Smart Grid Security—Attack and Defense Strategems

Wasfi Momen
CSC 6222
Department of Computer Science – Georgia State University
Atlanta, Georgia
wmomen1@student.gsu.edu

I. Introduction

The focus of development on the Smart Grid is filled with challenges of security and privacy. Attackers can use old and new attacks in order to infiltrate the realms of the Smart Grid. In this paper, we seek to understand definitive attacks and their defenses in order to better view what the current research has produced and where it needs to improve to create a power delivery system capable of securing users and their data.

II. Background

To understand the research going into the Smart Grid, a quick overview of the standards, concepts, and history of the system are required. Previously, requirements for services like natural gas, water purification, and electricity generation escalated during the 1960s along with technological innovations in both engineering and computers. This in turn produced the first generation of Supervisory Control and Data Acquisition Systems, or SCADA for short.

SCADA has developed through generations of improvement with new technology. These distributed systems used a mixture of mechanical and command line interfaces. The modern-day distributed, networked, and IoT SCADA systems of today still run on the protocols that run on TCP/IP traffic. Ethernet encapsulation remains as the outermost header with cyclic redundancy checks. However, there is a significant difference in the innermost application layer. Today, most current protocols that make up the application layer in the power grid are limited to three protocols: BACnet, Modbus, and DNP3. All of these protocols were built for interoperability instead of speed or security. They were made to communicate over RS-232 cables initially but now support Ethernet Cat5.

In the past, companies used to make their own in-house protocols and there were issues with compatibility between protocols. BACnet and Modbus became the biggest protocols out a series of corporate acquisitions, but unlike other standard protocols like Bluetooth the companies still continued to provide insecure protocols that remain in SCADA systems today.

Most modern-day SCADA systems include Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). These devices control the machines running on the industrial plant based on current and past data readings. Other computers placed either on or off-site delegate instructions to PLCs and RTUs in order to meet the supply and demand of the plant. SCADA systems also include data historian and logging servers that serve to track production of the plant and calls to services.

Regulations on SCADA started occurring once international security considerations demanded a response for safe, controllable environments. In the United States, the bureaucracy tied to development of standards for SCADA is the National Institute of Standards and Technology or NIST. Along with the current technological trends of the modern day and the need for a new power infrastructure, the world asks for a brand-new power grid connected not only by copper lines and steel transformers, but also by network system concepts and protocols. NIST is now developing the standards for the new Smart Grid.

NIST separates the Smart Grid into several realms: power generation, distribution, transmission, service providers, and the end user. Each of these realms have their own set of problems and attack spaces that attackers can infiltrate and disrupt. The interconnected Smart Grid must remain resilient for these new threats, so by Executive Order 13636 the United States provides research grants to protect the realms of the future Smart Grid.

Note that in this paper we will consider the “top” of the Smart Grid as just the power generation and transmission

realms while the "bottom" will consider the distribution, end user, and service provider. It is an interpretation of the NIST standard, but not one that should be taken as hard fact.

Within the realms of the Smart Grid, we need to look at the areas of data production and consumption to see where the attacks occur. The SCADA core will compromise the main plant in the power generation realm. The power generation realm only considers data processes within the perimeter of the plant, so all of the computers and PLCs responsible for electricity generation fall here.

It is unclear in the NIST standard or any discussion around the Smart Grid where the trust zones for data calculations lie relative to each other. For example, the false data injection attack in section II of this paper includes assault on data calculation responsible for tracking variables produced by the end user. The question arises whether a computer in the main SCADA plant is responsible for calculation or if it is delegated to service providers as well. Normally, it'd be part of only the SCADA core, but the new technology of the Smart Grid would mean large calculations across a variety of distances that would need to travel to the main power plant. A distributed algorithm might work better in favor where calculations are conducted across nodes of the power generation realm, and as is shown in section I can even include machine learning as a part of analysis.

The bottom part of the Smart Grid consists of the power distribution, transmission, end user, and service provider. Power distribution and transmission will still go through regular transformers that step down the voltage transfer of electricity and do not generally need computers to handle operations. Meanwhile, the end user and service provider realms are the largest addition to the Smart Grid. These two realms will make use of the Advanced Metering Infrastructure or AMI.

The AMI is responsible for communicating metrics on power consumption and price electricity consumption throughout the realms. NIST writes the AMI into different networks that make up the realms of the Smart Grid. Networks are separated in names such as Home Area Network, Wide Area Network, and Local Area Network which connect up to the top of the Smart Grid. Each of them have their own relays and best-fit algorithms to provide communication.

Due to ubiquity of the AMI, it represents a large attack space for attackers to control and infiltrate. A large amount of the AMI controlled by an attacker will be able to complete shut down the Smart Grid as is proved in [7]. Today, the AMI is still an untested, insecure field. As mentioned before, protocols of the previous SCADA generation were only intended for interoperability, not security. We will see how this affects communication between the AMI and power generation realm in the following Smart Grid attacks.

