The Privacy of a Nation: Smart Grid Data in the Global Space

Cameron Jackson

cameron.jackson@tufts.edu

Professor Ming Chow

Abstract

The United States, along with many other countries, has begun the process of distributing electric power using a "smart" or "intelligent" grid, an infrastructure that uses and analyzes real-time bi-directional data to adjust electric power transmission and delivery (Gellings 1, Makansi 80-81). From the individual consumer perspective, this involves the installation of "smart meters" in the home, which are IP addressable, internet connected devices, the "smartest" of which send real-time data concerning energy usage to and from energy service providers. While there have been many studies examining the privacy implications of consumers using smart meters (Paverd 1), this paper will focus on the privacy implications of the United States as a body in the greater geopolitical space. Upon the leakage of smart grid and smart meter data, telling information about the U.S. and its citizens is open for any attacker to take advantage of, wreaking financial havoc, planning well-timed terrorist attacks, or honing methodology for accessing and attacking the grid. Furthermore, as this technology is increasingly distributed and updated, the data stored about individual consumers, and by extension the U.S., will become more detailed and revealing. This paper will examine these concerns and summarize recent attempts to secure the privacy of smart grid data, demonstrating the implications of smart grid policies and data in the United States.

Introduction

According to the Congressional Research Service report on smart meters and privacy, the data usage recorded by a smart meter can imply a large amount of information, including the consumer's daily routine and which applications are used most frequently and at what times (Murill 7). Spikes in electricity usage can also imply the recent acquisition of a large appliance or electric car, and an increase in daytime electricity can point towards a recent unemployment

(Rottondi 2). The potential release of these personal details are often cited as the reason to avoid the installation of smart meters, and while the privacy implications of the consumer are indeed large, this paper will focus on the privacy implications of the United States as a national body.

If we extrapolate this level of detail to a much larger dataset, the analysis of the electrical usage of a nation paints a real-time picture of the United States, or any nation using a smart grid, from the perspective of both the consumer and the electric service provider. This allows a viewer of this dataset to draw meaningful conclusions about a country's citizens, gaining an understanding of the societal underpinnings and an ability to manipulate and harm them: as individuals and as a nation.

Overview of the Electric Grid Infrastructure

The current electric grid infrastructure is a complex, dynamic entity that maintains a symbiotic relationship with various energy industries including natural gas, petroleum, nuclear power, and coal (Makansi 132). As the global requirement for power grows, the United States must compete with other growing nations to ensure the viable purchase of the energy needed to supply electricity across the country. Furthermore, once the energy has been purchased (or produced in-house), it must travel successfully from major locations to the remainder of the United States. This system is formally called Transmission and Delivery (T&D) and consists of an intricate combination of stations and substations from which energy travels to all needed areas in the country (Makansi 81). Therefore, the implementation of any major change in the current electrical grid system must both incorporate the existing structures and communicate with all other energy industries.

To The Community

The 2003 Northeast-Midwest blackout brought to fruition the fears of the leaders electric and energy industry, bringing the extent of the devastation that would follow a true blackout to the attention of the average American citizen (Makansi 210). Additionally, it underscored the fragility of the current electric grid system; the cause of the blackout was determined to be a lack of proper tree - trimming (Makansi 210). In fact, many of the minor blackouts have been attributed to "acts of God," making true analysis and prevention of these events extremely difficult (Makansi 211). From a security standpoint, the assumption that a blackout is benevolent leads to complacency in responsiveness, allowing potential attackers to take advantage of a natural blackout to do serious damage to the infrastructure. With proper tools to analyze, visualize, and improve the nature of transmission and delivery of electrical power, the smart grid could in fact be more secure (Makansi 211).

Furthermore, the importance of energy efficiency in the U.S., and the world, has only been increasing in the recent years (Gellings 70-75). Smart grids have the ability to identify and relieve bottlenecks, providing a flexible service that reflects the current market. A smart meter can also allow a consumer to quickly and easily identify the most draining appliances; communication between a smart meter and an electric service provider can encourage the automatic shutoff of unused appliances after a certain amount of time (Gelings 10-11).

The smart grid is here to stay, and while many are working to make it as secure as possible, it is also important to consider the geopolitical status of energy supply and demand and the implications smart grid data has for the United States.

Security and Privacy Implications

Smart Grid Vulnerabilities

Due to the interconnectedness of the electric grid system, and smart grid by extension, there are various points of entry that a malicious attacker can take advantage of. This section will focus on the vulnerabilities that lead to information leakage of both consumer electricity usage and corporate electricity policies.

