Editors: Patrick McDaniel, mcdaniel@cse.psu.edu
Sean W. Smith, sws@cs.dartmouth.edu

Security and Privacy Challenges in the Smart Grid

PATRICK MCDANIEL AND STEPHEN MCLAUGHLIN
Pennsylvania State University

Global electrical grids are verging on the largest technological transformation since the introduction of electricity into the home. The antiquated infrastructure that delivers power to our homes and businesses is being replaced with a collection of digital systems called the smart grid. This grid is the modernization of the existing electrical system that enhances customers' and utilities' ability to monitor, control, and predict energy use.

A central element of US energy policy, the smart grid is a way to reach national energy independence, control emissions, and combat global warming. The motivation for the smart grid at the local level is somewhat more prosaic: it lets home users actively manage (and presumably reduce) their energy use, thus allowing them to become better citizens and control utility costs. From an industrial perspective, the smart grid enables time-of-use pricing (a key measure for controlling usage and reducing ceiling capacity by charging higher fees during peak hours), better capacity and usage planning, and support for more malleable energy markets. Grid controls could also enhance energy transmission management and increase resilience to control-system failures and cyber or physical attacks.

The energy industry and government are placing enormous pressure on regional providers to deploy the smart grid. In the US, the recent economic stimulus package allocates US$4.5 billion for smart grid technology development, with the energy sector making additional investments of equally large proportions. Similar efforts are under way internationally, with the EU, Canada, and China launching broad initiatives in recent years. Organizations are releasing smart grid products on a near-daily basis, with new companies entering the market frequently. In short, the smart grid is going to happen, and it's going to happen soon.

Although deploying the smart grid has enormous social and technical benefits, several security and privacy concerns arise. Customers work closely with the utility to manage energy usage in the smart grid, requiring that they share more information about how they use energy and thus exposing them to privacy invasions. Moreover, because grid customers are connected over a vast network of computerized meters and infrastructure, they and the infrastructure itself become vulnerable to scalable network-borne attacks. Here, we look at several security and privacy issues resulting from this new infrastructure and identify initiatives that might help reduce exposure to these ill effects.

The Smart Grid

The smart grid is a network of computers and power infrastructures that monitor and manage energy usage. Each energy producer—for example, a regional electrical company—maintains operational centers that receive usage information from collector devices placed throughout the served area. In a typical configuration, a neighborhood contains a single collector device that will receive periodic updates from each customer in the neighborhood via a wireless mesh network. The collector device reports usage readings to the operational centers using a long-haul communication media such as a dial-up line or the Internet. The utilities manage transmission and perform billing based on these readings.

The usage-reporting device at each customer site is called a *smart meter*. It's a computerized replacement of the electrical meter attached to the exterior of many of our homes today. Each smart meter contains a processor, nonvolatile storage, and communication facilities. Although in many respects, the smart meter's look and function is the same as its unsophisticated predecessor, its additional features make it more useful. Smart meters can track usage as a function of time of day, disconnect a customer via software, or send out alarms in case of problems. The smart meter can also interface directly with "smart" appliances to control them—for example, turn down the air conditioner during peak periods.

One of the smart grid's most

attractive features is its ability to support widespread customer energy generation. For example, many farms now offset energy costs by producing electricity using methane generators, solar panels, and wind turbines. In the new smart grid, farmers can sell excess energy generated back to the utility, thereby reducing or eliminating energy costs. Obviously, this not only changes the electrical grid's economics but provides attractive incentives for customers to deploy (hopefully clean) power-generation technology. If widely adopted, this could substantially lower the provider generating capacity required to support the nation's needs.

Although the long-term vision for the smart grid involves global energy management and home area networks that can control smart appliances, current deployments evolve around the deployment of onsite smart meters. Currently, several million homes and businesses have upgraded to these new meters in the US alone, with an additional 40 million scheduled for deployment in the next three years.

The Billion-Dollar Bug

Smart meters are extremely attractive targets for malicious hackers, largely because vulnerabilities can easily be monetized. Hackers who compromise a meter can immediately manipulate their energy costs or fabricate generated energy meter readings. This kind of immediacy of return on the hacker investment has proven to be a great motivator in the past. Consider the early days of cable television, when signal hijacking kits were sold in huge volumes. Notably—even after 30 years of investment—cable theft continues to be a daunting problem for the entertainment industry.

Imagine a day when we could purchase smart meter "hack" kits from Internet vendors for $100 or less. Possibly by exploiting bugs in the exposed infrared port or mesh network protocols, this fictional tool would let users manipulate internal energy tables or send forged control messages to supported systems within a home or enterprise. History has shown that at least a small percentage of customers would purchase and use these tools. Once commoditized, each new major vulnerability would represent a "billion dollar bug" for the industry, whose costs would not only be measured in customer fraud but also in the costs of patching hundreds of millions of individual meters.

