CYBER SECURITY: PROTECTING THE GRID IN THE DIGITAL AGE

THE STORY IN BRIEF

Electric utilities are as vulnerable to cyber attacks as other businesses, but the critical importance of the nation's power infrastructure and the move to a highly interconnected smart grid make cyber security of particular concern for the power industry.

Cyber security isn't just a headache for information technology experts in a small part of a utility's operation anymore. Concerns about the security of the nation's critical infrastructure shot up after the September 11 terrorist attacks and raised awareness that many utility systems needed to increase their security controls.

Likewise, connectivity is not just a buzzword in the world of iPad and Facebook. It also describes a massive undertaking by utilities in the smart grid universe, where new technologies are digitizing the control of power generation and delivery and potentially linking this control to home networks of appliances. And just as all parts of the grid management are increasingly connected and increasingly digital, they need to address potential cyber security attacks.

Worries about cyber security for the grid have only deepened with the deployment of smart meters and other equipment that brings onto the grid a much wider array of technology, software, communications, and integration to make possible communication and control for utilities to manage power supply and demand. Companies are equally concerned about how to address cyber security for older legacy systems and equipment.

All this combines for a big challenge: how do you armor these emerging networks and their millions of components and systems to detect and mitigate security threats?

A Primal Worry—Loss of Control

The emergence of Stuxnet, a very advanced program that can disrupt control systems while hiding its presence, highlighted the need for guidelines and tools to prevent service interruption of critical systems. Hackers have clearly demonstrated that Stuxnet can be used to reprogram equipment functions, with the best-known attack crippling a uranium enrichment operation in Iran.

"People used to think nobody would go after a control system, and Stuxnet woke up a lot of people," said Annabelle Lee, an EPRI technical executive for industry cyber security. "The policy of the United States is to support the modernization of electricity transmission and distribution, which means an increase in the use of digital controls. When it's digital, you have to worry about cyber security."

The control system isn't the only vulnerable spot in a utility's operation. Cyber security attacks can be launched against the electricity infrastructure at many points along the path, from power generation to substations to the final destination of the distribution—the homes. A weak link in the chain could invite security breaches that might impact the entire network.

"It's like having all of your house locked except for one window," said Neil Greenfield, senior cyber security architect and the cyber security technical team lead for gridSmart at American Electric Power. "If you forget to lock that window, then you open the whole house up to risks."

From Legacy Systems to Smart New Technology

Keeping intruders away isn't the only goal for utilities. Power plant operators must demonstrate their compliance with the North American Electric Reliability Corporation's physical and cyber security standards for generation and transmission, said Galen Rasche, an EPRI technical executive for industry cyber security.

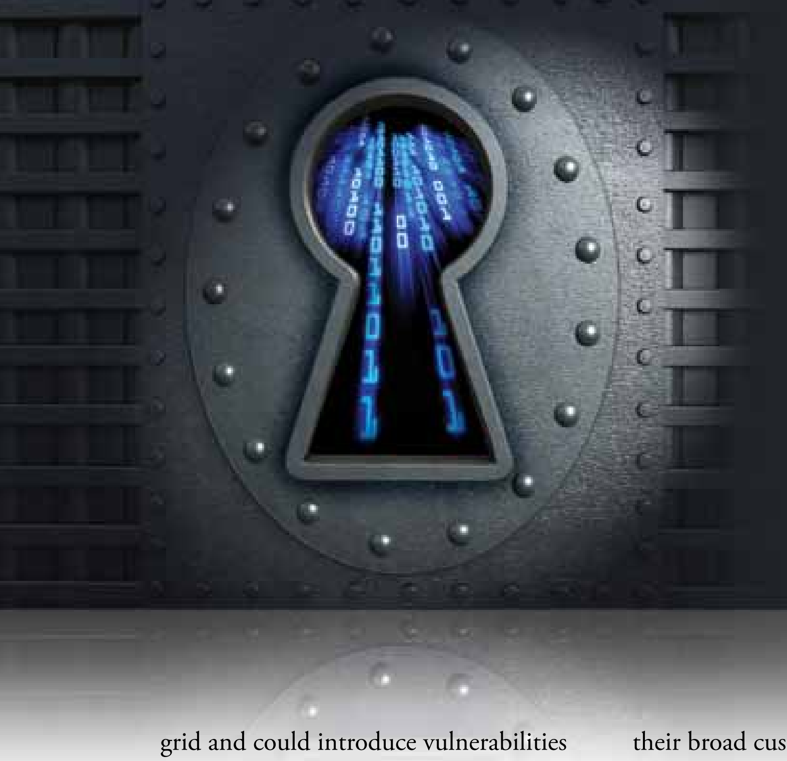
Rasche and Lee joined EPRI this past year to spearhead cyber security research and development efforts across all segments of the utility industry. They launched the Cyber Security and Privacy Initiative earlier this year to identify key challenges and technology gaps and to develop guidance and tools to help utilities draft their own cyber security strategies and mitigate risks. The work will address challenges for managing legacy systems and incorporating smart grid technologies. Through collaborations with industry and government groups, EPRI plans to start a permanent research and development program for cyber security in 2012.