1. Smart Meters

The most pertinent example lies in smart meters, which are IP addressable, internet connected devices, and therefore privy to many of the same vulnerabilities faced by other internet-connected devices. This includes, but is not limited to:

- Cloning : replacing a smart meter with a device that successfully interacts with the grid, but reports zero usage (Ali 176). This has serious financial repercussions for the electric service providers, but also holds a great potential for information leakage. The owner of the "clone" smart meter gains valuable information regarding a electric service provider's communication with the consumer. Additionally, the implied trust between a smart meter and a smart grid could leave a window of opportunity otherwise closed from a truly outside adversary.
- Network Sniffing : the smart meter connects to the network inside the home of a consumer, adopting the known vulnerabilities of the typical home-wireless network, including network sniffing. A successful perusal of the network could leak consumer energy use and/or cryptographic keys between the meter and the grid (Flick 219-220).

2. Broadband Over Power Lines

Additionally, in the past two decades, electric service providers have experiment with Broadband Over Power Lines (BPL), which is an emerging technology that allows electric service providers to communicate directly with consumers using existing power lines (Flick 211, Larson 1). This treats some of the most pressing security issues surrounding real-time bi-directional communication between meters and the grid (Larson 2). However, similar to any emerging technology, the vulnerabilities concerning BPL are not yet known, and as such many are wary to condone its exclusive use in the smart grid.

3. Intentional Leakage

Lastly, due to the experimental nature of smart grid research, many initial tests and datasets are currently available for use as open data sets (Barker). With this data, malicious attackers are aware of the format, breadth, and coverage of data to expect. I argue that even completely anonymous leakage of consumer data could lead to serious privacy concerns for the nation.

Privacy Concerns on the National Level

Financial Repercussions

In addition to the aforementioned privacy issues for individual consumers, the advent of changing prices based on consumer demand and electric service provider supply allows more room for corruption to take hold, on the part of both the consumer and the supplier. A consumer could attempt to siphon energy, and a supplier could use the information deduced from the smart meter data usage to raise or lower prices at certain times. On the national level, serious financial havoc could occur.

A demand response system stems from times of relative energy shortage, and is an attempt to reduce the total energy demand (so that supply is sufficient) through using incentives for customers (Paverd 3). These incentives include time-of-use pricing, or changing the rate based on the time of day, critical peak pricing, or raising the rate on specific, foreseeable peak usage times, and demand bidding, which is when an electric service providers indicates a known peak events and consumers bid on the amount by which they are willing to decrease demand at a given time (Paverd 4). A demand response system relies on a certain degree of trust between a consumer and an electric service provider; with the advent of the smart grid, an adversary could corrupt that trust, using it to shape the financial market in dangerous ways. For example, given a known peak usage time or event, an adversary could hijack the demand bidding process, severely straining the amount of money received by the electric service provider or the consumer, resulting in serious energy cost inflation. In turn, since the electric grid is so interconnected, the price of many of energy forms in the U.S. could rise, dealing a devastating blow to the energy industry, and American economy as a whole.

Furthermore, if we examine the current geopolitical space in terms of energy consumption, we see that China and India, the most rapidly growing nations in the world, will (relatively) soon overtake the U.S. in terms of average energy consumption (Makansi 250). All three of these countries rely on natural gas and oil strongholds, located in Russia and Iran, to supply their increasingly large energy demands (Makansi 251). Thus, hostile foreign nations, with the knowledge of American peak usage times and high usage events, could choose to raise the price of oil and natural gas at times designed maximize their profit and, by extension, the United States' deficit. Alternatively, they could force the United States' hand in an unrelated issue, introducing a natural gas or oil embargo with beforehand knowledge of the ideal time to do so. This could have serious financial and infrastructure repercussions for the United States.

Terrorism/Infrastructure Failure

The most initially apparent vulnerability to the U.S. upon the leakage of smart meter data lies in the easy identification of the habits of the American people. Given a microgrid (a section of the country, city, or even neighborhood, that is exclusively served by smart meters and smart grids), a hostile person could gain knowledge of where people are at any time of the day, planning an attack that will result in the highest possible damage. Alternatively, if the goal is theft, smart meter data also identifies not only when targets are away from home, but how valuable their appliances are (Murill 7-9).

