Challenging the Self-evident

George Danezis

Dept. of Computer Science,

University College London.

What is cryptography good for?

- Alice and Bob love each other …

They can use TLS1.2, OTR, IPSec, Tor to sweet talk in secret.

- Alice and Bob do not trust each other …

I need your half-hourly smart meter readings to calculate the correct bill.

I am not sure what else you are going to do with this information.

Alice's Home

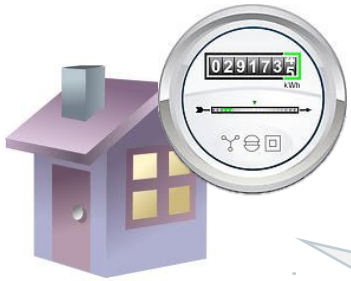
Bob Energy Ltd.

The self-evident surveillance option: A “Trusted Party” computes the bill

Tough s**t. Give me the data or your electricity will be more expensive.

Time to do some analytics to find out how to extract more “value” from Alice.

Maybe I could sell the data too!



All the metering data …

Alice’s Home

Eh … here it is.

Bob Energy Ltd.

The Inevitable:
“It is necessary to have the data to compute accurate time-of-use bills.”

Let me just have a look, to make sure Alice is not a terrorist (or grows weed, or suffers from early prostate cancer)

The privacy-friendly option 1: Meters compute bills (no crypto)

Meter is told tariffs and computes bill

I have to rely on the meter to give correct readings anyway …

Just the monthly bill …

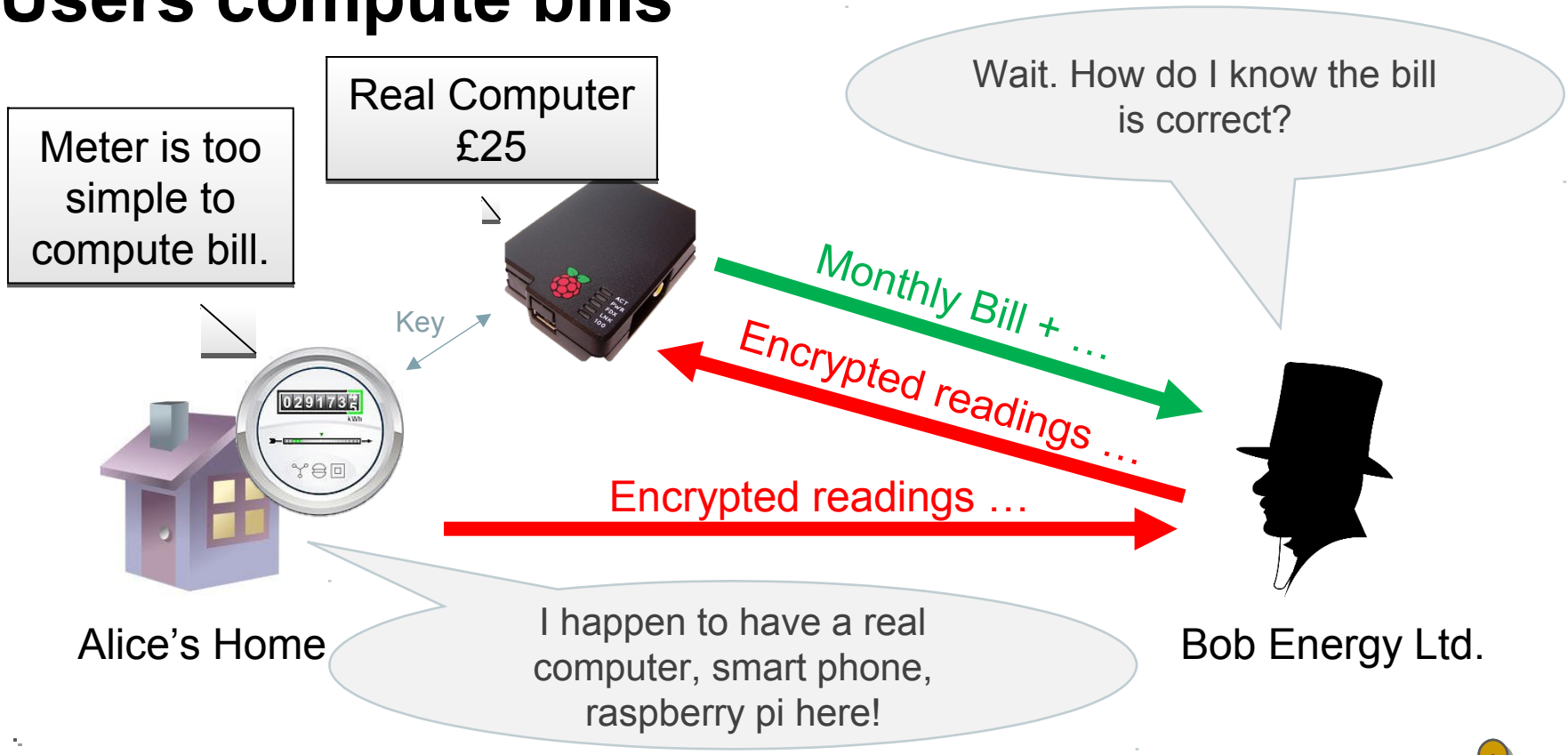
Let the meter compute the bill.

