Analysis of the Security Anomalies in the Smart Metering Infrastructure and Its Impact on Energy Profiling and Measurement

Pallab Ganguly[1], Sumit Poddar[1], Sourav Dutta[2] and Mita Nasipuri[3]
[1]*CESC Limited, Kolkata, India*
[2]*IBM, Kolkata, India*
[3] *Dept. of CSE, Jadavpur University, Kolkata, India*

Keywords: Encryption, Smart Grid, Smart Meter, Security, AMR, AMI, Consumer, M2M, Energy Meters.

Abstract: Security of the smart metering infrastructure, which is a part of the smart grid initiative, intended at transitioning the legacy power grid system into a robust, reliable, adaptable and intelligent energy utility, is an imminent problem that needs to be addressed quickly. Moreover, the increasingly intensifying integration of smart metering infrastructure with other ecosystem applications and the underlying communication technology is forcing both the consumer and the utility provider to meticulously look into the security and privacy issues of the smart grid. To achieve this, improvements on the existing architecture that uses smart meters interacting with smart grid is needed. This architecture would help in consolidation and aggregation of the energy usage and generation as intelligent communicators instead of focusing them as isolated passive units in the energy grid. The study presented in the paper analyses the various existing smart metering infrastructure, threats and vulnerabilities that has the potential to disrupt the operation and deployment of automation systems in smart grids. Furthermore, an elaborate study and subsequent analysis have been made on a live consumer meter setup in a non-invasive manner, which shows the various security loopholes and deficiencies of a large deployment of unattended smart meters. The study identifies the potential gaps and suggests possible measures for a cost effective and robust solution to cater for present as well as future needs.

1 INTRODUCTION

The interaction between a smart house and a smart grid based on *Information and Communications Technologies* (ICT) can fully exploit the capabilities of the smart energy network (Palensky, 2011). A smart meter is usually an electronic device that records consumption of electric energy at certain intervals (frequency of which can be programmed) and communicates that information on a regular basis with the utility provider for monitoring and billing. Smart meters enable two-way communication between the meter and the central system.

In today's scenario, the security of *smart metering infrastructures* is a very critical issue and plays an important role. In this study, the analysis is made on a live consumer meter setup, where the meter is serially connected with a communication modem and connected to the mobile communication network which, in turn is connected to the public Internet. The meter data through Internet reaches the corporate data communication network and is stored in the aggregation server. The interim data packets have been captured and analyzed from the live consumer meter setup in a non-invasive manner from the production environment and the findings were noted. The data is sent in a special format which is understood only by the aggregation server and processed in a proprietary manner. But there exists a high chance of manipulating this extracted data. The consumer billing is directly dependent on the meter reading parameters and if the meter data is tampered, the consumers and most importantly the utility service provider will be highly impacted. The number of services like meter reading, online pricing, information security or load control, which is the part of the energy ecosystem could get jeopardized. Thus, robust security mechanisms have to be incorporated in the design of the meter infrastructure to prevent any potential fraud. Since the power utility is one of the most mission critical infrastructure services today, the comprehensive

Ganguly, P., Poddar, S., Dutta, S. and Nasipuri, M.
Analysis of the Security Anomalies in the Smart Metering Infrastructure and Its Impact on Energy Profiling and Measurement.
In *Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2016)*, pages 302-308
ISBN: 978-989-758-184-7

security and privacy mechanisms are needed to ensure robust, reliable and smooth operation of the smart grid. A thorough analysis of technical vulnerabilities and identification of threats is an important step toward securing smart metering infrastructure.

The three most important security objectives that must be incorporated in the smart grid systems, are:

1) Ensure data integrity is maintained throughout the end to end communication channel, 2) Proper authentication and authorization needs to be adopted and 3) Confidentiality of user's data. The *smart metering infrastructure* is visualized as an unsecured system to permit authority from various gadgets and users. The potential security problems related to smart metering systems have been surveyed and an actual threat scenario has been implemented confirming the vulnerability of the current smart metering infrastructure.

The main sections in this paper are as follows:

- ✓ Study of the previous works in the field of security and privacy issues in smart energy metering infrastructure, over a considerable period focusing on recent implementations from meter manufacturers, standards as well as publications.
- ✓ Under the hood of Smart Energy Meters, discusses the internals as well as gives insight into the live consumer setup for interception and manipulation of energy metering data.
- ✓ Study of Smart Meters in a live big power utility's grid.
- ✓ Detection and Analysis of the energy metering data for veracity, discusses the various areas that need to be addressed for plugging the gaps.

