ITL BULLETIN FOR OCTOBER 2010

CYBER SECURITY STRATEGIES FOR THE SMART GRID: PROTECTING THE ADVANCED DIGITAL INFRASTRUCTURE FOR ELECTRIC POWER

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

A national effort is under way to transform the U.S. electric power infrastructure into an advanced digital infrastructure that will support the two-way communication of energy information for controlling equipment and for distributing energy. The major changes to the electric power grid are planned to take place over many years, and are expected to increase energy efficiency, advance the transition to the use of renewable sources of energy, reduce greenhouse gas emissions, and create new employment opportunities.

Called the Smart Grid, this advanced power grid for the 21st century is expected to foster new functions and applications. Progress toward these goals will depend upon the development of new techniques that will add to and integrate many different digital computing and communications technologies and services with the electric power infrastructure. Other technologies will be needed as well to protect the privacy of data stored and transmitted over the grid and to secure the computing and communications networks supporting the performance and availability of the electric power infrastructure. These technologies must be designed and implemented early in the development process to assure a smooth transition to the Smart Grid.

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) was charged with the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…" NIST is working with industry, government, and consumer stakeholders to identify and develop the standards that are critical to achieving a reliable and robust Smart Grid. Information about these activities to advance the Smart Grid is available from the NIST Web page http://nist.gov/smartgrid/.

Identification of Standards for the Smart Grid

NIST initiated its responsibilities under EISA by developing a plan to accelerate the identification of an initial set of standards that are potentially applicable to the Smart Grid, and to establish a framework for the development of the additional standards and testing activities that will be needed in the future. In the first phase of the plan, a high-level conceptual reference model for the Smart Grid was designed through an open public process involving many participants from the Smart Grid community and other government organizations.

NIST Interagency Report (NISTIR) 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, was endorsed by the Office of the National Coordinator

for Smart Grid Interoperability and issued in January 2010. It describes the reference model and identifies 75 existing standards that are, or are likely to be, applicable to the ongoing development of the Smart Grid; specifies 15 high-priority gaps and harmonization issues (in addition to cyber security) for which new or revised standards and requirements are needed; documents action plans and time lines for addressing these gaps through standards-setting organizations (SSOs); and describes the strategy to establish requirements and standards to help ensure Smart Grid cyber security.

The Smart Grid reference model will be further developed under the auspices of the Smart Grid Architecture Committee, a standing committee of the Smart Grid Interoperability Panel (SGIP). A public-private partnership formed by NIST in 2009, the SGIP engages stakeholders in an open process of active participation, input, and cooperation with NIST in the ongoing coordination, acceleration, and harmonization of standards development for the Smart Grid.

NISTIR 1108 is available from the NIST Web page http://nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*

NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, is a companion guide to NISTIR 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* The guidelines, which present an analytical framework for developing cyber security strategies, were developed as a consensus document by the Cyber Security Working Group (CSWG) of the SGIP. The CSWG includes more than 500 participants from the private and public sectors, representing vendors, service providers, manufacturers, standards organizations, academia, national research laboratories, privacy advocates, and government agencies. Some members are from outside of the United States.

Issued as a **three-volume report,** NISTIR 7628 helps organizations to develop effective cyber security strategies that can be tailored to their own particular characteristics, risks, and vulnerabilities related to the Smart Grid. The methods and supporting information presented in the report can be used by the many different organizations in the Smart Grid community to assess risks, and to identify and apply appropriate security requirements. Since the electric grid is changing from a relatively closed system to a complex, highly interconnected environment, each organization's cyber security requirements will evolve as technology changes and as threats diversify and increase.

• **Volume 1**, *Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements*, provides background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the grid and the confidentiality of specific information. Other topics covered include the cyber security strategy for the Smart Grid and specific tasks within the strategy; a risk assessment process, used to identify high-level security requirements; and the logical interface model used to identify and define categories of interfaces within and across the seven Smart Grid domains identified in the NIST Framework and Roadmap document. Also presented are the high-level security requirements for each of the 22 logical interface categories

identified and the technical cryptographic and key management issues for Smart Grid systems and devices.

The appendices to **Volume 1** provide a detailed chart with cross-references for Smart Grid cyber security requirements to the security controls included in NIST Special Publication (SP) 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, and to other federal government requirements. Also provided is a chart showing security technologies and procedures that meet high-level security requirements.

• **Volume 2,** *Privacy and the Smart Grid*, focuses on privacy issues within personal dwellings. It provides awareness and discussion of topics such as evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, their behavior within their premises and electric vehicles, and whether these new types of information may contain privacy risks and challenges that have not been legally tested yet; recommendations, based on widely accepted privacy principles for participants within the Smart Grid; and the education of consumers and others about the privacy risks within the Smart Grid and what they can do to mitigate these risks.

The appendices to **Volume 2** include references and Web page links to the Smart Grid and electricity delivery regulations that appear in the laws of States of the United States. Also included is a detailed analysis of some sample privacy use cases (a method of documenting applications and processes for purposes of defining requirements). Terms related to privacy are also defined and explained to help create a common base of understanding for their use.

• **Volume 3**, *Supportive Analyses and References*, is a compilation of supporting analyses and references used to develop the high-level security requirements and other tools and resources presented in the first two volumes. These include categories of vulnerabilities and a discussion of the bottom-up security analysis used by the working group in developing the guidelines; research and development themes involving paradigm-changing directions in cyber security to enable higher levels of reliability and security for the Smart Grid as it continues to evolve; and an overview of the process that the CSWG developed to assess whether standards, identified through the NIST-led process in support of Smart Grid interoperability, satisfy the high-level security requirements.