"We will be developing testing methodologies that utilities can use to look for vulnerabilities or to make sure equipment is configured properly before it is put in the field," Rasche said.

From Consumers to Power—Providing for a Common Defense

In many people's minds, *cyber security* refers to the protection of information technology systems, such as utility data collection and billing operations. The rollout of smart meters and communication gateways is modernizing these portions of a utility's overall operation. Smart meters are also enabling utilities to detect service interruptions and troubleshoot other problems much more quickly than before. As the role of communications and information technology in managing supply and demand is evolving, so are the cyber security risks.

Smart meters contain communication chips for sending and receiving data. This bi-directional flow of communication and control increases the complexity of the



The policy of the United States is to support the modernization of electricity transmission and distribution, which means an increase in the use of digital controls. When it's digital, you have to worry about cyber security.

grid and could introduce vulnerabilities and increase the exposure to potential attackers and unintentional errors. Each smart meter is, in effect, an entry point for potential adversaries to exploit and must be protected.

Meanwhile, as smart meters and other communication equipment are developed, technology companies have embraced different communications protocols and jockeyed to set industry standards.

Several communications protocols, such as WiMAX and cellular, have emerged as popular choices, largely because equipment vendors are promoting hardware with open standards. Using standard protocols saves money, enables diverse pieces of equipment to "talk" to each other, and makes scale-up easier. This increased level of interconnectivity opens the door for security incidents, however, because it can introduce common vulnerabilities.

But the benefits of using open standards outweigh the disadvantages. Lee points out that a primary focus of information technology experts is protecting the confidentiality and integrity of the data. In this context, using standard protocols does have advantages. Widely used protocols invite more aggressive security monitoring and improvement by hardware and software vendors, which have a deep financial interest in keeping their broad customer base happy. A breach in one utility's network can lead to security fixes that immunize not only its own system but also other utilities' systems that use the same communications standards.

Using open communications technologies is crucial for creating a smarter grid, which is supposed to facilitate expedient communication about energy consumption, equipment failures, and power supply and demand management among various stakeholders, including utilities, grid operators, and consumers. If utility networks in the same regional grid speak different languages, not only will they have trouble communicating with each other, but they will also likely find it difficult to work together on building up a strong defense against cyber attacks.

"As we move forward with modernizing the grid, we want these systems to interconnect. If operators of a wind farm in Nevada want to transmit electricity to Southern California, the only way they can do that is by using a standard communications protocol," Lee said.

The push for smart grid deployment also leads to growing interconnectivity in the power generation and transmission systems. That could make key equipment such as supervisory control and data acquisition (SCADA) systems more vulnerable.

Crafting and deploying a cyber security strategy at a power plant will have to align with priorities that are different from those for information technology networks. Lee noted that for control systems, availability and integrity are the most important objectives, not confidentiality. In fact, the need to keep the power plant running with minimal interruptions often makes it difficult for utilities to update security measures.

EPRI Launches Cyber Security Initiative

EPRI's cyber security initiative will address security challenges associated with both legacy systems and deployment of new technology, such as the smart grid. It is important that cyber security specifications be built into the smart grid and next-generation equipment and systems as they are developed, rather than added on after the fact. Legacy systems are largely analog technologies that were not designed with good—if any—security measures in place. Many of these legacy systems do not have a strong defense in place because they were built at a time when securing them against intrusion was not a priority. Large components—generators and transformers, in particular—are meant to run for several decades and are operated largely with proprietary communications protocols. Using proprietary protocols helps to shield the equipment from cyber attacks, because hackers cannot easily find the necessary

Uncle Sam Brings Guidance and Support for Cyber Security

The U.S. Department of Homeland Security has developed guidelines for protecting critical infrastructures, including the energy sector. In addition, the National Institute of Standards and Technology last September issued Interagency Report 7628, Guidelines for Smart Grid Cyber Security.

