Is your utility meter getting personal?

October 30 2012, by Steven Powell

As of 2010, more than a third of all utility meters in the United States used wireless automatic meter reading (AMR) technology – 47 million in all. They make it a lot easier for the utility company to gather data on electricity, natural gas and water usage. But as a University of South Carolina research team has shown, it's possible for their unencrypted broadcasts to be intercepted, giving a sophisticated eavesdropper a window into household activities.

Lead researcher Wenyuan Xu, a professor in USC's College of Engineering and Computing, says that much of the focus in the research security community right now is on the next generation of devices, the so-called "smart" meters. Utilities hope in the future they will be able to use these smart meters to match electricity flow to individual houses with overall demand, enabling much more efficient allocation of resources.

"There's been a lot of discussion about smart meters and whether they're secure or not," said Xu. "But smart meters are not yet widespread. So we wanted to look at the wireless readers common now. Are they secure? Will they leak private information?"

Wireless meters greatly reduce the need for human operators. A single truck can drive through a neighborhood and collect usage information on hundreds of dwellings that previously required a reader to walk to each meter and record data by hand.

Xu and her team reported at October's Association for Computing Machinery (ACM) conference on Computer and Communications

Security that they found neither security nor privacy in the representative AMR systems they tested. AMR systems use proprietary devices and communications protocols, and Xu's team was able to reverse-engineer the transmissions to obtain access to the usage data.

Once they understood how to read the data, they conducted an eavesdropping experiment in a local apartment complex. Using a modestly priced antenna and laptop located inside one of her graduate student's apartment, they were able to detect dozens of nearby electricity meters. By adding an inexpensive amplifier to the system, they were able to gather electrical data from every apartment in the complex – hundreds of units up to 500 yards away.

"We were able to detect even further than we expected," said Xu. "The complex had 408 units, but we were able to see 485, so we were seeing beyond the complex itself."

The data being transmitted had the potential to be matched to the individual dwellings because the transmitted packets contained an identification number that was stamped on the meter itself.

The team's analysis showed that, beyond raw usage data, a range of information could be deduced from analyzing the meter's activity, particularly when it came to electricity. "Most electrical meters broadcast data every 30 seconds," said Xu. "The gas and water meters, because they run on batteries, only transmit data after a wake-up call."

The detailed electricity data gave information about activities within the household – when the inhabitants got up, went to work and got home, for example. The team was able to deduce that 27 of the apartments within the complex were unoccupied.

That sort of information could be harmful in the wrong hands. Xu is

careful not to reveal too much detail in her publications, she said. "We don't want the bad guys to know too much. It's about letting the right people know what needs to be better protected."

The good news is that reliance on what's often called "security through obscurity" appears to be working. Obtaining personal household data through wireless meters is difficult. What Xu and her team hopes is that drawing attention to the potential for problems might help the industry realize the necessity of designing systems with security in mind.

"The meter data should have been encrypted before transmission and authenticated by readers in the drive-by trucks to prevent the potential misuses that we've discovered," said Xu.

Provided by University of South Carolina

Citation: Is your utility meter getting personal? (2012, October 30) retrieved 27 April 2024 from https://phys.org/news/2012-10-meter-personal.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.