III. Smart Grid Attacks

A. False Data Injection

In our first attack, we look both conceptual research and current impacts in violations of integrity. Integrity is defined as the manipulation of data either by a malicious adversary or an error-producing source that compromises the authenticity of information that can be gained from the data. In networks protocol design, some protocols use checksums or error correction codes in order to prevent or fix integrity violations. Unfortunately, only one power substation protocol, DNP3, gives any kind of integrity checking with checksums [5], but DNP3 is not as widespread as other, more insecure protocols like BACnet or Modbus. Today, most power substation setups utilize these insecure protocols as minimal as possible and only in machine-to-machine networks.

However, the Smart Grid aims to ubiquitous and secure across its realms. Therefore, new problems arise while implementing past-day solutions. An adversary might not have access to all parts of the Smart Grid, he or she can attack either at the top at the power generation realm or at the bottom at the distribution, end user, or service provider. Therefore, making use of either the top or bottom might compromise the other. By injecting integrity violations, the adversary can push incorrect data that will affect operations and lead to issues in power delivery service.

1) Integrity violation via calculations

With respect to integrity violations, Mrabet et al. [3] describe the *false data injection attack*. In the scope of the Smart Grid, false data injection is typically implemented at the bottom realms of power distribution, end user networks, and the service provider. By influencing the calculations on the metrics of power consumption, an adversary violates the integrity of the data and ensures a false result once the metrics reach to the SCADA core. Specifically, Liu et al. [7] give the calculation of state

estimation as describe by the linear regression model with z as the state variables that include end user metrics and H as the estimation matrix:

$$\vec{z} = \vec{H}x + e$$

By impacting values in z to find an attack vector, the estimation function H can be altered and produce a false result of the estimate. Liu et al. also debunk previously stated beliefs that an attacker would need a substantial probability to find an attack vector to compromise the network. In the experimental evaluation, the attacker only needs a 20 percent chance of random false data injections before the attack vector is found. A sample setup of this attack can be modeled by an attacker having access to a variety of RTUs or parts of the AMI such as a smart meter for a house. The formation of the state estimation for Smart Grids is primarily used as the basis for modeling an Intrusion-Based Detection System (IDS).

2) Integrity violation via hardware

Along with the manipulation of data via software inferred calculation, an integrity violation with easy accessibility to the attacker is found in the smart meter devices themselves as a part of the Smart Grid. An article written by reporter Brian Krebs informs of widespread hacking of smart meter devices in Puerto Rico [Krebs]. Puerto Rico is among one of many locations around the world that have implemented smart meter infrastructure due to natural disasters destroying the infrastructure. In Puerto Rico, some citizens have modified their smart meters to cut off metrics being sent back to the public power utility, PREPA. As a result, the FBI claims 400 million US dollars will be lost in the long term.

Halim et al. [4] give a review of various hardware hacks that can implemented on smart meters. Smart meter infrastructure, just like the rest of Smart Grid components, are still early in their development and deployment, but still ship with hardware vulnerabilities. First off, smart meters come without any encrypted or obfuscation of memory locations. Therefore, it is easy to get memory readouts via the pins connecting the devices and inject data to cause integrity violations. Another method is simply unplugging the meter's metric connection or placing a strong magnet on the meter—the technique used in Puerto Rico. No data at all still means disruptions of power consumption. Whole communities within the end user realm could use these techniques which are highly incentivized by the financial gain and highly accessible due to rise of a technology-savvy generation.

3) Preventing false data injections

By the Smart Grid's own interconnectedness, false data injection can cause widespread disruption in the network. As mentioned before, the calculation for state estimation is typically used for modeling an IDS. The solution proposed by current research involves various algorithms that try to decrease the number of false positives while maintaining true negative accuracy. Chen et al. [1] tries a machine learning approach that differs in the traditional statistical-based IDS. The authors formulate a consistent-inconsistent region to measure how much of a grid is reliable or not. Then, each state and its neighbor in a set is compared by trust-based voting to see if their state estimations are reliable. Finally, elements are targeted as "Good", "Abnormal", and "Unknown" if they fall into the consistency region or not.

In experimental evaluation, this method proved to produce false-positive rates two-thirds lower than the next best algorithm. It also provides configurable regions to let end users decide on how reliable they want the algorithm to perform. Various improvements can be made by strictly checking the "Unknown" components. According to the solution, "Unknown" components are caused when there is not enough data on state estimations to say a neighbor is reliable or not. Data-sparse regions in the Smart Grid are plentiful in more rural areas or places with poor data connection. If the solution is to be made for real-time correlation, some development in data-sparse areas should be considered, perhaps even utilizing data from the previous statistical-based models if applicable.

