Hacking the Smart Grid

Tony Flick
FYRM Associates
tony.flick@fyrmassociates.com

Abstract

The city of Miami and several commercial partners plan to rollout a “smart grid” citywide electrical infrastructure by the year 2011. This rollout was announced on the heels of news that foreign agents have infiltrated our existing electrical infrastructure and that recent penetration tests have uncovered numerous vulnerabilities in the proposed technologies. Simultaneously, the National Institute for Standards in Technology (“NIST”) has recently released a roadmap for producing smart grid standards. In this whitepaper, I will discuss the flaws with the current guidelines and map them to the criticisms of similar regulatory mandates, including the Payment Card Industry Data Security Standard (“PCI DSS”), that rely heavily on organizations policing themselves.

What is the Smart Grid?

The smart grid provides electricity from suppliers to consumers using digital technology. The proposed technology will allow suppliers to remotely monitor consumer usage as well as implement variable rates that increase and decrease during peak energy use times. Additionally, consumers will be able to monitor their energy use in real time, which could allow them to save money by conserving energy during peak energy use times. The major goals of the smart grid initiative are to increase efficiency, reliability, and safety of the country’s electrical infrastructure.

Security Initiatives

Every security-related document regarding the smart grid discusses and requires security to be integrated into the smart grid from the very beginning. This is a significant improvement over previous technology initiatives and shows that organizations and elected officials are beginning to understand at some level how to manage security in projects.

The Energy Independence and Security Act of 2007 provided the Department of Energy with the responsibility of developing the smart grid program. The Department of Energy then assigned NIST the responsibility of developing a framework of interoperability, including security of the smart

grid [1]. As a result, NIST has started the Smart Grid Interoperability Project to develop the framework [2] for the smart grid.

Timeframes

These initiatives, along with upcoming legislation on advancing the smart grid rollout, show the smart grid has received attention from the country's elected officials. However, these initiatives cannot ensure that security is integrated from the beginning since utility companies have been rolling out smart grid components for the past several years. Below is a list of example security initiatives with their associated timeframe:

- Energy Independence and Security Act of 2007
    - Initial bill passed by the House of Representatives on January 18, 2007
    - Final bill signed into law on December 18, 2007. [3]
- Advanced Metering Infrastructure (AMI) System Security Requirements v1.01
    - AMI-SEC Task Force formed on August 23, 2007 [4]
    - Released on December 17, 2008. [5]
- NIST Smart Grid Interoperability Framework
    - Initial list of standards for inclusion in version 1.0 released on May 8, 2009. [2]
- Critical Electric Infrastructure Protection Act (CEIPA) - (HR 2195)
    - Introduced April 30, 2009 [6].

Alternatively, smart grid design and implementations were initiated several years prior to these initiatives. For example, Austin Energy began designing and implementing their smart grid in 2002 [7] and the Salt River Project began installing smart meters in 2006 [8]. Although the security initiatives and elected officials have good intentions, they have missed the window of opportunity to truly integrate security from the beginning by several years. Similar to the credit card industry, banking industry, health care industry, and most industries that conduct business online, the next electrical infrastructure will have security featured as an add-on that is applied after the smart grid is implemented.

History Repeating

As of the writing of this white paper, NIST has released a draft framework for review that includes some of the proposed standards. While there are several security standards listed in the framework, NIST appears to be making the same mistakes of previous regulatory mandate governing bodies. For example, the PCI DSS standards have been criticized for not requiring sufficient security in environments that process cardholder data. This argument embodies the difference between compliant and secure. Specifically, one of the major criticisms is the "self policing" aspect of these standards. The credit card companies (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.) are responsible for ensuring that relevant companies are compliant with the standards. If a company is deemed non-compliant, then the credit card companies issue what they consider to be the appropriate punishment.

For merchants that do a certain amount of credit card transactions, PCI requires them to fill out a self-assessment questionnaire ("SAQ"), as opposed to an on-site assessment by an approved third party, to determine whether the merchant adheres to certain security controls. This approach relies on the "honor system" to ensure that companies are compliant with the PCI DSS. As a result, a company could potentially report inaccurate security controls in their SAQ. Similarly, a recent analysis by the North American Electric Reliability Corporation ("NERC") reported, "many utilities are underreporting their critical cyber assets, potentially to avoid compliance requirements." [9] These results show that the utilities should not be trusted to ensure that proper security is implemented.

The new framework, to be released by NIST, will rely on "self policing" by the utility companies as well. Currently, there are no processes to ensure that utility companies adhere to the proposed standards released by NIST. As shown by previous incidents, the utility companies do not always follow the recommendations to mitigate vulnerabilities. For example, the Homeland Security Committee recently released that numerous utilities did not mitigate a vulnerability, known as Aurora. Despite advisories from both NERC and the Federal Energy Regulatory Commission ("FERC"), the utilities had not implemented the recommendations to mitigate the risk associated with this vulnerability. [9]

The new standards also leave out critical details on how to implement the security requirements. As a result, energy companies and technology companies will need to determine how to implement the high level requirements. For example, authentication mechanisms are required for controlling access to devices. However, what authentication mechanisms should be used? Will the authentication be password based or PKI based?