2 EARLIER WORKS

There have been a number of works and commercial implementations based on certain standards throughout the world. An exhaustive study has been done both on theoretical work as well as the practical implementation available in the realms of energy meter hardware, communication standards/ protocols and the Information Technology system. The financial impact on the utility provider in the smart metering infrastructure is also discussed.

The major problems in *Advanced Metering Infrastructure* (AMI), especially embedded system are insecure data buses and serial connections, data capture and injection, radios and microcontroller units causing problems like replacing or stealing memory keys, firmware level vulnerabilities and resetting of *Joint Test Action Group* (JTAG) fuses. The AMI utility premises vulnerabilities like buffer overflows, Structured Query Language (SQL) injection, credential hijacking, needs firewalling in between the system components and internet connectivity to the head end. Only required ports should be open in the firewall and the other ports should be blocked by default. Researchers (Carpenter, 2008); (Lawson, 2010) have gained access inside the smart modules of electrical meters and identified the microcontroller. They were able to identify the JTAG pin outs and ultimately dumped the program inside the microcontroller through JTAG cable to a computer (Lawson, 2010). However, no further analysis was reported of the dump. The possibilities of breaking a meter were discussed in many forums and the software flaws and hardware weaknesses and also the disadvantages of the Microcontroller unit is a serious issue as cited by (Carpenter, 2008), (Lawson, 2010) and (Davis, 2009). It is important to point out that the software dump extracted from the microcontroller memory has severe implications across the entire AMI spectrum.

There are different kinds of communication protocols and standards used for the smart metering infrastructure. A survey on the communication protocols and standards used for *Automated Meter Reading* (AMR) application has been mentioned by Khalifa et al., (2011) and Feuerhahn et al., (2011). The paper discusses about the benefits of the 3G communication system, Device Language Message specification/ Companion Specification for Energy Metering standard and the *Internet Protocol* (IP) based *Session Initiation Protocol* (SIP) for signaling at the application level. While analyzing the future of AMR, the researchers agreed to the concern that the provision of data integrity in metering was given more priority than the data privacy cited by Ye Yan et al., (2013). In the paper by Ye Yan et al., (2012), the authors discussed that a built-in security mechanism is necessary in comprehensive smart grid communication architecture. Researchers have elaborated their points by giving the background, requirements, challenges and current solution. In explaining the background, they have given thrust to the Supervisory Controlled and Data Acquisition, Communication network and deployment. The authors discussed the motivations, requirement and challenges in the smart grid communication infrastructures in Ye Yan et al., (2013). The paper suggested how reliability, operational efficiency and customer satisfaction can be addressed with an AMI deployment. Authors have proposed a 2-phase method to provide security of data using dedicated authentication server, which inhibits malicious and unauthorized nodes to gain access to advanced meter infrastructure communication network cited by Mehra *et al*.(2013). The result found through a NS2 simulator confirms that security threats can be reduced by adding key management system over the existing infrastructure. The problem in this method is the huge overhead for manageability of the key for such a large deployment of smart metering system.

The recommendation by Florian Skopik et al., (2013) was to make the smart meters and concentrator nodes physically robust and tamper resilient. Authentication mechanism, digital certificates and signatures, encryption of communication data should be adopted. The author (Farid Molazem) discusses the Security and privacy of smart meters in detail and a security mechanism has been developed for smart metering system. It has been further classified into two categories viz. intrusion detection method and remote attestation method. The strength and weaknesses of both the methods have been mentioned. The paper concluded with the fact that the monitoring and the protection system for the software running inside the meters has to be explored and the existing security techniques applied to the smart meters rely on the running cryptographic algorithm on the meters but the old meters might not have the processing power or adequate memory to perform intense cryptographic operations.

Similarly, the authors (Finster and Baumgart, 2015) have surveyed the privacy issue of the smart metering infrastructure and have classified privacy problem from a metering perspective. They have approached the problem from two angles: metering for billing and metering for operations. For each of these problems they have identified generic approaches. They have compared the various approaches for the metering for billing issue by smart meter complexity, infrastructure complexity and attack complexity for trusted third parties, trusted computing and cryptographic proofs. Similarly they have compared the approaches to metering for operation by the same parameters but the approaches were for pseudonymization without aggregation, trusted third party with aggregation, aggregation without trusted third parties and submission of imprecise data. They have surveyed a number of papers and concluded that meter deployment and simultaneously maintaining privacy is a huge challenge and an avenue for further research.

