S. Brinkhaus, D. Carluccio, U. Greveler, B. Justus, D. Löhr, C. Wegener

SMART HACKING FOR PRIVACY

Abstract

Advanced metering devices (aka smart meters) are nowadays being installed throughout electric networks in Germany, in other parts of Europe and in the United States. Due to a recent amendment especially in Germany they become more and more popular and are obligatory for new and refurbished buildings.

Unfortunately, smart meters are able to become surveillance devices that monitor the behavior of the customers leading to unprecedented invasions of consumer privacy. High-resolution energy consumption data is transmitted to the utility company in principle allowing intrusive identification and monitoring of equipment within consumers' homes (e.g., TV set, refrigerator, toaster, and oven) as was already shown in different reports.

This talk is about the Discovergy / EasyMeter smart meter used for electricity metering in private homes in Germany. During our analysis we found several security bugs that range from problems with the certificate management of the website to missing security features for the metering data in transit. For example (un)fortunately the metering data is unsigned and unencrypted, although otherwise stated explicitly on the manufacturer's homepage. It has to be pointed out that all tests were performed on a sealed, fully functionally device.

In our presentation we will mainly focus on two aspects which we revealed during our analysis: First the privacy issues resulting in even allowing to identify the TV program out of the metering data and second the "problem" that one can easily alter data transmitted even for a third party and thereby potentially fake the amount of consumed power being billed.

In the first part of the talk we show that the analysis of the household’s electricity usage profile can reveal what channel the TV set in the household is displaying. We will also give some test-based assessments whether it is possible to scan for copyright-protected material in the data collected by the smart meter.

In the second part we focus on the data being transmitted by the smart meter via the Internet. We show to what extent the consumption data can be altered and transmitted to the server and visualize this by transmitting some kind of picture data to Discovergy’s consumption data server in a way that the picture content will become visible in the electricity profile. Moreover, we show what happens if the faked power consumption data reflects unrealistic extreme high or negative power consumptions and how that might influence the database and service robustness.