

CNET News

[Security](#)

April 10, 2009 4:00 AM PDT

Just how vulnerable is the electrical grid?

by [Elinor Mills](#)

- [Font size](#)
- [Print](#)
- [E-mail](#)

Smarter is not always better--at least when it comes to utilities.

More than a decade after initial reports said critical infrastructure in the U.S. is vulnerable to cyberattack, the situation has only worsened as utilities move their control systems closer to the Internet and install smart-grid technology, according to security experts.



Questions about the security of infrastructure in the United States arose this week following a [Wall Street Journal report](#) that said the nation's electricity grid has been compromised by foreign hackers. And several experts said in interviews this week that some energy systems have, in fact, gotten less secure as they have modernized. The Supervisory Control and Data Acquisition (SCADA) control systems used by the energy industry used to be segregated from public networks. But they have increasingly become more dependent on Internet protocol-based systems, the experts said. At the same time, their security precautions are inefficient, they said.

"The end result is that, as part of our modernization, we've made ourselves more vulnerable," said James Lewis, a senior fellow at the nonprofit Center for Strategic and International Studies (CSIS).

"Plant control networks (and their programmable logic controllers) should be disconnected from the Internet," said Peter "Mudge" Zatko, technical director of the national intelligence research unit at BBN Technologies. "These are the things lifting and lowering the plutonium rods into the water to make steam...It's on the Internet. This is terrifying."

Myriad operational problems

For many utility workers, it's easier to log onto the Internet from home when they get called at night. But if those home computers are infected with spyware, they can be used by attackers to get into the control systems, which are supposed to be separated from the

Internet.

And there are other problems that are more deeply embedded in the day-to-day operations of a utility's business. Network control software that utilities buy from outside vendors often includes the ability to run Web servers and enable remote access and wireless access. Then there are configuration problems, such as [routers](#) and other systems that use default passwords, or worse, don't use passwords at all, according to Zatko and others who have tested the systems.

"It's out of ease-of-use and the fact that there weren't strong restrictions (the electric utilities were deregulated to a large extent) that the networks are a mess in a lot of places," Zatko said. Often, "the systems themselves aren't robust because they were designed to be on networks that weren't talking to the public Internet."

Many warnings have been sounded over the years. In 1999, Zatko compiled a list of about 30 utilities whose plant control networks could be accessed remotely, and he says many of them still have the same problems today. In 2004, [Gartner did a report](#) concluding that the use of IP networks for critical infrastructure could serve as bait for cyberattackers.

"It's painfully easy to exploit" the control systems, said Frank Heidt, chief executive of professional security services company Leviathan Security. "Energy management systems really can't be connected to the Internet. It's going to be painful for some companies, but they're going to have to change this."

[Last year](#), a security expert at the RSA conference detailed how easy it is to break into power plants by downloading malware to employee computers through a socially engineered e-mail that directs them to a malicious server. Meanwhile, [Core Security found a hole](#) in the Suitelink software that is used to automate operations at power stations, oil refineries, and production lines.

Lewis of the CSIS acknowledged that using the Internet opens utilities up to cyberattack risks, but said there are "sound economic reasons" for them doing so.

"Most of the critical infrastructure on the Internet is there for legitimate business purposes," agreed John Bumgarner, a research director at the nonprofit U.S. Cyber Consequences Unit.

"Energy management systems really can't be connected to the Internet. It's going to be painful for some companies, but they're going to have to change this."

--Frank Heidt
CEO, Leviathan Security

Security company Industrial Defender has done more than 100 threat assessments over the past seven years, primarily in utility infrastructure, and identified 34,000 vulnerabilities, said company CEO Brian Ahern.

For the most part, utilities--among the most conservative businesses in spending on technology--don't do basic security monitoring of their power generation and distribution equipment, he said.

"You can't protect when you don't know what's happening. I think that less than five percent of utilities have a good sense of critical threats," he said.

Utilities "are sacrificing security for convenience and cost savings," said Richard Forno, a principal at KRvW, an information security consulting firm in Washington, D.C. "We've allowed the situation to get worse, and it will be harder to get away from these networks touching the public Net now that we are 10 years, 15 years into the process."

