renewGRID™ Reprinted with permission from the October 2009 issue

Hunkering Down To Specify Smart Grid Security Standards

Implementation of the smart grid increases the potential for cyber attacks, necessitating collaboration on new standards.

By Dan Burton

As the U.S. power industry moves toward a smart grid network of interconnected electrical utilities, service companies, producers and consumers, the frequency of attempted cyber attacks is expected to increase.

In turn, a massive effort is under way to define smart grid cybersecurity standards to detect and mitigate these attacks. The National Institute of Standards and Technology (NIST) is coordinating with industry experts and stakeholders to develop these standards, which will eventually drive cybersecurity regulations for entities communicating on the smart grid.

Traditional utility data networks have inherent security advantages in that they are typically proprietary, utility-specific networks that are not connected to any public networks. According to Dr. Erfan Ibrahim, technical executive and smart grid communications and cybersecurity lead at the Electric Power Research Institute (EPRI), "Each utility has its own trust domain. Within their trust domain, they have their own vendor-specific protocol to do command and control and data collection."

Erfan Ibrahim

He points out that these isolated trust domains, with their physical and logical isolation from the public network, have made it relatively difficult for an outsider to hack into a system.

However, even with the traditional security-by-obscurity barrier, the current grid is still under constant attack. LogLogic, a company focused on log, compliance and security management, recently completed a survey of utility information security professionals and published its findings. The survey found that over half of the utilities are experiencing more than 150 attacks per week, occurring on isolated, single trust-domain systems.

While the isolation of traditional utility information systems provides some advantage in keeping cyber attacks at bay, a major disadvantage has been that utilities cannot communicate with one another without tremendous amounts of custom integration. With the advent of an interconnected smart grid, all the entities that are supplying electricity to the grid will be able to communicate over a common network.

But the main challenge of this new smart grid network, states Ibrahim, is that "there is more potential for attacks because of the presence of multiple trust domains that need to exchange data."

Seth Bromberger, manager of information security at northern California utility Pacific Gas and Electric (PG&E), concurs with Ibrahim. "From an interconnectedness point of view, the primary challenge we face is the fact that we now have to manage and protect millions of endpoint devices that are outside of our physical control."

Seth Bromberger

These millions of endpoint devices can have their own vulnerabilities. IOActive, a computer security services company, recently demonstrated vulnerabilities in various smart meters that they had obtained and tested.

David Baker, director of services at IOActive, explains that the company has been able to demonstrate in a proof of concept that it could change the code on a smart meter, use wireless transmission to communicate with neighboring meters, copy the meters' firmware and reflash itself with the attached firmware. The model showed that this malicious self-propagation could spread to over 20,000 meters in a 24-hour period.

David Baker

But the cybersecurity challenges extend beyond smart meters.

Applying digital technology to the entire grid will increase the amount of accessible, real-time information flowing among parties.

"The more access you want, the more difficult it is to secure," says Ameen Hamdon, president and founder of SUBNET Solutions. "With the smart grid, the challenge is, how can we increase access while also increasing security?"

Ameed Hamdon

SUBNET Solutions approaches this security challenge by working with utilities to unify the communications between field devices and business systems to address the specific needs of the substations and the grid. Through this unification, security "islands" can be created around various systems in the substation.

Physical device standards for cybersecurity will be a major focus in implementation of the smart grid.

Ken Van Meter

In contrast to the PC industry, with its plug-and-play computers and peripherals, there are only emerging smart grid standards governing meters, mesh networks, re-closers and encryption devices.

Ken Van Meter, a principal in Lockheed Martin's Enterprise Integration Group, points out some good news: Security is managed in the interfaces more than in the devices, so designers will still be able to provide end-to-end system security by understanding, controlling and manipulating those interfaces. Still, he says, "The faster we can all agree on those standards and align to them, the better - from a security standpoint."

Standards in development

NIST's "Smart Grid Standards Interoperability Roadmap" project was launched in April 2008 to carry out its federal mandate from the Energy Independence and Security Act of 2007 to "coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."

The NIST cybersecurity standards will define the minimum functionality necessary to protect the grid against known threats. Stakeholders all along the smart grid supply chain will see regulations requiring them to design their systems to meet or exceed those standards.

EPRI has worked side by side with NIST over the past several months to define the requirements for the standards. Throughout the effort, they have placed a high priority on developing consensus among industry stakeholders in defining these requirements.

