

The Radio InterOperability System bridges the communications gap between disparate radios, satellite, cell, and VOIP phones



HSDailyWire  
2009 Media Kit  
USE OUR INTELLIGENCE

# HSDailyWire.com

THE BUSINESS OF HOMELAND SECURITY

USE OUR INTELLIGENCE

Home Transport / Border Biometrics Continuity / Recovery Infrastructure / IT Biodefense Surveillance Detection Sci / Tech Markets Policy Energy Search

Thursday, 30 April 2009

Marketplace Sign up

## Smart Grid offers savings, vulnerabilities

Published 30 April 2009

**A bill to be presented in Congress today aims to stop utility hackers; experts, legislators call for regulations on smart power meters to reduce new grid's vulnerability to hacking**

When it comes to the power grid, the debate between smart and secure may be about to heat up (see "Smart Grid Vulnerable to Hackers," 23 March 2009 *HS Daily Wire*). Today, Senator Joe Lieberman (I-Connecticut) and Representative Bennie Thompson (D-Mississippi) plan to release a draft of the Critical Electric Infrastructure Protection Act (CEIPA), a bill aimed at tightening the cybersecurity of the U.S. power grid. The new legislation responds to growing political attention to the lack of digital security surrounding the U.S. power system, including revelations earlier this month that cyberspies had penetrated American utility networks and may be capable of causing massive blackouts.

*Forbes's* Andy Greenberg writes that older generations of power systems are not the only ones vulnerable to hackers. So are the new smart metering systems slowly being rolled out in pilot programs across the country, cybersecurity researchers argue. Under the CEIPA bill, those technologies, aimed at responding to changing energy supplies in real-time and integrating wind and solar power, could also face new cybersecurity regulations.

In a statement, the House Committee on Homeland Security said the new bill requires the Federal Energy Regulation Commission, "to assess and establish interim standards deemed necessary to protect against known cyber threats to critical electric infrastructure." A source familiar with the draft text of the bill adds that the "critical electric infrastructure" would include "any system assets used for generation, transmission, distribution or metering of electric energy."

Including "metering" technology in that energy infrastructure definition puts smart-grid technology squarely in the regulatory spotlight--the systems use wireless "smart meters" to adjust energy demand and relay power-use data back to utilities. This smart-grid addendum is timely: Advocates of the smart grid argue that a power system revamp is necessary to deal with ballooning energy prices, which are estimated to increase 20 percent over the next 10 years. President Obama's economic stimulus package includes \$4.5 billion devoted to implementing smart-grid technologies.

Greenberg writes that even as enthusiasm around the smart grid grows, several cybersecurity researchers have warned about the potential for exploiting smart meters to disable or take control of electric networks. In January, for instance, independent cybersecurity researcher Travis Goodspeed gave a presentation at the S4 conference in Miami, describing a method for bypassing the encryption on Zigbee wireless chips, the same sort of technology that some metering systems would use to communicate with a smart grid.

By inserting a hypodermic needle into a meter's circuit board and using an oscilloscope to read the electrical signals before they're encrypted, Goodspeed was able to obtain the gadget's cryptographic key, a trick that could potentially be used to gain wider access to the grid. "You would just listen to the transmission and impersonate it," says Goodspeed. "Once you got the key, you could control not just that meter you stuck the needle into, but any meter in the system."

Last month, researchers at security firm IOActive used Goodspeed's research to create a proof-of-concept exploit that could potentially spread from meter to meter, taking control of an entire network. The company presented its findings in a Department of Homeland Security hearing on smart-grid security in March. Josh Pennell, IOActive's chief executive and founder, argues that smart meters in general are being pushed to market too fast to build them securely. "What you have is a highly accelerated product space," he says. "Smart-grid systems are being designed like it's 1990, as if everyone with access to them is our friend."

Whether either of those researchers' work represents "known cyber threats to critical electric infrastructure," as CEIPA's regulations would stipulate, still isn't clear. In fact, both IOActive's researchers and Goodspeed declined to name any smart-meter vendors that are vulnerable to cyber attacks for fear of informing potential malicious hackers. Goodspeed's exploit was also performed on an earlier generation of chip than the one used in some smart meters, though he says he plans to reveal vulnerabilities in the newest chip versions at the Black Hat security conference in August.

These ambiguities mean that assessing the real risk of an attack on the smart grid remains difficult, says Raj Vaswani, chief technology officer of Silver Spring Network, a networking company focused on smart-metering systems. "Depending on which device they grabbed, it's very hard to say whether these were legitimate experiments or not," says Vaswani. "Nonetheless, we've done a fairly diligent job of taking this threat model into consideration. We've gone through a variety of third-party penetration testing, and we feel good about it."

Itron, one of the energy industry's largest vendors of smart-meter equipment, similarly claims that its products aren't implicated in the researchers' findings. The technology is currently undergoing security tests, however, by researchers at the Idaho National Laboratory, according to the company's vice president of marketing, Russell Vanos. "We're pretty confident," Vanos says. "Though we'll have a better sense when the Idaho labs show us their results."

Still, the power utilities' cybersecurity track record has been far from spotless. In 2007, Alan Paller, the director of the security-focused SANS Institute, told *Forbes* that hackers had extorted hundreds of millions from critical infrastructure companies in a string of incidents. In January 2008, a CIA official revealed at a cybersecurity conference in New Orleans that hackers had caused power outages in multiple foreign cities. And most recently, *The Wall Street Journal* reported that cyberspies seemingly based in China and Russia had penetrated the U.S. power grid.

Given that history of cyber vulnerabilities, IOActive's Pennell says it would be foolish to believe that the smart grid doesn't need cybersecurity regulation. "There's never been a utility system that could keep up with determined hackers," he says. "To assume that the smart grid would be different is a stretch."

Connecting smart meters to the grid may offer an even easier entry point for potential cyber attackers, says Goodspeed. "In general, it's probably a bad idea to put control of the large portion of the grid in a meter on the side of building within reach of anyone who wants to mess with it," he says. "It'd be pretty difficult to do that in a secure way." The more complex the power grid becomes, says Goodspeed, the more likely it is to be exploited. "It's one of the depressing things about security: To break something, you only have to look one step closer than the designer did," he says. "That's true from parking meters to power plants."