Should two-factor authentication be required? Will the utility companies have the resources necessary to implement strong authentication effectively? The answers to these questions will need to be addressed by the energy and technology companies implementing the smart grid.

Counter Arguments

When discussing tighter regulation or security, the arguments of innovation being stifled will inevitably arise. Security and regulation should not prevent innovation; however, the proper levels of security and regulation need to be in place. As previously discussed, without proper regulation, the utility companies may not maintain a proper security posture. Additionally, recent penetration tests have shown that proper security mechanisms are not currently built into components of the smart grid. Recently discovered vulnerabilities in smart meters have been identified that could allow an attacker to obtain complete control of the meters. Specifically, an attacker could exploit these vulnerabilities to turn off electricity to hundreds of thousands of home. [10] Thus, an attacker could execute a wide-scale Denial of Service ("DoS") attack on the electrical infrastructure. These new vulnerabilities combined with the previously discussed issues that the industry faces provide the argument that tight regulation needs to be in place to ensure security is integrated into the smart grid.

Recommendations

Smart grid implementations have been rolled out in various cities across the United States as well as rest of the world for several years. The opportunity to integrate security into the smart grid from the very beginning has already passed; however, most of the implementations have been small. Before larger implementations, such as the smart grid rollout in Miami, the security frameworks and initiatives surrounding the smart grid technology should be allowed to mature.

While NIST is the proper organization to issue the security requirements, more granular requirements need to be addressed. Technology companies should not be left to determine which authentication mechanism to implement or what encryption key size to use. NIST should be responsible for determining these requirements.

In 2010, FERC is supposed to receive the authority to begin fining utility companies up to $1 million dollars a day for non-compliance with security standards. [11] While this will increase pressure on the utility companies to become compliant, a large portion of the smart grid will have been rolled out across the country already. As shown in the recent studies, these devices will not be compliant and utility companies will be forced to add security as a

feature. As such, the current rollouts of smart grid technology should be suspended until all components are compliant with stringent security standards.

The majority of discussion surrounding smart grid security has focused on what attackers could do to utility consumers. However, the risk to utility companies is just as severe. Utilizing the previously mentioned vulnerabilities [10], end-users could attempt to adjust the amount of electricity reported back to their utility company. Thus, end-users could be allowed to steal utilities, costing utility companies millions of dollars a year. As a result, the utility companies should adhere to the security recommendations to prevent loss of revenue.

Conclusion

Most experts attribute the current economic downturn to the deregulation of banks that allowed them to issue risky loans. When questioned by a congressional committee, the former Federal Reserve Chairman Alan Greenspan stated that he made a “mistake” [12] in trusting that free markets could regulate themselves without government oversight. Similarly, the utility and technology companies associated with the new electrical infrastructure should not be trusted to regulate themselves and strict oversight should be applied to ensure that these companies adhere to proper security standards.

References

[1] “Title XIII.” Energy Independence and Security Act of 2007. U.S. Government Printing Office. 14 Jun 2009. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf>.

[2] Standards Identified for Inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0. National Institute of Standards and Technology. <http://www.nist.gov/smartgrid/standards.html>.

[3] “Energy Independence and Security Act of 2007.” 22 May 2009. Wikipedia. <http://en.wikipedia.org/wiki/Clean_Energy_Act_of_2007>.

[4] Darren Reece Highfill. “UCAlug: AMI Security.” Sep 2008. <http://osgug.ucaiug.org/utilisec/amisec/Meetings/20080917%20-%20Telecon/AMI-SEC%20Overview%20-%20v1%20-%2020080917%20-%20drh.ppt>.

[5] “AMI System Security Requirements – V1.01.” 17 Dec 2008. AMI-SEC Task Force. <http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/1.%20System%20Security%20Requirements/AMI%20System%20Security%20Requirements%20-%20v1_01%20-%20Final.doc>.

[6] Thompson and Lieberman Introduce the “Critical Electric Infrastructure Protection Act”. 29 Apr 2009. United States House of Representatives Committee on Homeland Security Press Center. <http://homeland.house.gov/press/index.asp?ID=448>.

[7] “Smart grid.” 24 Jun 2009. Wikipedia. <http://en.wikipedia.org/wiki/Smart_grid>.

[8] “Salt River Project’s smart meter rollout nears completion.” 6 Feb 2007. METERING.COM. <http://www.metering.com/node/7500>.

[9] Homeland Security Committee Introduces HR 2195, a Bill to Secure the Nation’s Electric Grid. 30 Apr 2009. United States House of Representatives Committee on Homeland Security Press Center. <http://homeland.house.gov/press/index.asp?ID=450>.

[10] Mike Davis. “Black Hat USA 2009 Briefings Speaker List.” Recoverable Advanced Metering Infrastructure. 25 Jun 2009. <http://blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Davis>.

[11] Andy Greenberg. “Congress Alarmed At Cyber-Vulnerability Of Power Grid.” 22 May 2008. <http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security_cx_ag_0521cyber.html>.

[12] Kara Scannell and Sudeep Reddy. “Greenspan Admits Errors to Hostile House Panel.” 24 Oct 2008. The Wall Street Journal. <http://online.wsj.com/article/SB122476545437862295.html>.