Student Research Abstract: Trustworthy Remote Entities in the Smart Grid

Andrew J. Paverd
Department of Computer Science,
University of Oxford
Wolfson Building, Parks Road
Oxford, OX1 3QD, United Kingdom
+44 (0)1865 610716
andrew.paverd@cs.ox.ac.uk

ABSTRACT
It has been demonstrated that the frequent energy measurements from smart meters could pose a risk to individual privacy. Although various solutions have been proposed, this remains an open research challenge. This proposed research endeavour aims to enhance user privacy by introducing a novel element into the smart grid architecture. The *Trustworthy Remote Entity* (TRE) is a computational and communication system situated as an intermediary between a group of smart meters and the external smart grid entities. The TRE enhances user privacy by providing a degree of indirection in this bidirectional communication architecture. The proposed research methodology involves first modelling the behaviour of the TRE and then architecting this system using Trusted Computing technologies. Given the current state of smart grid development, it is anticipated that this research will have a significant impact on the smart grid.

Categories and Subject Descriptors
C.0 [**Computer Systems Organization**]: General – s*ystem architectures, modelling of computer architecture*

General Terms
Design, Measurement, Security

Keywords
Privacy, Smart Grid, Trusted Computing

1. INTRODUCTION
The concept of the *smart grid* broadly refers to the use of modern computational and communication systems to optimize the operation of the public energy infrastructure. The smart grid will undoubtedly provide various benefits, but it is also acknowledged that certain smart grid technologies introduce potential cyber security and privacy concerns. In particular, there are concerns about the privacy implications of smart meters for residential customers. Frequent energy measurements from smart meters are required to facilitate new functionality such as demand forecasting, network optimization and time of use (TOU) energy pricing. However, these measurements could reveal a relatively high level of detail about individuals. Research in the field of Non-Intrusive Load Monitoring (NILM) [3] and energy disaggregation [4] has demonstrated that it is possible to identify individual appliances and appliance settings using only frequent measurements of the home's total energy usage. If misused, this could constitute a breach of privacy. Various solutions have been proposed to protect user privacy in the smart grid including anonymization [2], aggregation over time [6], or aggregation amongst groups of homes [1]. Although the proposals address different aspects of this problem, the protection of user privacy in the smart grid is still an open research challenge.

2. PROPOSED APPROACH
To enhance user privacy in the smart grid, it is proposed that a novel element should be added to the smart grid communication infrastructure. The proposed element is called a *Trustworthy Remote Entity* (TRE). The TRE is a computational and communication system situated as an intermediary in the communication path between the smart meters and the other smart grid entities. The TRE is a separate system that is not under the direct control of any of the entities in the smart grid. The TRE will serve to enhance user privacy by providing a degree of indirection in the communication between homes and the external smart grid entities. For example, frequent energy measurements from homes could be aggregated by the TRE before being output to the Distribution Network Operator. It is proposed that the TRE could also be used to address the privacy challenges arising from two-way communication between the smart meter and the external smart grid entities. In order to achieve its objective, the TRE must be simultaneously trusted by the various relying parties. Assuming that all parties agree on how the TRE should function, they must all trust that it is currently functioning in this way. Given the value of the assets in the smart grid, the relying parties must have a suitable basis for the trust they place in the TRE. Although this could be achieved in various ways, the focus of this research is on using technological means to prove that the TRE is trustworthy. All parties should be able to observe and verify the correct operation of the TRE in great detail but none should be able to interfere with this system. The overall objective of this research is to investigate the use of this novel architectural element and to determine the extent to which the TRE can protect user privacy without significantly reducing the functionality of the smart grid. The primary hypothesis is that the Trustworthy Remote Entity can be used to enhance the privacy of home users whilst maintaining the primary functionality of the smart grid.

3. RESEARCH METHODOLOGY
Two main categories of research activities are proposed. Each has its own set of research objectives but also contributes to the outcomes of the other category.

SAC SRC program is sponsored by Microsoft Research.

