Smart Grid and Cyber Challenges

National Security Risks and Concerns of Smart Grid

Stephen Spoonamore and Ronald L. Krutz, Ph.D., PE, CISSP, ISSEP

This document surveys cybersecurity concerns associated with the Smart Grid. It assumes that the reader is familiar with the main aspects of proposed Smart Grid technology, and has a working knowledge of cyberattacks.

Executive Summary

Whether it is going to be a physical or cyber attack, the grid must resist two different attack strategies[1]:

1. Attacks on the physical power system, in which the infrastructure itself is the primary target.
2. Attacks through the power system, in which attackers take advantage of power system networks to affect the infrastructure systems, or supported commercial, financial, or government infrastructures.

The Smart Grid is required to be self-healing and resistant to attacks. 'Self-healing' has been a goal of networks for more than a decade and has never been achieved. It would be wiser to design Smart Grid so when it is attacked, the Smart Grid reverts to a Dumb (but working) Grid. Similarly, in spite years of research and development by myriad programmers, researchers, and designers, attack-proof networks have never to be achieved. In the experience of the authors it will never be achieved. Risk can be quantified, but never eliminated. Even SWIFT and the DoD's SIPRENET, both tightly controlled and monitored non-public networks have been victimized repeatedly by attacks.

It is self-deluding to claim a Smart Grid will be self-healing and attack-resistant. Achieving Smart Grid capacity in best-conditions is possible, but design bakes-in should limit to how far a system can be reprogrammed remotely. The potential for revolutionizing electrical transmission, distribution, metering, billing and so on is wonderful, however it must be understood casual pranksters, determined attackers or nation-state actors will use this lucrative entry point to either spoof with or attack end-point users, power generators or scheme to disable assets connected to the grid.

Extensive investments in cybersecurity in general, fail-to-Dumb-but-Working Mode rules and systems, and new Supervisory Control and Data Acquisition (SCADA) along with extensive and human capital intensive real-time distributed control system will be needed. These systems must be coupled to risk analysis and security paradigms at least equal to those in banking settlement and SWIFT wires, which have themselves been subject to numerous attacks and breaches in recent years. The probability of hacking into Smart Grid must be assumed to be 100%, and limitations of the damage possible by such entry must be a core element of the design. These designs should assume penetration of the network will take place at various layers and address responses on the network and in legal enforcements that are effective. There is also the concern False Positives of user activity on a Smart Grid may make the process of sorting attacks/malicious activity from user-intended actions extremely tedious . At this point in time, the authors do not believe the publicly discussed goals are 100% achievable, and further believe if care is not taken, the rush to make Electrical Systems IP addressable can result in catastrophic failures.

Background

A summary definition of the Smart Grid is given as follows[2]:

[1] A Systems View of the Modern Grid, RESISTS ATTACK," Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, January 2007.

[2] Order Code RL34288, Congressional Research Service Report for Congress, Smart Grid Provisions in H.R. 6, 110th Congress

[3] The NETL Modern Grid Initiative, "A VISION FOR THE MODERN GRID," Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, March 2007.

"The term Smart Grid refers to a distribution system that allows for flow of information from a customer's meter in two directions: both inside the house to thermostats and appliances and other devices, and back to the utility by IP addressable means."

Two of the key characteristics of the Smart Grid are defined[3] as:

1. "It will heal itself." The Smart Grid is touted to perform continuous self assessments to detect, analyze, respond to, and as needed, restore grid components or network sections. Acting as the grid's "immune system", self healing [4]will help maintain grid reliability, security, affordability, power quality and efficiency."
2. The Smart Grid will resist imbalances in the grid, but will be subject to deliberate IP attack. Security requires a system-wide solution that will reduce physical and cyber vulnerabilities and recovers rapidly from disruptions, it will need hard coded "fail-on" points, and strong, non-software based limitations on how much control the IP addressable elements can command. The Smart Grid will demonstrate resilience to some attacks, but all systems operating today have proven vulnerable to determined and well equipped attackers. The move to Smart Grid will further make the electric system subject to zero day attacks, and the constant need to remain ahead of the processing attacks made possible by each cycle of Moore's Law. The Smart Grid will need constant updating or will become subject to multiple, coordinated attacks over a span of time against forces of ever increasing processing power."
3. It should not be forgotten the current grid, or Dumb Grid, works, is relatively robust and has a long established historical working relationship with operators, customers, generation facilities and transmission. The risks of Dumb Grid are known, and systems, agreements and processes to address them are mature. A move to Smart Grid will bring numerous new risks, and may in fact undermine existing robustness of the Dumb Grid. This should be considered and examined in a more detailed analysis.