The appendices to **Volume 3** include diagrams and tables to assist organizations in the selection of security requirements that apply to their detailed logical interfaces, and diagrams and tables that allocate the logical interfaces to one of the logical interface categories.

The three volumes of NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, are available from the NIST Web pages:
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

Risks to the Smart Grid

Clearly, the convergence of the information and communication infrastructure with the electric power grid introduces new security and privacy-related challenges. However, the introduction of these technologies to the electric sector also presents opportunities to increase the reliability of the power system, to make it more capable and more resilient to withstand attacks, equipment failures, human errors, natural disasters, and other threats. Greatly improved monitoring and control capabilities must include cyber security solutions in the development process rather than as a retrofit.

A few examples of potential risks associated with the evolution of the Smart Grid include:

- Greater complexity increases exposure to potential attackers and unintentional errors;

- Networks that link more frequently to other networks introduce common vulnerabilities that may now span multiple Smart Grid domains and increase the potential for cascading failures; and

- There may be inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters.

The security of the systems and information in the information technology (IT) and telecommunications infrastructures must be addressed in all phases of the system development life cycle, from the design phase through implementation, maintenance, and disposition.

Cyber Security Strategies

NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, lays out cyber security strategies, risk assessment processes, and security requirements that each organization should consider in developing its own detailed cyber security approach for securing the Smart Grid.

Organizations should evaluate a constantly evolving cyber risk environment when they design, implement, and maintain their Smart Grid systems. The goal is to identify and mitigate cyber risks for a Smart Grid system using a risk methodology applied at the organization and system levels; cyber risks for specific components within the system should also be considered. This methodology in conjunction with the system-level architecture will allow organizations to implement a Smart Grid solution that is secure and that meets the reliability requirements of the electric grid.

Cyber security concerns for IT have traditionally focused on the protection required to ensure the confidentiality, integrity, and availability of information and the IT communication systems. Cyber security protection for the Smart Grid must be applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and the privacy of consumer information.

In the power industry, the focus has been on implementing equipment that can improve power system reliability. To a significant degree, coordination has been accomplished by linking systems with embedded, stand-alone communication networks. In today's electric grid, much communication and coordination continue to be accomplished by means of the telephone.

However, the effective recording, processing, and exchange of data are becoming increasingly critical to the reliability of the power system.

Cyber security in the Smart Grid must include a balance of both power and cyber system technologies and processes in the operation and management of electric power and IT systems. Safety and reliability are of paramount importance in electric power systems. Cyber security measures in these systems must not impede safe, reliable power system operations.

The strategies recommended in NISTIR 7628 recognize that both domain-specific and the overall common requirements of the electric power and IT systems must be evaluated when a risk assessment process is developed by an organization. A key aim of the risk assessment report is to ensure the interoperability of security solutions across the infrastructure. For each stakeholder, every domain, and the entire Smart Grid, the goal is to develop a cyber security strategy that effectively addresses prevention, detection, response, and recovery.

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors. The risk assessments include identifying assets, vulnerabilities, and threats, and specifying impacts to produce an assessment of risk to the Smart Grid and to its domains and subdomains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and electric sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid.

The security requirements and the supporting analyses included in NISTIR 7628 may be used by strategists, designers, implementers, and operators of the Smart Grid, including utilities, equipment manufacturers, and regulators, as input to their risk assessment process and other tasks in the security life cycle of the Smart Grid. This information will guide organizations in assessing risks and selecting appropriate security requirements.

Ongoing Activities to Develop Cyber Security Strategies for the Smart Grid

As the United States continues to transform the electric power infrastructure, new risks and threats will evolve. The electric power industry needs to remain vigilant to ensure energy efficiency, reliability, and security; to transition to renewable sources of energy; to reduce greenhouse gas emissions; and to build a sustainable economy that ensures future prosperity.

The CSWG will continue to address these new and changing issues as the Smart Grid evolves. Areas that have been identified currently include:

- The need for improved models and tools for identifying vulnerabilities and detecting anomalous behavior;

- The need for research and development to advance the confidentiality, integrity, and availability of the Smart Grid and its information;

- The use of cryptography and key management systems in the grid;

- Privacy concerns for individuals within business premises, such as hotels, hospitals, and office buildings, and privacy concerns associated with transmitting Smart Grid data across national borders; and

- The increased usability of the cyber security content and strategies information developed by the SGWG by a wide spectrum of electric power industry organizations in their technical analyses and adoption of solutions.

For Additional Information

NIST has identified five foundational families of standards as ready for consideration by regulators for implementation in the Smart Grid. These consensus standards, which are fundamental to overall Smart Grid interoperability, were developed by the International Electrotechnical Commission (IEC). The standards will help to enable efficient and secure exchanges of information within and across Smart Grid domains. For information about this initial set of recommended standards, see the NIST Web page http://nist.gov/public_affairs/releases/upload/FERC-letter-10-6-2010.pdf.

Many NIST standards and guidelines were used by the SGWG in developing the strategies for Smart Grid cyber security. For information about NIST standards and guidelines for information security, as well as other security-related publications, see the NIST Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.