Hacking the Smart Grid

The technology could open up all kinds of opportunities for attackers, researchers say.

The hurried deployment of smart-grid technology could leave critical infrastructure and private homes vulnerable to hackers. Security experts at the Black Hat conference in Las Vegas last week warned that smart-grid hardware and software lacks the necessary safeguards to protect against meddling.

Smart enough? This image shows the interior of a smart grid meter tested by Mike Davis of IOActive.
Credit: Mike Davis

Utilities are being encouraged to install this smart-grid technology--network-connected devices to help intelligently monitor and manage power usage--through funding from the U.S. government's 2009 stimulus package. The smart systems could save energy and automatically adjust usage within homes and businesses. Customers might, for example, agree to let a utility remotely turn off their air conditioners at times of peak use in exchange for a discount.

But to receive the stimulus money, utilities will have to install new devices across their entire customer base quickly. Security experts say that this could lead to problems down the road--as-yet-unknown vulnerabilities in hardware and software could open up new ways for attackers to manipulate equipment and take control of the energy supply.

Smart-grid deployments involve installing smart meters in homes and businesses across a utility's coverage area. These meters can communicate with the utility and with other networked devices--usually via a wireless network of some type. Some ways to hijack this type of equipment have already been revealed. Last year, Mike Davis, a senior security consultant at IOActive, created a piece of software that could spread automatically between smart grid hardware in different homes. The software would then be capable of shutting equipment down.

The security of the smart grid was a major topic at Black Hat. The conference brings together researchers from academia, industry, government, and the hacking underground.

Jonathan Pollet, founder and principal consultant at Red Tiger Security, a firm that analyzes the security of critical infrastructure, says the smart grid could be vulnerable to a range of attacks. Customers might simply figure out, for example, how to lower their electricity bills by manipulating how much energy their meters say they're using. But he says large-scale attacks may also be possible. A serious vulnerability might make it possible to shut down the power supply to an entire city.

The devices being deployed by utilities are meant to last for 15 to 20 years. It may be difficult and costly to apply security patches to these distributed systems, especially because they can't easily be taken out of commission for routine maintenance.

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, 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.

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, 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 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, 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 damnedest to fix the problems." Baker says. "It is getting really, really difficult to find these holes now."