3.1 Modelling of the TRE

The first category of research activities involves modelling the major flows of information within the smart grid as well as the behaviour of the TRE. In general, when a trusted-third-party (TTP) is used in a system, various assumptions are made regarding what the behaviour of the TTP. Since the proposed TRE will essentially fulfill the role of an enhanced TTP, it is necessary to formalize all assumptions about its behaviour. The information used to develop and subsequently evaluate this model will be obtained from various existing sources such as the NIST Privacy Impact Assessment (PIA) [5]. Initially the model will be developed using Unified Modelling Language (UML) constructs such as UML Communication Diagrams. The primary algorithms and functionality of the model will then be implemented in a high level software language in order to facilitate the evaluation. This model will be evaluated using publicly available smart meter measurement datasets such as REDD [4]. The output will be an abstract model which defines the major information flows in the smart grid as well as the characteristics, behaviour and functional requirements of the TRE. This first category aims to answer the question: *How does a TRE behave in the smart grid context?*

3.2 Realization of the TRE

The second category of research activities is an investigation into how a TRE can be realized in the smart grid context. The outcomes of the previous category will contribute a functional model of the TRE based on idealized technological capabilities. The primary objective in this second category is to determine how this model can be realized as a system. This will include an investigation into the potential system architecture of a TRE and an analysis to determine the feasibility of this architecture given current technology. It is anticipated that the TRE will make extensive use of existing Trusted Computing (TC) techniques such as remote attestation. However, there are still various challenges to address when using these techniques. Furthermore, TC approaches and technologies have not necessarily been designed for use in this context and it may be the case that additional TC capabilities are required to realize the TRE in the smart grid. The output of this category will be a system architecture or architectural framework for the TRE in the context of the smart grid based on current and/or proposed future technologies. This second category aims to answer the question: *How can a TRE be realized in the smart grid context?*

4. OUTCOMES AND IMPACT

It is anticipated that this research endeavour will lead to three major outcomes. Firstly, this research will contribute towards enhancing the current understanding of privacy challenges in the smart grid. By modelling the various information flows, it will be possible to draw more detailed conclusions about which information flows in particular could constitute a threat to user privacy. Furthermore, the processes and techniques used to complete this modelling will themselves be evaluated as a further scientific contribution. Secondly, this research will provide a thorough investigation of the concept of the TRE. This will include both an investigation into the use cases of this proposed element as well as the aspects related to the realization of this concept as a working system. The process and criteria used to evaluate the TRE will also be useful contributions from this work. Thirdly, this research will demonstrate the feasibility of this approach for protecting user privacy in the smart grid. This could form the basis for further research and development and potentially lead to this approach influencing a future smart grid deployment. Given the current state of smart grid technologies and infrastructure deployments, this research has the potential to have a significant impact at this time. This impact would range from raising awareness of privacy concerns to influencing the design of smart grid architectures. The ultimate objective is to provide a solution to the current privacy challenges in order to facilitate the widespread adoption of the smart grid.

5. CONCLUSION

This research endeavour proposes the inclusion of a new architectural element in the smart grid communication infrastructure. The Trustworthy Remote Entity (TRE) is an intermediary node in the communication path between smart meters and external smart grid entities. The TRE is a computational and communication system which is not controlled by any existing entities in the smart grid but is simultaneously trusted by all of them. The primary research hypothesis is that the TRE concept can be used to enhance user privacy whilst maintaining the functionality of the smart grid. Two main categories of research activities are proposed: The first involves modelling the smart grid information flows and the behaviour of the TRE. The second aims to develop the system architecture for the TRE using Trusted Computing technologies. This research endeavour will have a significant impact firstly in terms of enhancing user privacy in the smart grid and more generally in the field of trustworthy systems architecture.

6. ACKNOWLEDGMENTS

This research has been carried out as part of the *Future Home Networks and Services* project at the University of Oxford, funded by British Telecommunications. The author has also received funding through a Chevening Scholarship from the Foreign and Commonwealth Office of the United Kingdom.

7. REFERENCES

[1] P. Deng and L. Yang. A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure. In Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, pages 1–5, 2012.

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

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

[4] J. Z. Kolter and M. J. Johnson. REDD: A Public Data Set for Energy Disaggregation Research. In SustKDD11 - Workshop on Data Mining Applications in Sustainability, 2011.

[5] NIST Smart Grid Interoperability Panel – Cyber Security Working Group. NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. Technical Report August, 2010.

[6] 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, page 49, New York, New York, USA, Oct. 2011. ACM Press.