent most physical and some other attacks. The integrity of the operating system and metering software could be verified by the TPM during bootup. This could also be used in conjunction with local or remote attestation, that is, the cryptographic attestation of system integrity by an attached smart card or a remote server, respectively. The approach could also be

augmented with sensors in the meter casing to detect tampering and alert the provider or erase the encryption keys. However, none of these measures are able to prevent anyone from compromising the software while the smart meter is running.

Virtual machine sandboxing

In addition to the measures above, virtual machine sandboxing could be used to further fortify the system and reduce the attack surface to a minimum. This would mean running all applications, especially those requiring network access, in separate and fully-isolated environments with little access to the actual hardware. Thus, if one virtual machine is compromised, the rest of the system stays intact. An additional benefit of this approach is that both customers and providers could install their own VM appliances on the smart meter as needed. Updates to those appliances could also be disseminated and verified in a fully-automated manner, providing swift and effortless software updates to connected meters. Further information on the secure deployment of virtual machine images can be found in [5].

Intrusion detection systems

Intrusion detection systems (IDS) provide a way to detect attacks on the current system by monitoring the system state and/or the network. In the smart grid, IDSes could be used to detect tampering and subsequently exclude affected systems from grid communications, as well as notify the grid operator. This approach and the previous one could also be used in conjunction with virtual machine introspection (VMI), a technique which allows for the inspection of individual virtual machines while they are running. The integrity of each virtual machine could thus be monitored directly by an IDS and it could be stopped immediately if any intrusion is detected. More information on VMI-based IDSes can be found in [8]. This is also an open field of research here at the chair for network architectures and services.

5. CONCLUSION

It has been shown, that there is still a great deal of work to be done to make future smart metering systems more privacy-friendly and secure. The data collected by modern smart meters holds the potential to seriously affect each customer's privacy. The current practice of making fine-grained and attributable power measurements directly available to energy providers seems therefore unsustainable. Most of the proposed solutions to better protect consumer privacy could actually be implemented right away. Further developing those measures could prove to be a great step in order to raise the acceptance of smart meters by end-users. The approach to conceal the individual consumption in the smart meter itself by carefully distorting the measurement data seems to be especially promising.

There are evidently also great concerns for the security of metering installations. Most metering systems already offer a decent level of communications encryption. The protection of the metering systems themselves, however, still leaves room for improvement. Ideally, all of the countermeasures described in this paper should be implemented together, to offer the most security for both end-users and providers.

It should also be noted, that manufacturers of smart metering systems currently offer only little information on the security measures taken in their devices. Smart meters, however, are simply too significant for the power infrastructure to rely on security-by-obscurity. All in all, it can be safely assumed that the development of security and privacy solutions for smart metering systems and similar embedded devices will stay an open field of research.

6. REFERENCES

[1] C. Efthymiou and G. Kalogridis. Smart Grid Privacy via Anonymization of Smart Metering Data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238–243, 2010.

[2] S. Feuerhahn, M. Zillgith, C. Wittwer, and C. Wietfeld. Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 410–415. IEEE, 2011.

[3] U. Greveler, B. Justus, and D. Loehr. Forensic content detection through power consumption. In *ICC*, pages 6759–6763. IEEE, 2012.

[4] M. Jawurek, M. Johns, and K. Rieck. Smart metering de-pseudonymization. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, pages 227–236, New York, NY, USA, 2011. ACM.

[5] M. E. Jobst. Security and Privacy for Virtual Machine Images using Smart Cards. Bachelor's thesis, 2012.

[6] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda. Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 232–237, 2010.

[7] G. Kalogridis, Z. Fan, and S. Basutkar. Affordable Privacy for Home Smart Meters. In *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*, pages 77–84, 2011.

[8] T. Kittel. Design and Implementation of a Virtual Machine Introspection based Intrusion Detection System. Diploma thesis, Technische Universität München, Oct. 2010.

[9] K. Kursawe, G. Danezis, and M. Kohlweiss. Privacy-friendly aggregation for the smart-grid. In *Proceedings of the 11th international conference on Privacy enhancing technologies*, PETS'11, pages 175–191, Berlin, Heidelberg, 2011. Springer-Verlag.

[10] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. In *Proceedings of the 4th international conference on Critical information infrastructures security*, CRITIS'09, pages 176–187, Berlin, Heidelberg, 2010. Springer-Verlag.

[11] 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, pages 61–66, New York, NY, USA, 2010. ACM.

[12] E. Quinn. Privacy and the new energy infrastructure. *Available at SSRN 1370731*, 2009.

[13] E. Quinn. Smart metering and privacy: Existing laws and competing policies. *Available at SSRN 1462285*, 2009.

[14] 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, pages 49–60, New York, NY, USA, 2011. ACM.