For the first phase of the project, which was completed this August, NIST and EPRI created forums in which they brought industry stakeholders together, outlined the charter and facilitated open discussions. The presumption is that collaboration will result in very thorough definitions. Also, when the regulatory compliance mandate does take effect, all stakeholders will be aware of it and already be developing plans to meet it.

The development of cybersecurity standards is a balancing act between two competing forces. One force calls for the sharing of information with as many parties as possible to allow businesses to operate. Another force contends that the more parties involved in any interaction, the more security threats created.

"It's not one side or the other, because each one would stifle business," Ibrahim says. "If you opened it so much that you were constantly having hacks, you would have unavailable applications, and the businesses would fail. If you constrict it to the point where people have to jump through many, many hoops, then you would have the same challenge again. People would get turned off and not do business."

In order to identify the risks and determine security requirements (while striking that essential balance), NIST, EPRI and various stakeholders identified and studied hundreds of smart grid use cases. They determined the interfaces on which data exchanges were occurring and pinpointed a preliminary set of cybersecurity requirements for data sharing at those interfaces.

For example, an independent power producer (IPP) will need to communicate to buyers the quantity of electricity it is providing at any given time. The IPP will need some type of metering at that interface in order to bill the distribution company for the power it has sold.

The preceding reflects a multilayer transaction that includes all seven communication layers of the Open Systems Interconnection Reference Model (OSI Model) and a semantic layer, at layer eight, that keeps track of the actual data exchanged between the entities. This is a typical use case, where the actors are the IPP and the distribution company, and the interface is the physical and logical connection between them.

Value of experience

Fortunately, coming up with the requirements has not meant starting from zero. There are many similarities between the use cases of the smart grid and those of other industries that have already tackled cybersecurity risks.

PG&E's Bromberger says the massive size of the grid does pose significant security challenges with respect to authentication, authorization, confidentiality and integrity - such as ensuring that devices that are communicating within the smart

grid network are allowed to do so, and ensuring that the interactions among smart grid components are limited to essential communications required for the proper operation of the devices.

"There is a wealth of experience in these areas that can be brought to bear on the specific smart grid implementations," Bromberger remarks.

Augmenting this wealth of information-security experience is a very large existing base of commercial products. Dominique Levin, executive vice president of marketing and strategy for LogLogic, points out that product technology used in other systems already exists and will help information-security professionals protect smart grid infrastructure.

"Our technology, as with many of these security technologies, has already dealt with so many industries that the technology itself is very flexible," Levin says.

Dominique Levin

Moreover, as the technology embedded in utility equipment changes, cybersecurity software will need to change in step with it. "There will be a need to support new equipment over an extended life cycle, just as today we support equipment that is 20 years old," says Bryan Owen, cybersecurity manager at OSISoft.

Lockheed Martin, through its recently announced partnering with Black and Veatch, intends to apply its cybersecurity experience to the nation's energy infrastructure. For example, the company frequently works with government agencies and contractors, which regularly share threat and mitigation information among their networks. As utilities move to an advanced metering infrastructure architecture with large-scale secure communications, this kind of experience can be valuable.

Bryan Owen

Additionally, Lockheed Martin has existing tools that have been developed for other applications - like GPS and the Hubble space telescope - and can allow utilities to model, design and protect complex systems. The "situational awareness" garnered from these existing products can enable utilities to share information with stakeholders such as government regulatory agencies.

"It's an advanced form of program management," says Van Meter. "They can have secure, compartmentalized, appropriately packaged information presented to them in a variety of ways."

A systemic view

An overarching principle in developing protection against cyber attacks is that all stakeholders need to view the smart grid as a system. Doing so can help reduce the vulnerability inherent in device-centric designs.

"Think global, but act local," says Ibrahim. Such a systemic view must be pervasive in designing equipment and securing smart grid data. If vendor products include device-centric security features that are not scalable, there will likely be gaps, which hackers exploit. A systemic approach helps close those gaps.

Because the smart grid is such a huge undertaking, most of the associated initiatives will require the continued collaboration of multiple vendors.

"From the security perspective, there is probably nothing more important," says OSISoft's Owen. "One thing we've learned is that the bad guys will work together. As the good guys, we really have to work together to stay ahead of them."

Keeping a systemic view also creates the benefit of transparency. This transparency, in turn, allows third-party security and management tools to be used over the whole fabric of the system. And because there are so many eyes from third parties on the system, holes can be identified and plugged before catastrophic cybersecurity breaches occur.

Dan Burton is a freelance writer based in California.