Smart grids: Efficient but insecure

IP networks aren't the only problem. The use of smart-grid technology, which consists of networked meters designed for adjusting electricity flows and monitoring everything from power plants to individual appliances in homes, are also putting critical systems at risk, experts said.

Critical infrastructure insiders in the U.S. and Canada [surveyed last year](#) said the energy sector was the industry most vulnerable to cyberattack. The survey cited many contributing factors: an increase in the number of access points through the use of sensors, smart meters, and third-party contractors with remote access capability; use of more IP-based networks; integration between corporate and operational networks; reliance on standard or commodity IT platforms such as Microsoft Windows; and lack of attention to security by network automation and control system vendors. The biggest bottleneck to improving critical infrastructure security is cost, followed by apathy, they said.

"We've got to take a step back from the hurry-up approach with the smart grid. There needs to be a balanced approach between investing in (smart grid)

In March, IOActive, which provides application and smart-grid security services, said it had verified "significant" and "inherent" security flaws with multiple smart-grid platforms" and found them susceptible to common security vulnerabilities such as protocol tampering, buffer overflows, persistent and non-persistent rootkits, and code propagation.

"These vulnerabilities could result in attacks to the smart-grid platform causing utilities to lose momentary system control of

deployments and building security deeply into it."

**--Brian Ahern
CEO, Industrial Defender**

their advanced metering infrastructure smart meter devices to unauthorized third parties," the company [said in a release \(PDF\)](#). "This would expose utility companies to possible fraud, extortion attempts, lawsuits, or widespread system interruption."

More than 2 million smart meters are in use in the U.S. today, and an estimated 73 utilities have ordered 17 million additional smart meters, according to IOActive. The Obama administration's proposed 2010 budget has earmarked \$4.5 billion for smart-grid technologies in the electricity infrastructure.

"The plan now would be to put in largely unsecured networks for smart grid," said Lewis of CSIS. "Hopefully they'll fix it."

The worst case scenario is that a person would access and control a smart meter and control other networked smart meters - to disrupt the grid, said Ahern of Industrial Defender.

Standards for securing smart-grid technologies are still being finalized, but Ahern thinks that government-led efforts to modernize the grid should focus more on designing security in right at the beginning.

"We've got to take a step back from the hurry-up approach with the smart grid," he said. "There needs to be a balanced approach between investing in (smart grid) deployments and building security deeply into it."

The vulnerability of the critical infrastructure isn't news, so why the Wall Street Journal report, with its unnamed sources, now?

The story is likely linked to turf battles within the federal government over which agency will oversee the cybersecurity policies, and get the funding for it, several of the security experts suggested. For instance, the [Department of Homeland Security has been criticized](#) for not doing enough on cybersecurity, while the [director of Homeland Security's National Cybersecurity Center resigned recently](#), accusing the NSA of trying to wrest control.

The Obama administration in December [ordered officials to do a 60-day review](#) on the Department of Homeland Security's cybersecurity efforts, and that report is due to be released next week.

Meanwhile, the [administration's proposed 2010 budget](#) includes \$355 million to support the base operations of the National Cyber Security Division and the efforts of the

Comprehensive National Cybersecurity Initiative.

"We're right at the point where they're naming new cybersecurity czars and there's a grab for funding between the Air Force, Navy, NSA, and others that want the cybersecurity budget," said Zatzko. "There are a lot of renewed efforts in this particular field, and it's a field that's in a fair amount of disarray."

While experts discuss cybersecurity threats, physical attacks on infrastructure are taking place. AT&T [said on Thursday](#) that vandals are to blame for the massive phone and Internet outage in Silicon Valley on Thursday.

(CNET News' Martin LaMonica contributed to this report.)



Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. [E-mail Elinor](#).

Related

From CNET

[Microsoft: Scareware, PDF exploits rise](#)

[The marriage of identity yin and security yang](#)

[Report: Smart-grid hackers could cause blackouts](#)

From around the web

[Power Grid Hack Highlights Where Governm... eWeek](#)

[Threat Level - Wired Blogs](#) Wired

[More related posts](#) powered by  Sphere