

CNET News

[InSecurity Complex](#)

April 9, 2010 4:00 AM PDT

Securing the smart grid

by [Elinor Mills](#)

86 retweet

Share 9

Smart meters are arriving at homes and causing a stir. Consumers in California and Texas have complained about higher bills due to smart meters **[not working properly](#)**. And for a second time in about a year, researchers **[discovered holes](#)** in the meters.

It's enough to make one wonder: are these devices going to become a security nightmare, allowing attackers to do everything from vandalize home area networks to cause power outages?

A smattering of utility representatives and experts in the field say consumers shouldn't panic, that security issues at this point are theoretical and the industry is working hard to resolve them.

"We're in a lot better shape than we were two years ago," said Ed Legge, spokesman for [The Edison Electric Institute](#), a trade group representing most of the U.S. electric utilities. "The industry as a whole has done a lot and we'll continue working to ensure reliability and that includes securing the system from cyberattacks."

The problem stems from the fact that two worlds are colliding. There's the universe of utility companies that use SCADA (Supervisory Control and Data Acquisition) systems for monitoring and controlling critical infrastructure, and then that of the Internet. Putting smart meters outside of homes that automatically report usage and performance measurements in real time will make the system more efficient and save money, but it also provides additional targets for attacks, experts say.

"The smart grid is by definition going to be less secure than the existing grid," said Andy Bochman, founder of the [Smart Grid Security Blog](#). "That's what happens when you greatly interconnect something that previously used isolation as one of its primary security strategies. It's going to be less secure and more people from more diverse backgrounds will be able to reach parts of it ... even if we do a great job of securing it with rock solid security technologies and policies."



A typical smart meter.

(Credit: Martin LaMonica/CNET)

But the picture isn't all that bleak, he said.

"The positive side is it's the smarts in the smart grid that can detect problems early and respond much more rapidly than the mechanical, human systems can today," Bochman said. "That will help us work around those isolated security incidents and ultimately make the grid more reliable and efficient than it is today."

Part of the problem is that there needs to be a shift in the mindset of typically slow-moving utilities, said Brian Monkman, technology programs manager at ICSA Labs, a testing and certification firm.

The utilities are used to designing and implementing technology that has a projected lifespan of 30 to 40 years, which is eons in Internet time, he said.

"We have power meters within the country that were installed at a house 60 to 70 years ago and it's still running," Monkman said. "The biggest fear is that the lessons learned over the course of the last 10 to 15 years on the Internet will not be carried over to the smart grid."

The industry had a wake-up call last year when IOActive released [a report](#) in March 2009 that concluded that multiple smart grid platforms were susceptible to common security vulnerabilities that affect computers and Web servers on a daily basis.

"In 2009, we saw a good rush to market, and at that point people came together and some vendors have made their meters pretty darn secure," said David Baker, director of services at [IOActive](#), an infrastructure security consultancy. "We've seen individual utilities working with vendors. They're really interested in fixing the security problems and they've come a long way."

The industry isn't waiting around to debate security. About 60 million smart meters will be deployed in the U.S. this year, covering about half of the households), according to figures from [The Edison Foundation's Institute for Electric Efficiency \(PDF\)](#). The action is being propelled at least in part by the \$3.4 billion in stimulus funds set aside for smart grid technologies.

Vendors are cashing in on the electric industry's move toward efficiency so fast that the devices aren't being built with security in mind, said Gary McGraw, chief technology officer at software security consulting firm [Cigital](#).

"Major vendors supplying these meters aren't thinking of them as something that needs to be hardened against attack in any way," he said. The utilities have to put pressure on the hardware manufacturers to improve the security in the appliances or face unwanted regulation, he added.

What about the meters that are already attached to homes--can they be fixed? For the most part, the devices can be upgraded with security enhancements later, according to IOActive's Baker.

"New meters are flashable and you can upgrade the firmware (fixed programs that control devices) remotely to provide new security features and more robust firmware, so in essence, you can provide a remote way to upgrade the software on it to make it more secure," he said. "That said, there are potential weaknesses that are a result of older hardware being already deployed