Future scope of research exist in the field of system complexity, communication path, clash in between privacy preservation and information usage accomplishing advanced encryption techniques and interoperability between cryptographic system in smart grid elements like memory usage, Central Processing Unit utilization etc. (Bhatia and Bodade, 2014), Yonghe Guo et al., (2015). They also have discussed the cyber-attacks pertaining to the AMI viz. connection based attacks for communication media or protocol based attacks and security flaws in devices and recruitment of attack agent in metering device like implanting malicious program inside the meter or spread malware in the system. The subject concluded with the facts that besides deploying detection system, to maintain security levels, software bugs should be removed; updating firmware in regular intervals, updating protocol and Software patching is to be done. The author defined the smart grid and smart meter and discussed the related work on policy level and technology level Kalogridis et al., (2010), Khurana et al., (2010). The paper by Kalogridis et al., (2010) also emphasized on the load forecasting possibility in smart metering system. The current practices of cryptographic key management which is useful for small deployments of smart meters but for large deployments the management of the cryptographic keys would require more staffs which is an issue for a power utility. Aloul et al., (2012) concluded with some proposed solutions like Identity verification through strong authentication mechanism, organization should have implicit deny policy, malware protection in embedded system. The authors Liu et al., (2012) projected an overview of smart grid and relevant technologies and given a future research direction in the cyber security and privacy issues of smart grid. An archetypal attack tree approach has been developed to guide penetration testing across multivendor implementation by Stephen et al., (2010). Academic and Industrial penetration testing efforts have found flaws in meter hardware, firmware, network protocols and the Internet. Ultimately it could not throw much light on the protection mechanism present at the collector links to the backhaul network. (Jawurek, 2011) proposed future research work was necessary for the privacy and protection of the above data types. The data communication security of the advanced meter infrastructure in smart grid is a serious problem. The financial impact in smart metering infrastructure is a burning issue where the financial loss to premise owners, utility provider and the nation as a whole is of immense importance. If the meter reading of the consumer is altered, the premise owner has to pay extra bills for no reason. The attacker can also switch off the power supply at the consumer premises and take malicious remote control over the appliance present in the consumer premises. There is a chance of huge financial impact to a utility provider if the attacker attacks the utility server and manipulates the meter reading to lower usage than the actual consumption by the customer. If the attacker takes the control of the utility server, it can send erroneous control commands to the meter on behalf of the utility server. The customer will take advantage and will not pay the bills. In case of even bigger threat scenario, there could be major power blackouts which could impact the transport infrastructure, banking system, healthcare systems and various industry verticals all across the targeted country cited by Yussof et al., (2014). After the comprehensive literature study, the major findings indicate lack of security and privacy in the various layers of the present smart metering infrastructure. This paper addresses the security issues mentioned above and attempts to focus on the AMR and the communication mechanism as an immediate quick fix to the larger problem.

3 UNDER THE HOOD OF SMART ENERGY METERS

A smart meter is an electronic device that records consumption of utility services [such as electricity] at fixed intervals and communicates that information as per schedule with the aggregation server at the utility premises for monitoring and billing. Smart meters enable two-way communication between the meter and the central aggregation system for complete monitoring as well as control of the services. As shown in Fig 1, basically all smart meters usually contain a microcontroller with flash memory, external data memory, a liquid crystal display driver and a communication modem with suitable connectivity. The programmable memory can be a onetime erasable programmable read-only memory, a serial Electrically Erasable Programmable Read-Only Memory or a parallel Electrically Erasable Programmable Read-Only Memory. Some smart meters have external communication modems connected with a RS232 serial interface. Different meter vendors use different setup.