This paper will focus on items 1 and 2.

Background Statistics

The U.S electrical power grid is extremely large and complex, with the following characteristics[5,6]:

- More than 9,200 electric generating plants
- More than 1,000,000 megawatts of generating capacity
- Connected to more than 300,000 miles of transmission lines.
- More than 3,100 electric utilities
- 213 stockholder-owned utilities provide power to about 73% of the customers
- 2,000 public utilities run by state and local government agencies provide power to about 15% of the customers
- 930 electric cooperatives provide power to about 12% of the customers
- Nearly 2,100 non-utility power producers, including both independent power companies and customer-owned distributed energy facilities.
- Bulk power system consists of three independent networks: Eastern Interconnection, Western Interconnection, and the Texas Interconnection. These networks incorporate international connections with Canada and Mexico. Overall reliability planning and coordination is provided by the North American Electric Reliability Council.
- Ownership shifting from regulated utilities to competitive suppliers is occurring.

[5] "The Smart Grid: An Introduction," prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 560.01.04

[6] "Grid 2030, A National Vision for Electricity's Second 100 Years," United States Department of Energy, Office of Electric Transmission and Distribution, July 2003.

The state of the electric utility industry today relative to information system security, from the U.S. DoE "Resists Attack" document[7] is as follows:

- Incomplete understanding of threats, vulnerabilities and consequences.
- Industry as a whole lacks a standard approach to conducting these assessments, understanding consequences, and valuing security upgrades.
- Additionally, limited access to government-held threat information makes the case for security investments even more difficult to justify.
- Perception that security improvements are prohibitively expensive. When examined independently, the costs and benefits of security investments can seem unjustifiable.
- Increasing use of open systems. Open communication and operating systems are flexible and improve system performance, but are not as secure as proprietary systems. The increasing use of open systems must be met with industry approved and adopted standards and protocols that consider system security.
- Difficulty in recovering costs. Utilities must be armed with sufficient knowledge and justification to make the case for security investments.

The Energy Web

The Smart Grid is to be based on an "Energy Web," an analog of the Internet and World Wide Web. As with the Internet, this network will be packet-switched and provide for many diverse paths from sender to receiver for reliability and resiliency. Also, each computing resource, sensor, control element, and so on will have a unique, IP address, so that specific messages can be exchanged among the elements. Thus, electrical transmission and distribution will have two-way communications with sensors and computers. This capability will allow a heretofore unobtainable level of monitoring and control of the entire electrical grid and allow outside intruders or malicious insiders to damage the grid. Once intruders gain entry, they have the potential to remain in any compromised grid.

Areas of Concern

The Smart Grid goals of continuous self-assessment, self-healing and resilience to attack will not work. These characteristics have been proposed for the Internet, Banking Systems and SCADA systems for more than a decade, to date, they have not been accomplished. This idea must be replaced by a "Limits of Control" (LoC) "Range of Addressable a Commands" (RAC) and a risk-tolerant set of failure states. This model has proven successful in global credit card and banking settlement systems.

In a 2000 testimony before the U.S. Congress, Professor Raj Reddy of Carnegie Mellon University proposed a self-healing Internet[8]. In this testimony, he defined a self-healing network as:
"one which continuously monitors all the traffic within the system (every packet entering the system is validated before it can proceed) with a view to detect and disable abnormal traffic patterns. The goal of a self healing network is to provide a mechanism for detecting unauthorized use of networking equipment and provide a mechanism for tracking inappropriate uses and identifying the individuals using networks for malicious intent, without compromising individual rights to privacy and security on the network."

While this may be a worthy goal, it is not currently achievable, nor do most experts expect it ever will be.
Certainly in the near-term, a truly self healing network can not achieved to help Smart Grid deployment, instead Risk-Based planning with analysis of utility networks with disparate interfaces, standards, restrictive legacy systems, low bandwidth connections, and limited processing capabilities must be implemented.

[7] "A Systems View of the Modern Grid, RESISTS ATTACK," Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, January 2007.

[8] Reddy, Raj. "Towards a Dependable Self-Healing Internet," Input to March 8, 2000 congressional testimony, March 9, 2000.

For the Energy Web to be truly reliable, it must be resistant to attacks. Looking at the Internet as an historical example, even though thousands of security experts address attacks every day, attack resistance is poor, and mostly reactive. Banking systems, with much higher security expert to end user ratios are better, but still subject to frequent compromise. While, in theory, the World Wide Energy Web will not be an "open" network that can be accessed by unauthorized individuals, in practice, if the system is made IP addressable it will be accessed by unauthorized and malicious entities. In fact, in the conception, design, and implementation of the Smart, it should be assumed that a malicious attacker will gain access to the network and associated hardware and metering. Red Team planning should determine the limits of damage tolerable when such an attack occurs and design the system to that discovered limit.