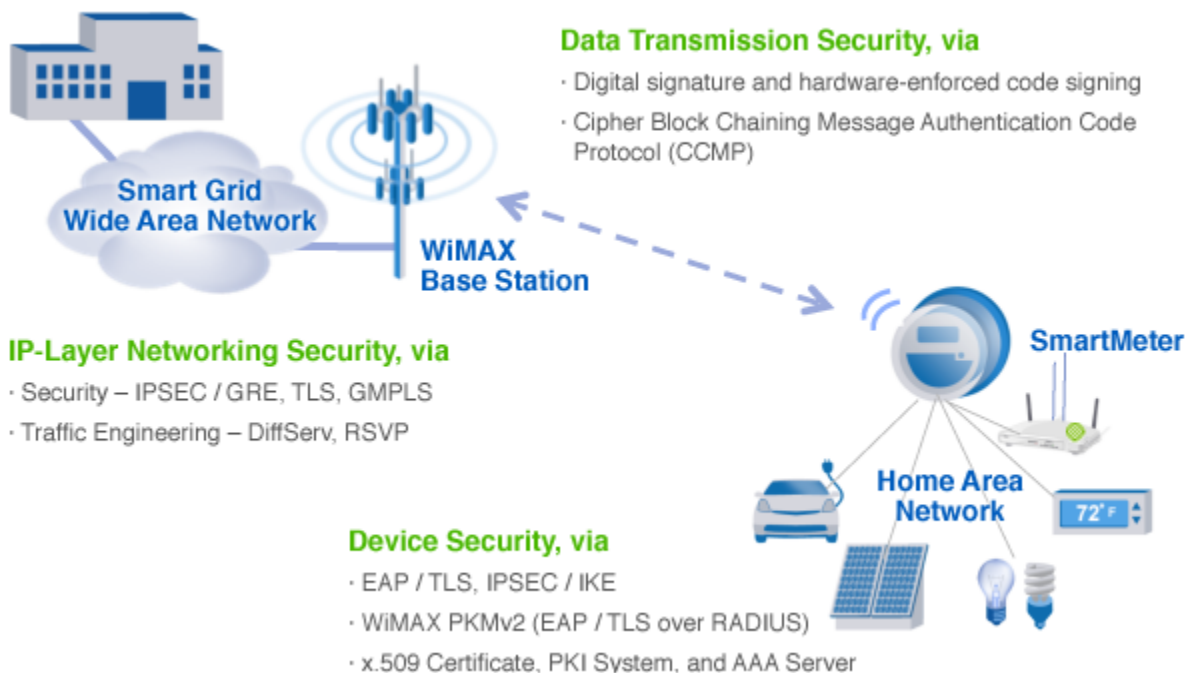
that have hardware weaknesses."

It's unclear what can be done to secure the older hardware other than swap it out, but that wouldn't happen for at least a decade, according to Joe Weiss, managing partner at [Applied Control Solutions](#), which offers consulting services to utilities.

Internet-utility mashup

One company that is jumping in with a solution is San Francisco-based [Grid Net](#). The company is applying encryption, authentication, and multilayer security technologies that are common in the Internet world to the smart grid platforms.

"Grid Net is proposing a different approach--embracing Internet Protocol for the utility infrastructure," said Andres Carvallo, chief strategy officer at Grid Net who helped build the first smart grid while working at Austin Energy, the ninth largest public power utility in the U.S. "The grid needs to reinvent itself and be distributed, interactive, and self-healing."



This graphic shows the technologies Grid Net uses to secure smart grid platforms.

(Credit: [Grid Net](#))

The company has two deployments in Australia, pilots with General Electric and Consumer's Energy in Michigan and American Electric Power, and is working with six other utilities in the U.S. that Carvallo said he could not disclose.

"Our software is embedded on smart meters, electrical vehicles or solar panels, inverters, transformers switches...any device within the utility infrastructure," he said.

Asked about the concern that the meters could be attacked and used to commit chaos in the grid much like botnets of compromised computers on the Internet are used to shut down Web sites, Carvallo said his company addresses that problem. "If there is a compromise on the endpoint it can only go as far as breaking down that one device," he said.

Utility industry veteran Weiss said Grid Net's approach could end up causing more problems than it solves.

"IT solutions and suppliers have caused multiple cases of shutting down control equipment and in at least one case have killed hardware. And the reason is they're trying to employ technology that works in the IT or enterprise environment that simply doesn't work in an industrial control environment," he said. "You have to understand the environment you're trying to apply it in. For example, penicillin is a great solution unless you have an allergy to penicillin."

In addition, the Internet technologies won't be able to help secure activity at the substations and control centers and power plants, where legacy equipment has vulnerabilities built in, Weiss said.

"We just had a situation occur this past year where a utility tried to meet the NERC (North American Electric Reliability Corp.) cybersecurity requirements to put in a security locking device," he said. "That device shut down the hard drives and all of the SCADA functions. That was the security device. Is something wrong with this picture?"

While the smart meters could conceivably be used to compromise other meters, it's highly unlikely they would offer an attacker an easy path to a control system at a utility company, said Brian Ahern, president and chief executive of security provider [Industrial Defender](#).

"Hackers have the potential to create nuisance attack scenarios that are focused on residential communities, but it's highly improbable...that it would find its way back to take control of the nation's bulk power system," he said.

Jesse Berst, managing director of the [Global Smart Energy](#) consultancy and founder of [Smart Grid News](#), said he didn't see any reason why the energy industry wouldn't be able to secure the infrastructure as it modernizes.

"The physical security concerns me more than the cyber security because we've solved the cyber (security issues) for other big consequential infrastructures (like financial and Internet) and I think we can solve it to that same degree of safety for this one," Berst said.

Experts agreed that it will take all parties working together to tackle the problem.

"This requires a cyber Manhattan Project," Weiss said. "The genie is out of the bottle. We just have to figure out how to do it in a more reasoned, knowledgeable way...There is no silver bullet."



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](#).