CYBER SECURITY IN SMART GRID

Rekha, Kanika Wadhwa,
Assistant Professor, MVSIT, Jagdishpur Sonipat rrekha13rana@gmail.com , wdhw.knk@gmail.com,
Department of Electrical Engineering

ABSTRACT

The electric grid is one of the mostcomplex and important infrastructures ever created, and is vital to modern quality of life and the economy. Generation of electricity is also a significant source of greenhouse gas emissions. Modernization of the grid is central to many nations' efforts to address climate change and improve energy efficiency and reliability. The smart grid represents the integration of information and communications technologies into the existing power system to provide measurement and control needed for increased use of distributed and renewable generation, enabling dynamic management of demand as well as generation, improving reliability, and support for electric vehicles.
Keywords- Interagency Report (IR), Field Message Bus (FMB), Federal Information Processing Standard(FIPS)

I. *CYBER SECURITY AND THE ELECTRICSECTOR:*

The critical role of cyber security in ensuring the effective operation of the Smart Grid is documented in legislation and in the Department of Energy (DOE) Energy Sector Plan as described below: The Energy Independence and Security Act of 2007 (P.L. 110-140) states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid: 1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid. 2. Dynamic optimization of grid operations and resources, withfullcyber-security "

DOE's Energy Sector-Specific Plan2 "envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government."

II. THE SMARTGRID

Maybe you have heard of the Smart Grid on the news or from your energy provider. But not everyone knows what the grid is, let alone the Smart Grid. "The grid," refers to the electric grid, a network of transmissionlines, substations, transformers and more that deliver electricity from the power plant to your home or business. It's what you plug into when you flip on your light switch or power up your computer. Our current electric grid was built in the 1890s and improved upon as technology advanced through each decade. Today, it consists of more than 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines. Although the electric grid is considered an engineering marvel, we are stretching its patchwork nature to its capacity. To move forward, we need a new kind of electric grid, one that is built from the bottom up to handle the groundswell of digital and computerized equipment and technology dependent on it—and one that can automate and manage the increasing complexity and needs of electricity in the 21stCentury.

WHAT MAKES A GRID "SMART?"

In short, the digital technology that allows for two-way communication between the utility and its customers, and the sensing along the transmission lines is what makes the grid smart. Like the Internet, the Smart Grid will consist of controls, computers, automation, and new technologies and equipment working together, but in this case, these technologies will work with the electrical grid to respond digitally to our quickly changing electric demand.

What is the research plan? The research plan is to conduct research that will enable the development of industry standards and guidance in order to successfully implement secure Smart Grid technologies, including through the following:

- Technology Transfer – Technical leadership of the SGCC: Providing cyber security expertise, technical leadership, and oversight required to

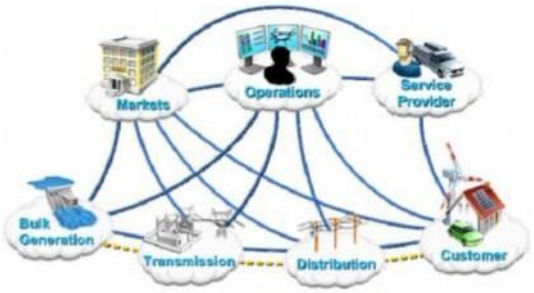
manage theSGCC.

- Technology Transfer – Review identified standards and Smart Grid interoperability requirements against the high-level security requirements in NIST Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Securityto identify any cybersecurity gaps and provide recommendations for further work to mitigate gaps.
- Technology Transfer – Collaboration with CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) Smart Grid Information Security (SG-IS): Collaborate with the European Union's SG-CG SG-IS to develop a white paper on the relationship between the SG-IS Security Levels and NIST Interagency Report 7628 Rev. 1, Guidelines for Smart Grid Cybersecurity.
  - Technology Transfer– Cybersecurity Frameworks Case Study: Work with utilities to develop a case study on how different voluntary cybersecurity guidance frameworks (e.g., Cybersecurity Capability Maturity Model, Framework for Improving Critical Infrastructure Cybersecurity, NISTIR 7628) are implemented. The case study will highlight different methodologies for implementing the frameworks, goals, results, benefits, and lessons learned. Contribute to the SGIP Open Field Message Bus (FMB) Project by identifying cybersecurity recommendationsfor the Distributed Intelligence Platform.
  - Fundamental and AppliedResearch

  – Cybersecurity Smart Grid Testbed: Collaborate with ITL Software and Systems Division on cybersecurity related research in relation to the IEEE 1588 standard on time synchronization. Conduct research on smart grid applications of cryptography for constrained environments and delayed authentication. Conduct research on providing cybersecurity for legacysystems.

