

Get AP Mobile for your phone at APnews.com



Security researchers offer caution on smart grids



By JORDAN ROBERTSON

Published: Jul 31, 2009

Story user rating:



LAS VEGAS (AP) - The race to build a "smarter" electrical grid could have a dark side. Security experts are starting to show the dangers of equipping homes and businesses with new meters that enable two-way communication with utilities.

There are many benefits to upgrading the nation's electricity networks, which is why a smart-grid movement was already revving up before the recent economic recovery package included \$4.5 billion for the technology. Smarter grids could help conserve energy by giving utilities more control over and insight into how power flows.

But presentations at the Black Hat and DefCon security conferences here this week highlighted potential problems with moving too fast.

The risks are similar to what happens when computers are linked over the Internet. By exploiting weaknesses in the way computers talk to each other, hackers can seize control of innocent people's machines.

In the case of the power grid, better communication between utilities and the meters at individual homes and businesses raises the possibility that someone could control the power supply for a single building, an entire neighborhood, or worse.

In one of the talks here, Mike Davis, a senior security consultant with Seattle-based IOActive Inc., demonstrated how a computer worm could hop between the meters at homes and businesses in a smart grid network. The worm could give miscreants remote control of the meters, which would let them take advantage of a utility's ability to, for example, disconnect someone's power for not paying his bill.

The key vulnerability was found in devices made by only one manufacturer, a company that Davis did not name. But he said the worm could have spread to other manufacturers' products that used the same communications technologies and can be used to remotely disconnect people's power.

To get the computer worm going, a hacker might have to get physical access to one of the meters in order to program it with malicious code. That could

start a chain reaction in which the worm spreads meter to meter over the grid's communication network. This hack might also be done remotely, Davis said, if the traffic on the network isn't encrypted, which means it's not cloaked in special computer coding so outsiders can't read it.

Davis compared the security of the nascent smart grids to the early days of the personal computer.

"Every time we redesign a new technology like this, we're doomed to relive the '80s and '90s all over again and the same vulnerabilities," he said.

Davis says he supports the smart-grid movement, but is troubled that smart meters are being deployed with remote-disconnect capabilities. Without that, "there's no real danger," he said.

The more benign uses of smart meters are why they're so hot. They help utilities distribute power more efficiently, and they could help consumers lower their bills by giving them more flexibility in how their homes use power. For instance, people could set appliances in their homes to scale down power consumption in peak times, when electricity is more expensive.

More than 50 million smart meters are expected to be deployed by U.S. electric utilities by 2015, according to a list of publicly announced projects kept by The Edison Foundation. More than 8 million have already been deployed.

Davis' research was commissioned by an unidentified utility. Other security researchers said it's uncommon for utilities to open their doors for outside hackers to test their technologies, which means Davis' research provides a rare public view of some of the problems that can crop up in smart grid rollouts.

Ed Legge, spokesman for Edison Electric Institute, a trade organization for shareholder-owned electric companies, said utilities are already doing similar security testing that isn't made public.

"We have the ultimate vested interest in securing our systems - if they stop working, or if they are brought down in any way, we can't run our businesses, and we lose money," he said. "We can't make this car without a seat belt. We have to be deliberate about this."

Some people in the industry argue that a more connected grid could be even safer than the aging and patchwork energy-distribution system we have now, because with new technology, security can be baked in from the start.

That argument rings hollow to some security researchers. They point out that the grid is already under attack, and that smart meters can create even more openings.

Spies have broken into parts of the U.S. electric grid and left behind programs that would allow them to disrupt service, government officials revealed this

spring. The intrusions were discovered only after some electric companies opened their doors to audits. The full scope of the attacks is unknown, though, because the government doesn't have blanket authority to examine other electric systems.

Tony Flick, a principal with the Tampa, Fla.-based Fyrm Associates Inc., who spoke in Las Vegas on the regulations surrounding smart-grid security, says the system suffers from some of the same problems as the credit card industry, which lets many retailers self-certify that they're following the rules designed to prevent data breaches.

"In smart grids, utility companies are largely self-policing" their security, Flick said. "There's this gold rush to basically grab some of that money to get it out there, but when you rush things to market you're more likely to make mistakes."

AP Mobile. © 2009 The Associated Press. All Rights Reserved.