Protecting the Grid in a Smart-Grid Environment

Parker Soares
NET-150-01: Network Fundamentals
Professor Jason Reeves
April 24 2021

The world has become increasingly dependent on a reliable, consistent source of electricity as humanity moves further into the technological age. The electric grid infrastructure implemented in the United States has been struggling to meet the rapidly growing demand for power, and because of this the nation is moving towards the smart grid environment. The goal of turning the power grid into a dynamic network which utilizes sensory technology and two-way interactions not only creates opportunities for efficiency and productivity, it also threatens the security of energy companies and ultimately the availability of electricity across the nation. It becomes necessary to ask- "What needs to be done in order to protect the smart grid, and how can cyberattacks in this context be responded to?" In order to mitigate attacks on the smart grid and ensure a more secure environment, protocols, policies, and standards must be implemented. Through the examination of energy policy, interoperability standards, and anticipated issues, the goal of a more secure smart grid becomes attainable.

Before focusing on the strategies used to mitigate cyberattacks on the smart grid, it is vital to first understand the history of the traditional electric grid and define the smart grid. "Our current electric grid was built in the 1890s and improved upon as technology advanced through each decade" (Smart). According to smartgrid.gov, the current electric grid is not going to be able to keep up with the energy demands that arise as a result of advancements in technology. "...we are stretching its patchwork nature to its capacity" (Smart), and this is not sustainable as the world continues to expand the boundaries of technology. The proposed solution is the smart grid, which introduces superior monitoring capabilities for providers and helps mitigate issues including blackouts or brownouts (grid). Data would travel in both directions, towards the consumer and the producer, providing opportunities for advancement but also introducing additional security risks.

In order to address these security risks, in July of 2010 The House of Representatives held a hearing on Smart Grid Architecture and Standards. This hearing addressed the National Institute of Standards and Technology (NIST) developing what are known as "Interoperability Standards" for the smart grid (Wu). In the hearing, these standards were defined as follows: "It helps identify where information exchange needs to take place between devices and networks to meet the functional requirements of the system" (Wu).

These interoperability standards are crucial to the development and deployment of the smart grid due to their widely interconnected nature. Because the traditional power grid is a combination of "Federal, State, and private-sector stakeholders," there needs to be a set of guidelines to ensure cooperation (Wu). In the context of cyber security, policy is necessary in order to hold parties accountable, and in networking interoperability is necessary to ensure accessibility. Both cyber security and networking rely on clear guidelines, and these standards provide organized guidelines which need to be followed by all involved parties related to the smart grid.

It is not uncommon for policy to face scrutiny regarding its effectiveness and completeness. Richard J. Campbell is a specialist in energy policy who published a report in 2011 regarding the smart grid and cyber security- with a focus on the issues surrounding the regulatory policy put into place. His work sought to address additional challenges faced by securing the smart grid, and highlights the need for amendments. The most prominent concern voiced by Campbell was regarding how security policy is defined, and the limitations that places on the overall security of the smart grid:

> While reliability standards are mandatory, the ERO process for developing regulations is somewhat unusual in that the regulations are essentially being

> established by the entities who are being regulated. This can potentially be an issue when cost of compliance is a concern, and acceptable standards may conceivably result from the option with the lowest costs. (Campbell)

In the interest of context, the Electric Reliability Organization (ERO) enforces said reliability standards as was defined in Campbell's summary.

Campbell's critical analysis of the energy policy surrounding the smart grid sheds light on the complexity of securing something so vast that it covers the nation. With so many points of entry, a network of this size will inevitably contain numerous vulnerabilities, and if weak points aren't reinforced with proper security policy it only increases the threat of a cyber attack. Having a comprehensive policy is a daunting task, and the more people there are working on the policy the stronger it will theoretically be.

Campbell's work is beneficial with regard to addressing the complexity of the issue, however it does not address a detailed solution. Christopher Bosch has a more comprehensive overview of the smart grid, beginning with the grid evolution and ending with a resolution to the issue of securing the smart grid. Bosch proposed that NIST be given the capability to establish standards for all members of the smart grid.

> Having identified and analyzed these fundamental communication building blocks, NIST can regulate from a position of substantive knowledge in setting security requirements for Smart Grid communications with a focus on these fundamental blocks, allowing for a regulatory system that is applicable to diverse business models. (Bosch 1402)

This proposed solution would standardize and stabilize the security of the smart grid, and allow the ramifications of the previous policy to be exposed as the nation works towards a solution.

Through the examination of proposed policies, professional critique of said policies, and potential solutions to various implementation issues, the question of what needs to be done in order to protect the smart grid and what responses to cyber attacks would look like can be answered, to a degree. The implementation of networking on a massive scale requires the implementation of robust policy, and security must live at the heart of that policy. Once that concept is understood by those involved, the goal of securing the smart grid can be reached.

Works Cited:

Bosch, Christopher. *Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards*, 41 Fordham Urb. L.J. 1350 (2014).

Campbell, Richard J. *The Smart Grid and Cybersecurity- Regulatory Policy and Issues*. CRS Report for Congress, R41886, Congressional Research Service, 15 June 2011, https://fas.org/sgp/crs/misc/R41886.pdf.

"Grid Modernization and the Smart Grid." *Energy.Gov*, https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid. Accessed 25 Apr. 2021.

"The Smart Grid." *SmartGrid.Gov*, https://www.smartgrid.gov/the_smart_grid/smart_grid.html. Accessed 5 Mar. 2021.

Wu, David. *Smart Grid Architecture and Standards: Assessing Coordination and Progress*. U.S. Government Publishing Office, 1 July 2010, https://www.govinfo.gov/content/pkg/CHRG-111hhrg57602/html/CHRG-111hhrg57602.htm.