

Monday, April 05, 2010

Hacking the Smart Grid

One researcher shows how your house's power could be shut down remotely, but the threat is only theoretical--for now.

By Robert Lemos

Components of the next-generation smart-energy grid could be hacked in order to change household power settings or to spoof communications with a utility's network, according to a study of three pilot implementations.

The problems were highlighted in a presentation given last week by security researcher Joshua Wright of [InGuardians \(http://www.inguardians.com/\)](http://www.inguardians.com/), a consulting firm with many infrastructure companies among its clients. Vulnerabilities discovered by Wright could let attackers remotely connect to a device or to intercept communications with the managing power company.

The report caused a kerfuffle, and InGuardians has refused to disclose further details. However, one expert familiar with the content of Wright's presentation says that it highlights security problems with many devices. "These are fairly common mistakes," says Marcus Sachs, director of the Internet Storm Center, part of the SANS Institute, where Wright presented his research. "Most of the wireless meters are subject to the same vulnerabilities that we saw [in Wi-Fi devices] 10 years ago."

The power industry is in the midst of a massive rollout of smart-grid technologies fueled by \$3.4 billion in stimulus funds. By delivering detailed usage information, smart meters promise to allow consumers to control their power usage and to enable power companies to better manage their distribution networks. Nearly 60 million smart meters--covering half of the U.S. households and businesses--are expected to be deployed this year, according to estimates by the Edison Foundation's [Institute for Electrical Efficiency \(http://www.edisonfoundation.net/iee/\)](http://www.edisonfoundation.net/iee/).

To help test the infrastructure, InGuardian's Wright created an open-source hacking tool, dubbed KillerBee. This tool lets security researchers test the security of the most popular wireless communications protocol for smart meters, a low-power wireless communications technology called ZigBee. This protocol has a longer range than Bluetooth and is the most popular way of creating a home-area network (HAN).

"It's how your meter--the gateway--will talk to your dryer, your thermostat, and your water heater," says John Shaw, senior vice president of products and technology at [Industrial Defender \(http://www.industrialdefender.com/\)](http://www.industrialdefender.com/), an infrastructure security company.

Researchers have previously warned that allowing network access to the home opens up a host of security issues. Last year, security firm IOActive [found flaws \(http://www.technologyreview.com/computing/23179/\)](http://www.technologyreview.com/computing/23179/) in a smart-meter device that allowed its researchers to insert code into one device and have it spread to others--essentially, injecting a computer worm into a local power network.

"If you could get that meter to talk to its neighbors and those to talk to their neighbors, you could conceptually tell them to turn off and cause a fairly broad power outage," Shaw says.

The [ZigBee Alliance \(http://www.zigbee.org/\)](http://www.zigbee.org/), which oversees the protocol, has submitted its specification for smart-grid-specific communications to three separate security reviews, according to Bob Heile, the group's chairman. "What comes back is that [the specification] is okay, but there are always suggestions to make it better," Heile says. "We always implement those suggestions."

Using KillerBee, Wright found that some ZigBee devices exchange encryption keys in the open, allowing an eavesdropper to grab the information needed to clone a device, the researcher stated in a presentation given late last year at ToorCon, a hacking conference.

"He developed a suite of tools that allows (hackers) to do what they can do in the wired world," says the SANS Institute's Sachs. "If you have a radio that can receive ZigBee, then you can use these same tools."

Despite the latest research report, the threat remains theoretical for now. Smart meters are not yet attached to most households, device manufacturers are taking security more seriously, and utilities are testing their networks for vulnerabilities, says Industrial Defender's Shaw. Overall, the manufacturers and utilities have become better at talking to security researchers, he says.

"Yes, there are vulnerabilities there, but this is more of a public relations issue and a nuisance issue than a threat to the power infrastructure," Shaw says. He points to an industrywide agreement on a single process for upgrading software on the devices as a sign of progress.

David Baker, director of services for IOActive, another company that counts power companies and device manufacturers among its clients, also says that the industry as a whole is making progress. "The utilities are acutely aware of the issues and are trying their damndest to fix the problems." Baker says. "It is getting really, really difficult to find these holes now."

Copyright Technology Review 2010.

Upcoming Events

[Green:Net 2010 \(http://events.earth2tech.com/greenet/10/\)](http://events.earth2tech.com/greenet/10/)

San Francisco, CA

Thursday, April 29, 2010

<http://events.earth2tech.com/greenet/10/> (<http://events.earth2tech.com/greenet/10/>)

[BetterWorld at MIT Conference \(http://www.betterworldatmit.org\)](http://www.betterworldatmit.org)

MIT Media Lab, Cambridge, MA

Friday, April 30, 2010

<http://www.betterworldatmit.org> (<http://www.betterworldatmit.org>)

[FEI 2010 – The Annual Front End of Innovation Conference A New Front End: The Era of Collaboration \(http://www.iirusa.com/feiusa/fei-home.xml?registration=FEI2010TECHREV\)](http://www.iirusa.com/feiusa/fei-home.xml?registration=FEI2010TECHREV)

Boston, MA

Monday, May 03, 2010 - Wednesday, May 05, 2010

<http://www.iirusa.com/feiusa/fei-home.xml?registration=FEI2010TECHREV>

[\(<http://www.iirusa.com/feiusa/fei-home.xml?registration=FEI2010TECHREV>\)](http://www.iirusa.com/feiusa/fei-home.xml?registration=FEI2010TECHREV)

[BIO International Convention \(<http://convention.bio.org>\)](http://convention.bio.org)

Chicago, IL

Monday, May 03, 2010 - Sunday, May 10, 2009

<http://convention.bio.org> (<http://convention.bio.org>)

[MIT Sloan CIO Symposium \(<http://www.mitcio.com>\)](http://www.mitcio.com)

MIT Campus, Cambridge, MA

Wednesday, May 19, 2010

<http://www.mitcio.com> (<http://www.mitcio.com>)

[Tech Connect World \(<http://www.techconnectworld.com>\)](http://www.techconnectworld.com)

Anaheim, CA

Monday, June 21, 2010 - Friday, June 25, 2010

<http://www.techconnectworld.com> (<http://www.techconnectworld.com>)

[2010 IEEE Conference on Innovative Technologies for an Efficient and Reliable Electricity Supply \(<http://www.ieee-energy.org/>\)](http://www.ieee-energy.org/)

Waltham, Massachusetts

Sunday, September 27, 2009 - Tuesday, September 28, 2010

<http://www.ieee-energy.org/> (<http://www.ieee-energy.org/>)