



**CNN.com**

 **PRINT THIS**

Powered by  Clickability

## 'Smart Grid' may be vulnerable to hackers

- Story Highlights
- Smart Grid will use advanced sensors to improve electricity efficiency and reliability
- Cyber-security experts say some types of meters can be hacked
- Company: \$500 in materials, electrical background all that's needed to hack system
- Officials say they have made system better, working to make it even more secure

By Jeanne Meserve  
CNN Homeland Security Correspondent

**WASHINGTON (CNN)** -- Is it really so smart to forge ahead with the high technology, digitally based electricity distribution and transmission system known as the "Smart Grid"? Tests have shown that a hacker can break into the system, and cybersecurity experts said a massive blackout could result.

Until the United States eliminates the Smart Grid's vulnerabilities, some experts said, deployment should proceed slowly.

"I think we are putting the cart before the horse here to get this stuff rolled out very fast," said Ed Skoudis, a co-founder of InGuardians, a network security research and consulting firm.

The Smart Grid will use automated meters, two-way communications and advanced sensors to improve electricity efficiency and reliability. The nation's utilities have embraced the concept and are installing millions of automated meters on homes across the country, the first phase in Smart Grid's deployment. President Obama has championed Smart Grid, and the recent stimulus bill allocated \$4.5 billion for the high-tech program.

But cybersecurity experts said some types of meters can be hacked, as can other points in the Smart Grid's communications systems. IOActive, a professional security services firm, determined that an attacker with \$500 of equipment and materials and a background in electronics and software engineering could "take command and control of the [advanced meter infrastructure] allowing for the en masse manipulation of service to homes and businesses."

Experts said that once in the system, a hacker could gain control of thousands, even millions, of meters and shut them off simultaneously. A hacker also might be able to dramatically increase or decrease the demand for power, disrupting the load balance on the local power grid and causing a blackout. These experts said such a localized power outage would cascade to other parts of the grid, expanding the blackout. No one knows how big it could get.

The utility industry has made significant improvements to the power grid since the blackout of 2003, which disrupted power to an estimated 50 million people in the eastern United States and Canada. The utility industry said it is now better able to detect and isolate outages, and some elements of Smart Grid technology will enhance that capability.

Also, industry representatives said, they have no intention of putting an unsafe grid online.

"We are not going to manufacture this car without a seat belt," said Ed Legge, a spokesman for the Edison Electric Institute.

But as of now there are no clear-cut Smart Grid cybersecurity standards.

"There are a lot of discussions about where the requirements will come from and who will be ultimately responsible," said a Department of Homeland Security official, speaking on background.

Itron, a major manufacturer of automated meters, said its products are secure. Matt Spaur, a senior product marketing analyst, said his company tried to make hacking a meter "unappealing and unrewarding if you do it. And it is very traceable." But Spaur acknowledged that the Smart Grid is vulnerable.

"Any network can be hacked," he said.

One expert said security concerns have put "the fear of God" into the utility industry, vendors of Smart Grid products and the federal government. They have been working cooperatively to detect and mitigate vulnerabilities.

"Industry is working to make meters more secure. They have done a good job," said Joe Weiss, an expert on utility control systems.

Still, experts like Skoudis recommended that Smart Grid deployment be slowed until security vulnerabilities are addressed. Otherwise, he said, Smart Grid equipment deployed now may have to be replaced later.

Utility managers are taking heed.

Garry Brown, chairman of New York's Public Service Commission, said he believes the benefits of Smart Grid outweigh the risks, but his state is taking a hard look at cybersecurity before making large investments in the technologies.

"Before we go rushing headstrong into a Smart Grid concept, we have to make sure that we take care of business, in this case cybersecurity," he said.

William Sanders, principal investigator for the National Science Foundation Cyber Trust Center on Trustworthy Cyber Infrastructure for the Power Grid, concurs.

"I don't think the sky is falling," he said. "I don't think we should stop deployment until we have it all worked out. But we have to be vigilant and address security issues in the Smart Grid early on."

All About [Computer Security](#) • [Energy Technology](#)

**Find this article at:**

<http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html>

Check the box to include the list of links referenced in the article.

2008 Cable News Network