Cryptology ePrint Archive: Report 2011/544

Designing Privacy-preserving Smart Meters with Low-cost Microcontrollers

Andres Molina-Markham and George Danezis and Kevin Fu and Prashant Shenoy and David Irwin

Abstract: Smart meters that track fine-grained electricity usage and implement sophisticated usage-based billing policies, e.g., based on time-of-use, are a key component of recent smart grid initiatives that aim to increase the electric grid's efficiency. A key impediment to widespread smart meter deployment is that fine-grained usage data indirectly reveals detailed information about consumer behavior, such as when occupants are home, when they have guests or their eating and sleeping patterns. Recent research proposes cryptographic solutions that enable sophisticated billing policies without leaking information. However, prior research does not measure the performance constraints of real-world smart meters, which use cheap ultra-low-power microcontrollers to lower deployment costs. In this paper, we explore the feasibility of designing privacy-preserving smart meters using low-cost microcontrollers and provide a general methodology for estimating design costs. We show that it is feasible to produce certified meter readings for use in billing protocols relying on Zero-Knowledge Proofs with microcontrollers such as those inside currently deployed smart meters. Our prototype meter is capable of producing these readings every 10 seconds using a \$3.30USD MSP430 microcontroller, while less powerful microcontrollers deployed in today's smart meters are capable of producing readings every 28 seconds. In addition to our results, our goal is to provide smart meter designers with a general methodology for selecting an appropriate balance between platform performance, power consumption, and monetary cost that accommodates privacy-preserving billing protocols.

Category / Keywords: applications / zero-knowledge, privacy, metering, microcontrollers

Publication Info: Paper currently under review

Date: received 3 Oct 2011

Contact author: amolina at cs umass edu

Available formats: PDF | BibTeX Citation

Version: 20111003:174531 (All versions of this report)