The important global standards used in Smart Metering are IEC 62051, IEC 62056, IEC 62351, IEEE 1377, RFC 3394, ANSI C12.19, ANSI C12.22 etc. The standard IEC 62051 is used for Data exchange for Meter Reading, Tariff and Control. IEC 62056 is used for Electricity meter data exchange. The power systems management and associated information exchange with Data and communication security uses the IEC 62351 standard. IEEE 1377 is used for the metering communication protocol in the application layer & RFC 3394 is for advanced encryption standard key wrap algorithm. ANSI C12.19 is needed for utility industry end device data table & ANSI C12.22 is needed for protocol specification to interface with data communication networks. There are no specific standards on communication and cybersecurity for Wide Area Networks, Neighborhood Area Networks and Home Area Networks. If we look into the global smart metering journey, the first generation had one way Radio Frequency or low bandwidth Power Line Communication technology, business benefits focused on optimized meter reading costs and maximum deployment of smart meters took place in the United States. The benefits of smart metering includes improving billing efficiency, providing meaningful consumption information, reducing operational cost and reducing overall and peak demand. The trends in smart metering increased the analysis of data and frequency of reading, the numbers and types of devices to manage multivendor access and high volume processing on the immediate horizon. Gradually legacy utility application has adapted to an AMI environment. It impacted the meter information on consumer and the consumer information system needed to be integrated with the meter data management system. The device communication strategy needed to allow multiple protocols for meaningful communication and integration with multivendor gadgets. The *Machine to Machine* (M2M) devices include the smart meter, communication interface, communication devices and the central aggregation server. Different approach models like M2M device models and Semantic models were suggested by global system integrators. Device model is a digital description of physical devices and their relationships. The model should be able to integrate cross domain functionality water, energy, transport, public etc. Each domain has their own standards, language, models etc. The meaning of each of the domain can be explained with the Semantic model, where the devices with their standards and relations are captured. The approach makes use of storing the devices in specified formats. The M2M devices can either communicates directly using low level protocols or standards or via M2M gateway or central Hub. To model a M2M gateway as a generic model, the sensors, actuators, components could also be defined with the device model.

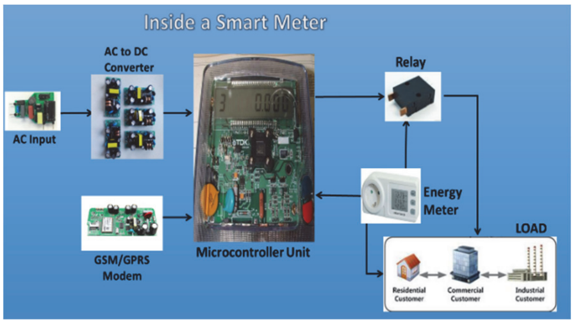

Figure 1: Schematic of a Smart Meter.

Figure 2: Actual Equipment used for the test setup.

4 STUDY OF SMART METERS IN A LIVE BIG POWER UTILITY'S GRID

We have built an experimental setup with trial meters inside a big power utility in India, distributing electricity to 2.9 mil consumers. The meters communicate with the application ecosystem of the utility provider using extant public communication mechanisms. The smart meters had a *General Packet Radio Service* (GPRS) supported modem built-in which communicates with the *Base Transceiver Station* (BTS) of the mobile service provider. The mobile service provider routes the data to the Internet through which the data traverses and enters the Utility provider's router. It is further channelized through the internet link load balancer and then filtered through a packet filtering Firewall which supports *role based access-control* (RBA) stateful fire-walling. After passing through the firewall it reaches the core switch which again performs role based access control and according to a particular access control statement sends the data to the meter data acquisition system test server. Here the data is processed and the requisite files are sent to the test instance of the billing server for trial customer bill statement. We have captured the data through a packet capturing tool from the public Internet and analyzed, re-engineered by manipulating the meter data with our customized algorithm and channelized into the grid to reach the designated test server, without tampering any of the entries in the firewall or the core switch. After processing the data through the back-end application, we found that the re-engineered data was accepted in the test system and the manipulated data were reflected in the test billing system. The major challenges in this activity were to find the encryption and decryption algorithms and the data model used in the system-on-chip of the smart meters and the head end system. We could identify the various stages from where the data could be manipulated, injected and/or accessed and have come with several solutions to plug those. It is currently under research as this has come as a surprise even to the provider. The actual experimental setup is given in (Fig.3).

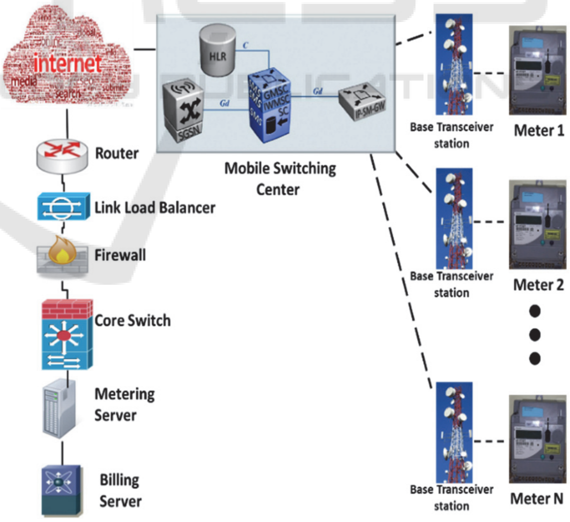

Figure 3: Actual Experimental Setup.