IV SMART GRID CYBER SECURITY STRATEGY

The overall cyber security strategy used by the CSWG in the development of this document examined both domain-specific and common requirements when developing a risk mitigation approach to ensure interoperability of solutions



across different parts of the infrastructure. The cyber security strategy addressed prevention, detection, response, and recovery. This overall strategy is potentially applicable to other complex infrastructures. Implementation of a cyber security strategy required the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential foranunwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk, which 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 and includes 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 information included in this report is guidance for organizations. NIST is not prescribing particular solutions through the guidance contained in this report. Each organization must develop its own detailed cyber security approach (including a risk assessment methodology) for the Smart Grid. The following

documents were used in developing the risk assessment methodology for the Smart Grid: 5 NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010 •SP800-39, DRAFT Managing Risk from Information Systems: An Organizational Perspective, NIST, April 2008; • SP 800- 30, Risk Management Guide for Information Technology Systems, NIST, July 2002; • Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, NIST, March 2006; • FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004; • Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment, North American Electric Reliability Corporation (NERC), 2002; • The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency, Department of Homeland Security, 2009; • The IT, telecommunications, and energy sector-specific plans (SSPs), initially published in 2007 and updated annually; • ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, International Society of Automation (ISA), 2007; and • ANSI/ISA- 99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, ISA, January2009.

Smart grid conceptual model

V. SECURITY REQUIREMENTS

The availability of electric power in North America depends in part on the availability of the power grid control systems. As part of the development of smart grid, these control systems are becoming more sophisticated, allowing for better control and higher reliability. Smart grid will require higher degrees of network connectivity to support the new sophisticated features.
This higher degree of connectivity also has the potential to open up new vulnerabilities.
According to the Electric Power Research Institute (EPRI) one of the biggest challenges facing the smart grid development is related to cyber security of systems. According to the EPRI Report, “Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address notonly deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.”

REFERENCES

[1] Towards trustworthy systems with open standards and trusted computing European Multilaterally Secure Computing Base,2005 [Online]. Available: http://www .emscb.com/content/pages/493 73.htm

[2] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/ InterimSmartGridRoadmapNISTRestructu re.pdf

[3] Draft smart grid cyber security strategy and requirements, NIST IR 7628, Sep. 2009 [Online]. Available: http://csrc.nist.gov/publications/ drafts/nistir-7628/draft-nistir-7628.pdf

[4] “Public key infrastructure,” Wikipedia Feb. 18, 2010 [Online]. Available: http://en.wikipedia.org/wiki/Public_key_in frastructure

[5] WiMax Security 2010 [Online]. Available: http://www.topbits. com/wimax-security.html

[6] 802.16e Notes—Mitchell Group, Stanford Univ.. Stanford, CA, pp. 94305– 9045, Jun. 6, 2005 [Online]. Available: http://www.iab.org/liaisons/ieee/EAP/802. 16eNotes.pdf

[7] L. Cuilan, “A simple encryption scheme based onWiMAX,” presented at the Int. Conf. E-Business and Information System Security, Wuhan, China, 2009.

[8] N. Davis, Secure software development life cycle processes Software Eng. Inst., Carnegie Mellon Univ.,2009.

[9] Shaneck, K. Mahadevan, V. Kher,and

Y. Kim, Remote softwarebased attestation for wireless sensors Comput. Sci. Eng., Univ. Minnesota— Twin Cities, 2005,. :,.

[10] Catalog of Control Systems Security: Recommendations for Standards Developers, DHS Sep.2009.

[11] D. Challener *et al., A Practical Guide to Trusted Computing*. Upper Saddle River, NJ: IBMPress.