Editors: John Steven, jsteven@cigital.com
Gunnar Peterson, gunnar@arctecgroup.net
Deborah A. Frincke, deborah.frincke@pnl.gov

Smart-Grid Security Issues

HIMANSHU KHURANA
University of Illinois at Urbana-Champaign

MARK HADLEY, NING LU, AND DEBORAH A. FRINCKE
Pacific Northwest National Laboratory

The North American electric power grid is a highly interconnected system, considered by many as one of the 20th century's greatest engineering feats. Still, changing power supply and demand are motivating changes in this system; this ongoing modernization is often called the "smart grid." This process has many drivers, such as reliability and efficiency, and many potential benefits—for example, minimizing climate impact by making it easier to incorporate renewable energy sources such as geothermal and wind power, and increased consumer participation.

However, these improvements will incur increased risk. Some risk will be tied to tighter incorporation of the digital-communications and computer infrastructure with the existing physical infrastructure, with all the inherent vulnerabilities. Other risk comes from changes in how power companies and consumers interact. Here we describe some looming changes and highlight security issues related to the infrastructure's digital element.

A Look at Smart Grids

The smart grid (see Figure 1) uses intelligent transmission and distribution networks to deliver electricity. This approach aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning.

The smart grid incorporates many resources, applications, and enabling technologies. Resources are the devices that affect supply, load, or grid conditions, including delivery infrastructure, information networks, end-use systems, and related distributed energy resources. Applications are operational strategies that use resources to create benefits or value. Enabling technologies include essential, crosscutting elements of the smart grid that facilitate many resources and applications, including smart meters, standards, and protocols.

The smart grid is poised to transform a centralized, producer-controlled network to a decentralized, consumer-interactive network that's supported by fine-grained monitoring. For example, consumers react to price signals (that is, supply) with the help of smart meters to achieve active load management. On the monitoring side, old metering data recorded hourly or monthly is replaced by a smart meter that collects data every minute. Similarly, current supervisory control and data acquisition (SCADA) systems collect one data point every 1 to 2 seconds, whereas phasor measurement units (PMUs) collect 30 to 60 data points per second.

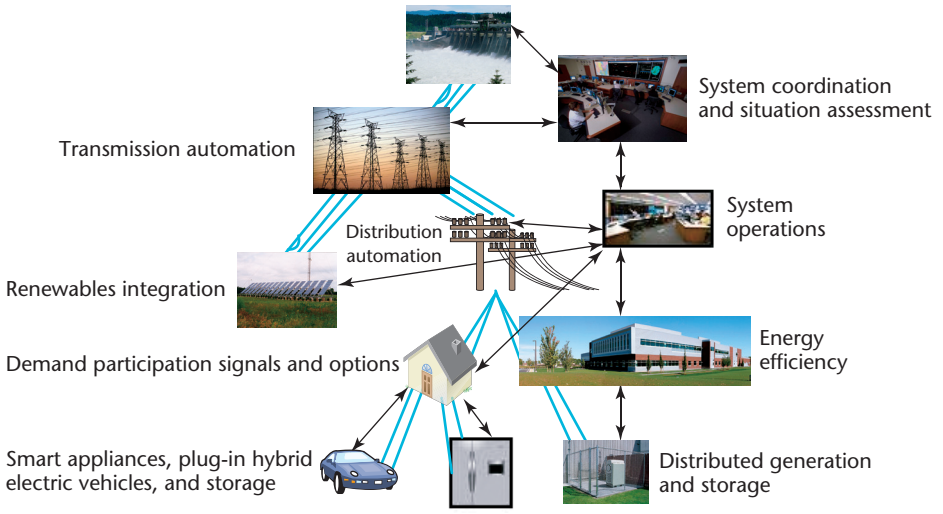

Figure 1. The smart grid's physical layers and communication and control systems. Smart-grid data availability places considerably more stringent demands on the communication and control system than traditional supervisory control and data acquisition (SCADA) systems do.

The PMU in the power transmission grid and the advanced metering infrastructure (AMI) in the power distribution system will provide the power grid an "MRI," compared to the "x-ray" available from SCADA technology. In addition, smart-building and home-automation technology extends control and monitoring to the end-user level. Thus, widely used digital control and communication technologies provide operators unprecedentedly abundant information and inform them of the status of the multitude of devices connected to the power grid, such as generators, breakers, and home appliances.

Smart-grid technology features distributed control and monitoring technologies that extend control to consumer equipment such as distributed generators and office and home appliances. Control and monitoring signals travel via different media networks to many end-use devices with various vulnerabilities. Serious concerns have been raised about whether the smart grid can resist attacks and heal itself without causing infrastructure and equipment damage or large-scale blackouts. The massive use of low-cost communication and electronics provides an explosion of information that bears different data formats and time stamps, with or without secured information interchange mechanisms.