In 2009, the U.S. Department of Energy announced the largest-ever single investment for electricity grid modernization by awarding grants totaling $3.4 billion to 100 smart grid projects. Many of the projects involved installing smart meters and building out communication networks for power transmission, distribution, and other electricity grid monitoring and control systems. Among the funding criteria were some that Lee and others helped DOE develop: requirements for cyber security. The importance that DOE places on this issue is reflected in the fact that it rejected one proposal that was good in every category except cyber security.

codes to create a virus and install it on the legacy equipment. The smart grid buildout will gradually connect these legacy systems to newer digital equipment that runs on open communications standards. These interconnections will expose legacy systems to cyber security threats. As a result, utilities need a road map to incorporate effective cyber security practices as they gradually upgrade various segments of their networks.

"Protecting legacy systems is a big issue for our members," Rasche said. "These systems typically don't have the computational capabilities or the bandwidth to support security updates."

Understanding the sources of potential threats is critical. Cyber incidents will not always be malicious or come from outside sources, Rasche said. Security breaches could result from employees who lack the training to handle sensitive data or who accidentally key in wrong commands. Disgruntled employees, because they may have ready access to proprietary information and control systems, pose a more serious threat than do hackers from the outside. One way to prevent internal missteps is to clearly delineate authentication procedures. And utilities must have processes in place to respond to security breaches that result not just from human actions but also from equipment failures or natural disasters.

"Once systems are interconnected, you could potentially have a failure that would impact more than a regional grid," Lee said. "The northeast blackout of 2003 is a good example."

EPRI's cyber security initiative will help assess security needs and risks and provide incident analyses and action plans for procuring and deploying solutions. The new set of tools will also allow utilities to quickly respond to cyber security threats. EPRI plans to provide a framework for installing an intrusion detection system for advanced metering infrastructure (AMI) networks. The framework will provide guidance on, among other things, where to place sensors on a communication network and how to set standards for alerts and alarms from different vendors. EPRI will also offer tools and techniques for testing the defense of a network that incorporates gadgets and smart appliances in homes. Nuclear power plant operators face unique safety challenges. EPRI is working on a system procurement guideline this year that will include cyber security requirements.

The new EPRI tools will help utilities tackle the daunting challenge of formulating a cyber security strategy, something that many utilities have not considered to be a priority. Changing this mind-set will be a crucial starting point. Another first step in crafting a cyber security strategy will be to take stock of what protective measures are already in place and what existing cyber security requirements and best practices from federal regulators and industry groups should be used. For example, the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), cosponsored by the Department of Energy, has been developing security profiles for various smart grid applications. The EPRI initiative is also supporting this effort and will build on these profiles.

"Security is like insurance. There is no return on your investment until something happens," Greenfield said. "But if you don't take into account the risks, then you might run into issues in the future."

This article was written by Ucilia Wang. Background information was provided by Galen Rasche, grasche@epri.com, 650.855.8779, and Annabelle Lee, alee@epri.com, 202.293.6345.

Galen Rasche, a technical executive in the R&D Group's Senior VP Office, coordinates cyber security research across the Power Delivery and Utilization, Generation, and Nuclear sectors. Before joining EPRI in 2010, he worked at the Southwest Research Institute and at the Center for the Commercialization of Electric Technology. Rasche received B.S.E.E. and M.B.A. degrees from the University of Kentucky and an M.S. in electrical engineering from the University of Illinois at Urbana-Champaign.

Annabelle Lee is a technical executive in the Power Delivery and Utilization Sector. Before joining EPRI earlier this year, she spent 15 years as a senior cyber security strategist at the National Institute of Standards and Technology (NIST), where she established and led the Smart Grid Cyber Security Working Group. While at NIST, she was detailed to the Department of Homeland Security for four years to direct programs in its National Cyber Security Division. Lee holds a B.A. in psychology from Stanford University and an M.A. in educational psychology from Michigan State University.