5 DETECTION AND ANALYSIS OF THE ENERGY METERING DATA FOR VERACITY

In this paper we have studied meters from multiple vendors and have carried out the experiment on a particular brand. But the underlying architecture remains the same for all the vendors. The meter data is usually passed through public internet service providers for connectivity with the Utility Service Provider's aggregation systems. There is always a possibility of the data getting manipulated under the present setup. The meter data is usually encrypted using very rudimentary mechanism countenancing the possibility of manipulation of the data generated. The veracity of data generated at the meter thus cannot be guaranteed with the present implementation. The study results of four meter manufacturing vendors are provided in (Fig. 4). We have considered the typical three high-level security objectives for the smart grid: Availability, Integrity and Confidentiality per the NIST guidelines (NISTIR 7628, 2010). The widely used representation for availability is the ratio of the value of the uptime of a system to the total of the values of the up and down times (planned as well as unplanned).

A=Uptime / Uptime + Downtime (planned) + Outage

For the values of integrity and confidentiality, we have taken few parameters to keep it simple at this level e.g. for integrity – whether it is possible to modify the meter in an unauthorized manner, destruction of the meter data etc. and, for confidentiality – whether the default setup is used [known access to all], use of any standard encryption mechanism or plain text data in complex format. As the result indicates, the availability part is satisfied by all the vendors. The integrity part has been handled in a primitive manner and needs more focus. The confidentiality issue has to be given more attention keeping in view of the increasing use of open public communication channels instead of point-to-point tremendously expensive private networks.

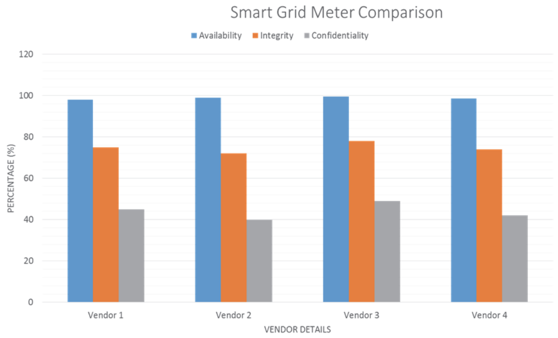

Figure 4: Common-of-the-Shelf (COTS) Smart Grid Meter Comparison.

6 CONCLUSIONS

Advanced metering infrastructure is being implemented across the globe, and detailed information about millions of consumers' electricity use will be streaming into energy utilities for various reports and other operational analyses. It is of paramount importance that the analysis of the security anomalies in the smart metering infrastructure and its impact on energy profiling and measurement to be done with respect to the current and future trends. This paper gives an insight into the current smart metering techniques with its merits and demerits. The work studied has been categorized into end equipment [meter hardware]; communication mechanism and the back end IT applications. With the huge deployment of smart meters, security is a grave concern from a financial perspective as well. The end to end traversal of data from the smart meter at the customer premises to the aggregation unit at the service provider's end is usually via the open public communication channels basically because of ease of deployment and most importantly, due to financial constraints. Albeit difficult to understand, it is possible to manipulate the data which has a huge financial as well as operational implication. In this paper we have also studied and analyzed a live consumer meter setup in a non-invasive manner [of a tier-1 power service provider] and found the various loopholes and deficiencies of a large deployment of smart meters. It was also found that the current metering standards and protocols cited by Khalifa et al., (2011), Feuerhahn et al., (2011), and Mehra et al., (2013) are inadequate to address these security challenges. For the successful smart grid implementation, the *Information Technology* and the *Operational Technology* (IT/OT) convergence needs to be established so that the Master control center of a power utility can be integrated with the smart metering data management system through a common information model. Without the mitigation of the anomalies in the smart metering infrastructure, the IT/OT convergence will not be possible and potential area for research. The execution of the ICT security measures is expected to have a high impact, throughout the full electricity value chain, on energy efficiency, sustainability and grid management efficiency. Further work is being done to address the various gaps and propose a cost effective and robust solution to cater for present as well as future needs.