Alice's Home

Bob Energy Ltd.

The Truth about Smart Meters: They are really not that smart.
(< 100 Kb of memory, 9600bps unreliable modem, delicate things …)

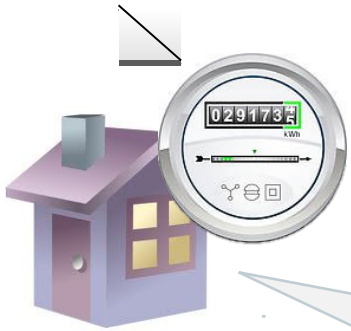
The privacy-friendly option 2: Users compute bills



The magic of modern cryptography: Alice's device can prove it performed the computation of the bill correctly, without revealing the readings. ("*Zero Knowledge Proof*")

The privacy-friendly option 3: A collection of authorities compute bills

Meter is too simple to compute bill.



Alice's Home

PRIVACY INTERNATIONAL

OPEN RIGHTS GROUP

EFF

Encrypted readings …

Encrypted readings …

Monthly Bill + …

Bob Energy Ltd.

I trust that not all "authorities" will collude to violate my privacy.

Impossible.

The magic of modern cryptography: Any computation can be split amongst *n*-parties, that do not learn the secret inputs, and cannot influence the correct result. ("*Secure Multiparty Computation*")

The research

Alfredo Rial, George Danezis: **Privacy-preserving smart metering.** WPES 2011: 49-60

Klaus Kursawe, George Danezis, Markulf Kohlweiss: **Privacy-Friendly Aggregation for the Smart-Grid.** PETS 2011: 175-191

George Danezis, Markulf Kohlweiss, Alfredo Rial: **Differentially Private Billing with Rebates.** Information Hiding 2011: 148-162

George Danezis, Benjamin Livshits: **Towards ensuring client-side computational integrity.** CCSW 2011: 125-130

Andres Molina-Markham, George Danezis, Kevin Fu, Prashant J. Shenoy, David E. Irwin: **Designing Privacy-Preserving Smart Meters with Low-Cost Microcontrollers.** Financial Cryptography 2012: 239-253

Gilles Barthe, George Danezis, Benjamin Grégoire, César Kunz, Santiago Zanella Béguelin: **Verified Computational Differential Privacy with Applications to Smart Metering.** CSF 2013: 287-301

George Danezis, Cedric Fournet, Markulf Kohlweiss and Santiago Zanella-Beguelin. **Smart Meter Aggregation via Secret-Sharing.** ACM SEGS 2013: Smart Energy Grid Security Workshop, Berlin, 2013.

Carmela Troncoso, George Danezis, Eleni Kosta, Josep Balasch, Bart Preneel: **PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance.** IEEE Trans. Dependable Sec. Comput. 8(5): 742-755 (2011)

George Danezis, Markulf Kohlweiss, Benjamin Livshits, Alfredo Rial: **Private Client-Side Profiling with Random Forests and Hidden Markov Models.** Privacy Enhancing Technologies 2012: 18-37

Engineering is all about choices.