Microsoft

RESPONSE OF MICROSOFT TO THE
SMART METERING IMPLEMENTATION PROGRAMME
CALL FOR EVIDENCE ON DATA ACCESS AND PRIVACY
13 October 2011

EXECUTIVE SUMMARY

Microsoft Research has developed privacy technologies that allow computations on fine-grained readings, including billing using time-of-use tariffs, with no need for consumers to disclose electricity readings. Additionally, Microsoft Research has developed technologies to enable privacy friendly aggregation of readings from multiple meters without disclosing raw meter readings. These privacy technologies rely on well understood cryptographic techniques and have been the subject of academic peer-review, independent validation, implementation and evaluation on current smart-meters.

PRIVACY ENHANCING TECHNOLOGUES FOR SMART METERING

Question 18: What current and future technical options exist for energy consumption data minimization / privacy enhancing technologies? How might aggregated or anonymised data be provided in practice? Would this imply additional services to be provided by DCC?

- Information computed on the basis of fine-grained smart-meter readings has multiple uses within the energy industry, including billing, providing energy advice, settlement, forecasting, demand response, and fraud detection. Microsoft Research has developed technologies that allow for these computations to be executed without the need for customers to disclose raw meter readings. In brief, smart-meters transmit encrypted certified meter readings, that are processed by any customer device (smart phone, web browser, home gateway, personal computer) to compute the information required, and further provide them to authorised parties. These privacy-friendly computations can include time-of-use bills, settlement values, fraud detection flags, or usage profiles. Cryptographic mechanisms protect the privacy of the data and the correctness of the computations even when performed on customer devices.

- Energy industry processes, such as settlement, monitoring, financial forecasting, transmission network development or demand response, require real-time aggregates of readings across populations of meters. Microsoft Research has developed privacy technologies that allow the direct aggregation of encrypted meter readings. The sum of readings, as well as their mean and variance, can be computed in real-time, without revealing individual meter readings.

- The Microsoft Research privacy technologies have been the subject of academic peer review, and accepted for presentation at leading academic venues specialising in privacy technologies. Their full references are respectively:

[RD11] Alfredo Rial and George Danezis. Privacy-Preserving Smart Metering. Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society, WPES 2011, Chicago, USA, October 17, 2008.

[KDK11] Klaus Kursawe, George Danezis, Markulf Kohlweiss: Privacy-Friendly Aggregation for the Smart-Grid. Privacy Enhancing Technologies - 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27-29, 2011. ISBN 978-3-642-22262-7: pages 175-191

Subjecting security and privacy technologies to peer-review and publication ensures that they receive the appropriate independent scrutiny as to their claims of practicality and security. These works have already come under scrutiny as witnessed by further academic publications referencing them.

- The Microsoft Research privacy technologies have been implemented on current generation smart electricity meters in collaboration with a major meter manufacturer. The results confirm that their computation overhead is small and comfortably within the realm of current meters. Their communication overhead is minimal. Further details on the implementations are available in [RD11] and [KDK11] referenced above.

- Further work studies the feasibility of implementing the privacy technologies on very cheap, low-power micro controllers. These are found in many currently fielded smart-meters or older smart-meters. The study confirms that these privacy friendly technologies can be comfortably implemented on such platforms. Therefore older meters may be retrofitted to support privacy using local or remote software upgrades, at no additional hardware costs. The study is currently under peer-review but available as a pre-print:

  [MDFSI11] Andres Molina-Markham and George Danezis and Kevin Fu and Prashant Shenoy and David Irwin. Designing Privacy-preserving Smart Meters with Low-cost Microcontrollers. Cryptology ePrint Archive: Report 2011/544. 3 Oct 2011.

- A large body of literature exposes the ineffectiveness of naïve anonymisation mechanisms. Merely removing personal identifiers from load profiles, does not fully prevent re-linkage of the readings to an individual. Trivial side information, such as house occupancy or on-line activity, can be used to re-identify a naively anonymised load profile. A study looking at the potential for re-identification of load profiles is due to be published as:

  [JJR11] Marek Jawurek, Martin Johns, Konrad Rieck. Smart Metering De-Pseudonymization. Annual Computer Security Applications Conference 2011. Orlando, USA, December 2011.

  The study finds that Microsoft Research privacy techniques are secure against this risk.

- The state of the art technologies for processing personal data to extract statistics are based on Differential Privacy. These data processing techniques ensure that published or shared aggregate statistics, for example on load profiles, do not leak information about an individual. A survey of results is available:

  [D08] Cynthia Dwork. 2008. Differential privacy: a survey of results. In Proceedings of the 5th international conference on Theory and applications of models of computation (TAMC'08), Manindra Agrawal, Dingzhu Du, Zhenhua Duan, and Angsheng Li (Eds.). Springer-Verlag, Berlin, Heidelberg, 1-19.

- The Microsoft Research privacy techniques do not necessitate any additional hardware or DCC components. Only Smart-meter software has to be adapted to support the technologies, and to output secured readings. The readings can be aggregated in real-time, and further computations can be performed by any user device. Deploying these readings to customer devices relies on currently available technologies such as the web applications, or smart-phone applications. Any future customer platform for computation or communication can be supported as it does need to be trusted to ensure the integrity of computations.

- The Microsoft Research privacy technologies support customer choice when it comes to privacy as well as usage of third party services. Customers that are less privacy sensitive can chose to revert to providing raw or periodic readings to the energy industry or any third parties – reverting to the current proposed architecture with no privacy protection. Customers that do not wish, or are not able, to manage interactions with the energy industry through their own devices may chose a third party provider that performs billing and other computations on their behalf. The secured readings provided to customers, can be used with third party value added services on the same basis as to regulated entities, ensuring that no competitive advantage exists due to privileged access to readings.

• • •

More information about Microsoft Research privacy solutions for smart metering is available at: *http://research.microsoft.com/privacy_in_metering/*

Microsoft would be pleased to provide further information or assistance on this review as required.

[redacted]

[redacted],
[redacted]

[redacted]
[redacted]
[redacted]

[redacted]
[redacted]

[redacted],
[redacted]

[redacted]
[redacted]
[redacted]
[redacted]

[redacted]
[redacted]