Through digital and information technology, the smart grid allows close interaction and interoperation of the transmission and distribution grid, building and house controllers, and distribution generation. This increases the possibility of cyberattacks and cascade failures propagating from one system to another. Consequences include power system blackouts, smart-grid IT infrastructure failures, energy market chaos, damaged consumer devices, endangered human safety, and less severe but more frequent incidents such as smaller-scale outages. As the grid matures, it will be important to devise a defense supervisory system that can efficiently process myriads of data to evaluate system status, identify failures, predict threats, and suggest remediations.

Grid Security Challenges

The smart grid will require developing and deploying extensive computer and communication infrastructure that supports significantly increased situational awareness and allows finer-grained command and control. This is necessary to support major applications and systems such as demand-response wide-area measurement and control, electricity storage and transportation, and distribution automation.

Any complex system has vulnerabilities and challenges, and the smart grid is no exception. Numerous challenges will arise with the integration of cyber and physical systems, along with such factors as human behavior, commercial interests, regulatory policy, and even political elements. Some challenges will be quite similar to those of traditional networks, but involving more complex interactions. We consider four areas in this section.

Trust

For control systems, we define trust as our confidence that, during some specific interval,

- the appropriate user is accessing accurate data created by the right device at the expected location at the proper time, communicated using the expected protocol, and
- the data hasn't been modified.

Many people view the grid's control systems as operating in an environment of implicit trust, which has influenced design decisions. If some participants aren't trustworthy, new methods of addressing this beyond existing monitoring approaches might be required.

Communication and Device Security

Traditional electric-grid communications have relied predominantly on serial communication environments to provide monitoring and control. Serial communication is reliable, is predictable, and, owing to the nature of the communications protocols, provides some containment. However, increasing numbers of

smart-grid deployments are using Internet technologies, broadband communication, and nondeterministic communication environments. This issue is compounded by the rapid deployment of smart-grid systems without adequate security and reliability planning. For example, whereas traditionally communications involved devices that were in areas with physical access controls (such as fences and locked buildings), two-way meters being deployed now are accessible by consumers and adversaries. Consequently, we must consider automatic meter reading (AMR) environments hostile in such cases.

Privacy

Historically, the electric grid's security objectives have been availability, integrity, and confidentiality. However, as the grid incorporates smart metering and load management, user and corporate privacy is increasingly becoming an issue. Electricity use patterns could lead to disclosure of not only how much energy customers use but also when they're at home, at work, or traveling. When at home, it might even be possible to deduce information about specific activities (for example, sleeping versus watching television). It might also be possible to discover what types of appliances and devices are present by compromising either the customer's home area network or the AMR network. Also, increases in power draw might suggest changes in business operations. Such energy-related information could support criminal targeting of homes or provide business intelligence to competitors. Further research is needed in mitigating such threats.

Security Management: Issues in Complexity and Scale

The complexity and scale of future power systems that incorporate smart-grid concepts will introduce many security challenges. Currently, a large utility communicates with thousands of devices to manage the electrical grid. Both the volume of data and the number of devices with which a utility communicates will likely increase by several orders of magnitude. With these larger networks, routine maintenance, managing trust, and monitoring for cyberintrusion become challenges.

One particular issue is cryptographic-key management. Current practice for smart meters utilizes an X.509 certificate for device identification and cryptographic-session establishment. However, a certificate's cryptographic keys are static for each device—in essence, providing a key lifetime equivalent to the meter's useful life (5 to 15 years). Cryptographic solutions in this context should include a key management solution to periodically update keys, or at least to revoke them.

Consider an organization with a public-key infrastructure (PKI) system used to provide X.509 certificates to employees. It will need support staff to maintain the PKI servers, address user software issues, maintain the network infrastructure, and develop and implement policy-and-practices documents. Laboratory operational experience shows that one support staff is required for approximately 1,000 user certificates. Consider a utility with 5.5 million smart meters. If similar ratios apply to smart-meter certificates, maintaining the PKI environment would require 500 staff! No utility can support this requirement.

Other concerns are the time and processing required to update cryptographic keys. Devices currently planned for monitoring and controlling the smart grid might not have the processor cycles and memory to adequately support fast and high-volume cryptographic computations. Table 1 provides the time requirements for various processors to perform cryptographic functions using the OpenSSL FIPS (Federal Information Processing Standards) Crypto Module 1.1.1 compiled against the 0.9.7m OpenSSL library.