REFERENCES

Peter Palensky “Demand Side Management: Demand Response, Intelligent Energy Systems, and Smart Loads” Delft University of Technology, IEEE Transactions on Industrial Informatics, September, 2011.

Carpenter M. Hacking AMI. (2008). [Online]. Available: http://inguardians.com/pubs/090202-SANS SCADAHackingAMI.pdf.

Lawson N. Reverse-engineering a smart meter. (2010). [Online].Available: http://rdist.root.org/2010/02/15/reverse-engineering-a smart-meter.

Mike Davis- Senior Security Consultant at Black Hat USA 2009, “Smart Grid Device Security Adventures in a new medium”.

Khalifa, T.; Naik, K.; Nayak, A, "A Survey of Communication Protocols for Automatic Meter Reading Applications,” Communications Volume: 13, Issue: 2 , 2011.

Feuerhahn, S.; Zillgith, M.; Wittwer, C.; Wietfeld, C, "Comparison of the Communication Protocols DLMS/COSEM, SML and IEC 61850 for Smart Metering Applications," Smart Grid Communications (SmartGridComm), IEEE International Conference, 2011.

Ye Yan, Hu R. Q, Das S. K, Sharif H,” An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid. ”Network, IEEE Volume: 27, Issue: 4, Publication Year: 2013, Page(s): 64 – 71.

Ye Yan, Yi Qian, Hamid Sharif, and David Tipper, “A Survey on Cyber Security for Smart Grid Communications,” IEEE Communications Surveys and Tutorials, Vol.14, Issue 4, pp.998-1010, 4th Quarter 2012.

Ye Yan, Yi Qian, Hamid Sharif, and David Tipper, “A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges,” IEEE Communications Surveys and Tutorials, Vol.15, Issue 1, pp.5-20, 1st Quarter 2013.

Mehra, T, Dehalwar, V, Kolhe, M, “Data Communication Security of Advanced Metering Infrastructure in Smart Grid,” 2013 5th IEEE International Conference on Computational Intelligence and Communication Networks.

Florian Skopik, Zhengdong Ma, Thomas Bleier, Helmut Gruneis, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructure," International Journal of Smart Grid and Clean Energy, August 13.

Farid Molazem, “Security and Privacy of Smart Meters: A Survey”, University of British Columbia.

Rajiv. K. Bhatia, Varsha Bodade, "Smart Grid Security and Privacy: Challenges, literature Survey and Issues," International Journal of Advanced Research in Computer Science and Software Engineering, volume 4, Issue 1, January 2014.

Yonghe Guo, Chee-Wooi Ten, Shiyan Hu, Wayne Weaver, “Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure," IEEE PES Innovative Smart Grid Technologies, Washington, DC; December 2015.

Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., and Cepeda, R. Privacy for smart meters: Towards undetectable appliance load signatures. 2010 First IEEE International Conference on Smart Grid Communications (2010), 232–237.

Khurana H, Hadley M, Lu N, and Frincke D,” Smart-Grid Security Issues.”, IEEE Security & Privacy, 2010; 8(1)81–85.

F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, " Smart Grid Security: Threats, Vulnerabilities and Solutions," International Journal of Smart Grid and Clean Energy (IJSGCE), 1-6, September 2012.

J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,’ IEEE Communication Survey and Tutorials, pp. 981-997, Vol. 14, No. 4, 2012.

Stephen E. McLaughlin, Dmitry Podkuiko, Sergei Miadzvezhanka, Adam Delozier, Patrick Drew McDaniel, “Multi-vendor penetration testing in the advanced metering infrastructure.”ACSAC 2010: 107-116.

Marek Jawurek, Felix C. Freiling, “Privacy Threat Analysis of Smart Metering,” informatik 2011.

Salman Yussof, Mohd. Ezanee Rusli, Yunus Yusoff, Roslan Ismail, Azimah Abdul Ghapar, “Financial Impacts of Smart Meter Security and Privacy Breach,” 2014 IEEE International Conference on Information Technology and Multimedia (ICIMU), November 18 – 20, 2014, Putrajaya, Malaysia.

Elias Leake “Privacy and the New Energy Infrastructure”, Fall 2008, Center for Energy and Environmental Security, CEES Working Paper No.09-001.

S Finster and I Baumgart, “Privacy-aware smart metering: A survey", IEEE Communication Surveys and Tutorials, 2015.

The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 (2010) 1–597.