As Gary Brown, Chair of the New York State Public Service Commission states[9], "Smart meters will be located in very insecure locations since they can easily be reached by the public. Therefore physical security or "walls" around the meter are impractical. Since meters are on customer premises, attempts to tamper or vandalize cannot be 100 percent prevented. Will there be technology to detect such attempts – in real time?"

In a presentation to the National Classification Management Society (NCMS) in Plymouth, Minnesota on August 1, 2008, David Berglund of the Defense Security Service (DSS) stated that even the classified DoD SIPRENET network "got a virus and within 4.3 seconds, 700 computers across 6 bases in Europe were affected." Viruses have been found in new, never opened software and CDs. We must assume Smart Grid will not be as secure as SIPRENET, one of the most restricted and protected networks in the world. But in many real world ways, with real world impacts the Electrical Grid is even more dangerous to expose to attackers. It is, by definition connected to everything critical and trivial in our nation

Implementing a fully interconnected Smart Grid, will without question open up new avenues of control for Electrical distrobution efficiency and Green Technology. However it will do so by exposing the U.S. electrical infrastructure to two-way IP communications and execution of control commands. The risks of this might expose the following issues if not implemented properly:

- Exploitation of real vulnerabilities to associated systems dependent on the Electrical Grid.
- Actually reduce the security posture of transmission and distribution systems
- Increase the probability of serious attacks on entire transmission and distribution systems from remote locations
- Face constraints of legacy systems that small memory and processing capacity other than for controlling operations
- Provide unauthorized access to the entire grid through a poorly protected customer's or user's computers
- Vandalizing or compromising of information of Intelligent meters
- Low bandwidth limitations on some connections that will not support digital authentication certificates
- Interoperability issues among extant multiple, and disparate computer systems

Another very important issue in self-healing and attack resistance is the case of warning systems issuing false positive indications of attacks. False positives are a common problem in intrusion warning systems and can lead to dangerous and catastrophic consequences if acted upon without verification.

Recommendations

Improved methods for gauging risks and the security posture of real-time distributed control systems and SCADA systems will be required in order to provide a basis for the implementation of the Smart Grid. SCADA systems manage the ongoing operations of transmission and subtransmission lines and equipment between the generator and substation.

[9] Brown, Gary, Chair, New York State Public Service Commission, "The Future of the Smart Grid," SANS Process Control & SCADA Security Summit, February 2, 2009.

The Smart Grid development life cycle should assume successful penetrations and attacks from external sources as well as disgruntled insiders. The Smart Grid should have the ability to isolate large grid segments from compromised segments in near real time to prevent a contaminated section from infecting other large areas of the grid.

Self-healing must be dismissed as a concept and replaced with Risk-Assessed, Fail-Open LoC and RAC managed systems. Self-healing element themselves, if used, must be investigated more thoroughly to ensure that the “healing” does not introduce more problems than the original issue across the disparate systems of the Grid.

Mechanisms have to be explored to reduce false positives to a minimum level along with algorithms to validate positive intrusion indications and minimize responses that can initiate damages to the grid from reacting to false positives.

Bibliography

1. Amin, M. and B.F. Wollenberg “Toward a Smart Grid: Power Delivery for the 21st Century,” IEEE Power and Energy Magazine, Vol 3, No 5, Sep/Oct 2005.
2. Amin, M. “Toward Self-Healing Energy Infrastructure Systems,” cover feature in the IEEE Computer Applications in Power, pp. 20-28, Vol. 14, No. 1, January 2001
3. Electric Power Research Institute. 2004. Electricity technology roadmap: Meeting the critical challenges of the 21st century. Summary report, product no. 1010929.
4. Federal Energy Regulatory Commission. 2006. Rules concerning certification of the electric reliability organization; and procedures for the establishment, approval, and enforcement of electric reliability standards. 18 CFR Part 39, Docket No. RM05-30-000, Order No. 672.
5. Huber, R. and R. Fanning. 2003. Distribution vision 2010. Transmission and Distribution World (January), http://tdworld.com/mag/power_future_distribution/.
6. Modern Grid Initiative Web Site (www.netl.doe.gov/moderngrid)
8. U.S. Department of Energy Office of Electric Transmission and Distribution. 2003. “Grid 2030”: A national vision for electricity’s second 100 years.
7. U.S. Department of Energy, National Energy Technology Laboratory, Modern Grid Initiative, http://www.netl.doe.gov/moderngrid/opportunity/vision_technologies.html