Table 1. The time required for various processors to perform cryptographic functions using the OpenSSL FIPS (Federal Information Processing Standards) Crypto Module 1.1.1 compiled against the 0.9.7m OpenSSL library.

Platform	Parameter generation time (sec.)	Public/private-key generation time (sec.)
Transmeta Crusoe TM5800 731 MHz 240 Mbytes of RAM Microsoft Windows XP SP2	227.75	0.0300
Intel Pentium 4 2.80 GHz 480 Mbytes of RAM Microsoft Windows XP SP 2	50.64	0.0154
2x Intel Xeon 3.0 GHz 1.0 Gbytes of RAM Microsoft Windows Server 2003 SP1	46.80	0.0188
Intel Pentium M 2.13 GHz 2.00 Gbytes of RAM Microsoft Windows XP SP2	39.83	0.0032

The parameter-generation time includes processes to ensure the parameters meet randomness requirements. In the example of a utility with 5.5 million smart meters, manually updating each device once a year would require processing an average of 10 key pairs every minute. Current technology doesn't support these requirements and presents another smart-grid challenge. Alternate designs are needed; for instance, involving back-end servers for key generation would allow for batch generation of keys by higher-end computational modes.

Architecture-Based Requirements and Solutions

Here, we look at solutions to smart-grid vulnerabilities from an architectural perspective, focusing on authentication and encryption.

The grid's physical and cyberinfrastructure layers comprise generation, transmission, and distribution systems. These layers are hierarchical in nature. For example, in transmission systems, SCADA components enable balancing authorities (BAs) to exchange command and data information with substations for sensing and actuation of grid parameters. At higher layers, BAs communicate regularly with reliability coordinators (RCs), and entities engage in market transactions with independent system operators (ISOs).

Whereas the physical and cyberinfrastructure layers are hierarchical, the time frame granularity for operations varies depending on the kind of activity involved. For example, protection and control mechanisms at substations operate at the granularity of milliseconds. State estimators and contingency analyses in BAs and RCs operate at the granularity of minutes. Hourly and day-ahead power markets run by RCs operate at the granularity of hours and days, respectively.

On the distribution side, the cyberinfrastructure is less structured than on the transmission side. However, ongoing changes such as AMR are resulting in increased use of cyberinfrastructure systems in homes, neighborhoods, field networks, and utility networks.

Requirements for Effective Cybersecurity Solutions

R&D of effective cybersecurity tools and technologies requires understanding current and emerging smart-grid architecture, particularly its constraints and opportunities. Solutions must reflect several key priorities.

First, among the traditional cybersecurity properties of confidentiality, integrity, and availability, availability usually gets highest priority when it comes to power. This is largely because the cyberinfrastructure manages continuous power flow in the physical infrastructure and must therefore have high availability. Making sure power is available when needed is more important to most users than making sure that information about power flows is confidential.

Second, developers must consider efficiency and scalability. Depending on where the solution will be employed, the grid has varying real-time requirements that make efficiency essential. Common use of constrained devices and networks add to this need. At the same time, scale is important regarding the number of devices and the increasing number of interactions between grid entities.

Third, developers must include adaptability and evolvability. Devices tend to last decades and can sometime outlast cryptographic tools' lifetimes. So, designs must allow for adaptations and evolution.

Finally, the grid's extensive, controlled, and monitored infrastructure offers potential benefits and opportunities for designing effective cybersecurity solutions. Such benefits include structured protocols and message exchanges, formally specified power flows, presence of trusted third parties, and inherent redundancy for contingencies.

As with any large-scale system, these properties are only guidelines. Solutions to specific problems should carefully consider the relevant architectural constraints and opportunities. This is especially true regarding the grid's ongoing modernization.

Recent Authentication and Encryption Solutions

Here, we focus on solutions involving transmission substations, constrained SCADA networks, policy-based data sharing, and attestation for constrained smart meters.

Transmission substations. Authentication technologies for transmission substation networks face short, strict real-time constraints. In certain cases, multicast messages must be delivered in less than 4 milliseconds. Addressing this challenge requires not only efficient authentication algorithms to minimize computational cost but also avoidance of buffering packets so that presented data can be processed immediately. Multicast authentication schemes should also have small communication overhead, packet-loss tolerance, and resistance against malicious attacks.

By leveraging one-time-signature and one-way hash chain cryptographic constructs, Qiyan Wang and his colleagues have developed such an authentication solution.[1] Their solution provides fast signing and verification and buffering-free data processing.