Another less obvious vulnerability stems from the transmission substations necessary to connect the the energy flowing from the interconnections that make up the U.S. national grid: The Eastern Interconnection, the Western Interconnection, Canada, and Texas (Makansi 81). These locations are not publicly shared, but given adequate knowledge of energy pull and flow, could be deduced (Makansi 80). Furthermore, the substations are not given any extra layers of security since they are automated, with no human workers, and should their location be discovered as a result of an information leak, a hostile person could take down entire sections of the national grid system (Makansi 81). In truth, this vulnerability is not unique to the smart grid, but the degree to which this vulnerability is exploitable varies within different implementations of a smart grid for the U.S., and as such should be taken into consideration.

Defenses

Many researchers have studied the ways in which the smart grid and its data can be securely stored and transmitted (Ali 169). To protect data, general solutions include the use of firewalls, the encryption of messages, the avoidance of insecure protocols, and the avoidance of authentication weaknesses (Ali 179). However, as we know, an attacker needs only one entrance for a system to fail, and as such it is necessary to implement additional mechanisms to protect the privacy of consumers, and the privacy of the United States, should information regarding smart meter and demand response system data be released.

Once such mechanism uses noise to dilute the data sent between smart meters and the smart grid, hiding individual consumer loss within a sea of irrelevant information. This decreases the likelihood of an attacker's ability to extract individual consumer data should it be leaked (Pohls 82). Additionally, the transmission and delivery element of the smart grid system could be more adequately protected, with better physical security for substations and more rigorous attempts to protect the location of these substations.

Conclusion

The electric grid infrastructure is so complex and interconnected that at times, it is difficult to prioritize all aspects of security, and by extension, privacy. Due to the dubious nature of the U.S. governments' privacy policies, it is easy to place the privacy concerns on the consumer level under the umbrella of "national security." However, it is crucial to remember that when pooled together, smart meter and smart grid data show a great deal of information about the American people, economy, and energy infrastructure. While individual consumer privacy is important, the electric grid infrastructure courses through the veins of this country, and is crucial to its continued success; as such, it is essential to consider the financial, national security, and individual repercussions of the leakage of grid data. As we move towards complete adoption of the smart grid, this data becomes easier to access, and the security and privacy implications become close to coming to fruition. Therefore, we must focus on equating security to privacy during the development of the smart grid.

Supplemental Material

Since this paper is relevant not just to engineers and computer scientists but also to policymakers and consumers, this paper is accompanied by a more digestible informational video concerning this topic. Link : http://youtu.be/BM1Y2fF_EYU

Works Cited

Ali, A. B. M. Shawkat, ed. *Smart Grids: Opportunities, Developments, and Trends*. 2013 edition. London: Springer, 2013. Print.

Aloul, Fadi et al. “Smart Grid Security: Threats, Vulnerabilities and Solutions.” *International Journal of Smart Grid and Clean Energy* 1.1 (2012): 1–6. Print.

Barker, Sean et al. “Smart*: An Open Data Set and Tools for Enabling Research in Sustainable Homes.” *SustKDD, August* (2012): n. pag. *Google Scholar*. Web. 24 Nov. 2014.

Flick, Tony, and Justin Morehouse. *Securing the Smart Grid: Next Generation Power Grid Security*. 1 edition. Amsterdam; Boston: Syngress, 2010. Print.

Larson, Rodney L. “Communication over Power Lines.” 19 Sept. 1995. Web. 11 Dec. 2014. Makansi, Jason. *Lights Out: The Electricity Crisis, the Global Economy, and What It Means To You*. 1 edition. Hoboken, N.J: Wiley, 2007. Print.

Murrill, Brandon, and Liu, Edward. “Smart Meter Data: Privacy and Cybersecurity.” N.p., n.d. Web. 24 Nov. 201104.

Pöhls, Henrich C., and Markus Karwe. “Redactable Signatures to Control the Maximum Noise for Differential Privacy in the Smart Grid.” *Smart Grid Security*. Ed. Jorge Cuellar. Springer International Publishing, 2014. 79–93. *link.springer.com*. Web. 11 Dec. 2014. Lecture Notes in Computer Science.

Rottondi, Cristina, Simone Fontana, and Giacomo Verticale. “A Privacy-Friendly Framework for Vehicle-to-Grid Interactions.” *Smart Grid Security*. Ed. Jorge Cuellar. Springer International Publishing, 2014. 125–138. *link.springer.com*. Web. 11 Dec. 2014. Lecture Notes in Computer Science.