Consumer fraud in the electrical grid isn't new—current estimates indicate that as much as $6 billion is lost by providers to fraud in the US alone. Customers can turn a traditional physical meter upside down in the electrical socket to cause the internal usage counters to run backward (called *meter inversion*) or manipulate the physical contacts to impede the electrical flow calculation. However, the smart meter will change the nature (and likely volume) of customer fraud. Attacks move from crude (and dangerous) physical system manipulation to the remote penetration and control of complex, stateful computers. This enables more sophisticated attacks that could, for example, allow subtle changes to individual usage (which could be small enough to evade attention), falsely indict targeted victims, or launch large-scale attacks on the electrical grid.

This last attack bears further comment. As evident in other physical infrastructure domains, the computerization of the electrical grid enables remote attacks to scale—potentially reaching across continents. For example, researchers recently created a worm that spread between smart meters. This isn't surprising: meters are built on easily obtainable commodity hardware and software and will be subject to many or all of the maladies of Internet life. Meter bots, distributed denial-of-service attacks, usage loggers, smart meter rootkits, meter-based viruses, and other malware are almost certainly in these devices' future.

Widespread smart meter misuse could also have broader effects. Usage misinformation can seriously harm the electrical infrastruc-

ture when injected into control systems. Substantial fraud would mislead the utility into making incorrect decisions about local or regional usage and capacity and blind utilities to impending problems or ongoing attacks. It doesn't take much effort to imagine ways that nation states or terrorists would use such capability to mount massively damaging attacks on local or national critical infrastructure.

Privacy

Smart meters also have unintended consequences for customer privacy. Energy use information stored at the meter and distributed thereafter acts as an information-rich side channel, exposing customer habits and behaviors. Certain activities, such as watching television, have detectable power consumption signatures. History has shown that where financial or political incentives align, the techniques for mining behavioral data will evolve quickly to match the desires of those who would exploit that information.

Utility companies aren't the only sources of potential privacy abuse. The recently announced Google PowerMeter service, for instance, receives real-time usage statistics from installed smart meters. Customers subscribing to the service receive a customized Web page that visualizes local usage. Although Google has yet to announce the final privacy policy for this service, early versions leave the door open to the company using this information for commercial purposes, such as marketing individual or aggregate usage statistics to third parties.

Although services such as Google PowerMeter are opt-in, the customer has less control over the use of power information delivered to utility companies. Existing privacy laws in the US are in general a patchwork of regulations and guidelines. It's unclear how these or any laws apply to customer energy usage.

What Now?

A broad national effort is needed to investigate smart grid security and privacy. We can't wait to determine whether current laws and technology sufficiently protect users, utilities, and the nation's interests. Security and privacy failures in first-generation technology deployments of electronic voting and medical devices, for example, should act as cautionary tales here.

This national effort should pursue several objectives concurrently. The first is a regulatory one. Governments need to establish a national regimen of consumer protections. Such rules should be tantamount to a HIPAA (Health Insurance Portability and Accountability Act) for the grid, in which laws would identify the rules of the road for how customer data is collected, to whom it's exposed, and the consequences of information abuse, such as substantive penalties. Because these laws will help customers, utilities, and vendors assess risk, they could dramatically increase smart grid adoption.

Second, government, academia, and industry must more extensively evaluate the security of these devices both in the laboratory and in the field. Although initial system design investigations show that they're largely sound, we need substantially more independent investigation into the smart meter. Traditional security analysis methods, such as certification and internal quality assurance, are important but don't go far enough for critical systems. Industry and government must be creative in evaluating smart grid systems. National red-teaming competitions, open standards, independent source code review by security professionals and researchers, and the creation of publicly available testing laboratories could improve these systems' quality at minimal cost.

Finally, we must plan for failure. Complex software systems such as these are by nature going to have exploitable bugs. The utility industry must work with the vendor community to develop comprehensive recovery strategies. These plans must enable software patching or the rapid identification and isolation of compromised systems. To wait for the first major exploit to establish a recovery plan is to invite an otherwise avoidable disaster.

Moving to a smarter electrical grid is imperative not only for the nation but also for the planet. However, we must be realistic about the risks and anticipate and mitigate the security and privacy problems they introduce. In moving to the smart grid, we replace a physical infrastructure with a digital one. A similar transition in other infrastructures hasn't always been easy, and we must expect that some problems will occur. How we deal with these problems will make the difference between a smooth transition to a less costly and more environmentally sound future, or the lights going out. □

Patrick McDaniel *is an associate professor in the Department of Computer Science and Engineering at Pennsylvania State University, and is also partnering with Lockheed Martin to analyze smart grid technology. His research interests include network and systems security, telecommunications, and policy. McDaniel has a PhD in computer science from the University of Michigan. He is a member of the ACM, the IEEE, and Usenix. Contact him at mcdaniel@cse.psu.edu.*

Stephen McLaughlin *is a graduate student in the Department of Computer Science and Engineering at Pennsylvania State University. His research interests include storage security, SCADA security, and security analysis of critical infrastructure. McLaughlin has a BS in computer science from Pennsylvania State University. Contact him at smclaugh@cse.psu.edu.*