Constrained SCADA networks. Patrick Tsang and Sean Smith have developed a similar, "bump in the wire" solution for authentication for legacy SCADA devices.[2] They first apply Hash-Based Message Authentication Code to byte streams with minimal buffering. They then convert the ran-

dom-error detection available on legacy systems into a mechanism that guarantees data authenticity and freshness. This solution achieves very low latency.

Designing authentication solutions for SCADA and other power grid systems poses challenges different from those in Internet systems. Himanshu Khurana and his colleagues have applied past research in authentication design principles to power grid architectures, emphasizing efficiency, availability, and evolvability.[3] Mark Hadley and his colleagues use an alternate approach in SSCP (Secure SCADA Communications Protocol), which provides SCADA protocol-independent authentication and encryption technologies that can be embedded into field devices or deployed as bump-in-the-wire solutions. This is beneficial because the performance impact dramatically decreases when authentication can be embedded, and it's also important to support deployment in varied environments in which embedding isn't appropriate. Future research integrating these disparate styles would be worthwhile.

Policy-based data sharing. The North American Synchrophasor Initiative (www.naspi.org) is designing wide-area measurement systems. Such systems aim to use GPS-clock-synchronized fine-grained power grid measurements to provide increased grid stability and reliability. Key to achieving this is securely sharing the measurements (synchrophasor measurements gathered by PMUs) among power grid entities over wide area networks. Typically, such sharing follows policies that depend on data generator and consumer preferences and on time-sensitive contexts; for example, entities will more likely share information during an emergency.

Rakesh Bobba and his colleagues have leveraged the presence of trusted third parties to design a mediated policy-based encryption system that protects the secrecy of data and policies while releasing them to authorized entities.[4] Their research extends the key encapsulation mechanism/data encapsulation mechanism (KEM/DEM) encryption framework and leverages RCs and ISOs for policy enforcement. This example shows how the power grid offers opportunities (in this case, trusted third parties with regulatory oversight that might not exist in other environments) for designing solutions.

Attestation for constrained smart meters. Smart meters are a key element of the smart grid and represent a constrained embedded platform. A key challenge is ensuring that these devices' software is authentic, to prevent energy theft and other attacks. These devices' cost, power, memory, and computational limitations restrict the ability to deploy standard trusted platform modules on them.

Michael LeMay and Carl Gunter's Cumulative Attestation Kernel is an architecture implemented at a low level in the embedded system.[5] It provides cryptographically secure audit data for an unbroken sequence of firmware revisions installed on the system, including the current firmware. LeMay and Gunter have developed a prototype that employs microcontrollers typically used in smart meters and formally verifies the remote-attestation protocol.

This article has given a broad-brush description of issues related to smart-grid security. Designing solutions in at this stage, before widespread deployment, would be beneficial; in some cases solutions exist, whereas in others research investments will be needed. Several open questions about goals still require discussion, especially around such topics as how (and how much) privacy can be supported. We hope that this article will help further such conversations. □

References

1. Q. Wang et al., "Time-Valid One-Time Signature for Time-Critical Multicast Data Authentication," *Proc. 28th IEEE Int'l Conf. Computer Communications* (Infocom 09), IEEE Press, 2009, pp. 1233–1241.
2. P. Tsang and S.W. Smith, "Yasir: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," *Proc. IFIP TC 11 23rd Int'l Information Security Conf.* (SEC 08), Springer, 2008, pp. 445–459.
3. H. Khurana et al., "Design Principles for Power Grid Cyber-infrastructure Authentication Protocols," to be published in *Proc. 43rd Ann. Hawaii Int'l Conf. System Sciences* (HICSS 10), IEEE Press, 2010.
4. R. Bobba et al., "PBES: A Policy Based Encryption System with Application to Data Sharing in the Power Grid," *Proc. 4th Int'l Symp. Information, Computer, and Communications Security* (ASIACCS 09), ACM Press, 2009, pp. 262–275.
5. M. LeMay and C.A. Gunter, "Cumulative Attestation Kernels for Embedded Systems," *Computer Security—ESORICS 2009*, LNCS 5789, Springer, 2009, pp. 655–670.

Himanshu Khurana *is a principal research scientist at the Information Trust Institute at the University of Illinois at Urbana-Champaign. Contact him at hkhurana@illinois.edu.*

Mark Hadley *is a research scientist at the Pacific Northwest National Laboratory. Contact him at mark.hadley@pnl.gov.*

Ning Lu *is a research scientist at the Pacific Northwest National Laboratory. Contact her at ning.lu@pnl.gov.*

Deborah A. Frincke *is Cyber Security Chief Scientist at the Pacific Northwest National Laboratory. Contact her at deborah.frincke@pnl.gov.*