For the issue of hardware violations, it is representative of the more "security through obscurity" problem largely present in the current power generation grid. Mandatory requirement for future standard IEC 62056-21 should be implemented across the Smart Grid which includes simple passwords, encrypted passwords, and handshaking to smart meters. Future specifications of the standard should include higher cryptographic protocols. The meters themselves should be secured based on a minimal set of requirements to delay tampering or notifying the end user or power company.

B. Popping the HMI

Mrabet et al. [3] acknowledge the HMI or *Human Machine Interface* in the paper as part of the exploitation an attacker can use to gain access to critical systems in the Smart Grid. The HMI is defined as the mechanism for human interaction to the SCADA interface. In the past,

this used to relate to buttons and knobs of generation one SCADA via mechanical switches. However, today's generation and the future will utilize web browsers as the main HMI since they are well-supported and tested through everyday use.

Mrabet brings up the point that exploiting HMI vulnerabilities "does not require advanced networking skills or significant experience in security and industrial control system to perform" and puts the attack as a high severity, but then puts it as low probability for implementation which seems contradictory. HMI attacks high severity due to their ability to compromise confidentiality, integrity, and accessibility throughout the Smart Grid. However, the research for HMI attacks in SCADA and other components of Smart Grid systems only count to a few studies and therefore represent a blind spot for security.

Popping the HMI is a term used to relate attacks on the HMI interface. Any attacks on web browsers apply to the HMI of the smart grid system at all levels. Normally, attacks are part of an implementation of a library or system that the HMI requires. For example, most web browsers use OpenGL as the main shading language for users and files to gain access to the GPU functions to render content. While thoroughly developed and optimized, there are still some problems outside of actual software vulnerabilities. GPU operations have regularly timed I/O operations that can be captured and analyzed to see what the user was doing at the time. This timing aspect is what makes up one of the greatest threats to the Smart Grid.

1) Timing attacks on the HMI

While there are many different vectors of attack on the HMI, ranging from cross-site scripting to library substitution, we focus on timing attacks on the HMI that reveal what the system was doing at the time. The attacker's goal is reconnaissance of the target network topology in the Smart Grid. Specifically, the attacker wants to know which devices that are Type 1A/P2 that need a critical time delay of 3 milliseconds to conduct operations—these devices will be highly targeted areas of the network [10]. Over a large sample of requests, the attack will either divulge the target devices or give enough information to conduct additional attacks.

The procedure of the attack is nothing new to vulnerabilities of web browser development. Javascript and the loading of HTML and CSS at particular times by Content Delivery Networks give enough information to determine which web site a user is browsing, and since a user-agent string is sent via Content headers in HTTP the attack space narrows to specific browsers. The attacker uses a time statistic to base their measurements, sends some code to the target machine, and then sees how long the process takes.

Since HMIs are sold along with the machines that make up components of the SCADA core, fingerprinting browser can go down to the application level and development stacks of the power substation setup. For example, the Siemens WinCC HMI had a CVE (Common Vulnerability and Execution) that came from its Windows Server Version that required an update. Since Siemens HMI will be perform and execute at consistent times with caching and perform at different times relevant to other popular HMIs, the attacker has learned crucial and valuable information that can be now shifted into other aspects of the Siemens SCADA system.

2) Defense with Deterministic Browsers

Due to the potential of attacks, browsers built for security tend to reduce their fingerprinting as far as possible. The Tor browser, built on top of the Tor networking protocol, tells its users to always keep a low profile by keeping every aspect of the modern web browser in check. Tor has options to reduce screen resolution to keep with the most popular formats, disabling Javascript entirely, and, according to Wang et al. [10] even prevents timing attacks by adding "jitters to the browser clock".

However, mitigating attacks on the timing of web browsers has proven difficult with options becoming more distinct over time with the different hardware and software provided in the modern day. As mentioned before, SCADA systems will use the most supported web browser, but the Smart Grid SCADA core requires even more security. The *deterministic browser* provides a possible defense against timing attacks for web browsers of the Smart Grid.

Wang described the process of developing deterministic browser to defeat timing attacks. The deterministic browser produces a time based on the attacker's input so the attacker will get a different time than the actual time the process took to complete. The browser is constantly ticking time on the clock even if there are no process tasks to be done. The actual time the process takes is slotted inside a constant time window that

is resistant to timing attacks. Currently, Wang has built a custom build of Firefox named Deterfox that defends against timing attacks. Even over a large sample of devices, files, times, and popular websites, there was no useful information gained from conducting performance metrics. All operations seem to complete in constant time as seen by the adversary.

If adopted as a primary browser for the Smart Grid and researched further, the deterministic browser can become a new defense against a difficult attack. However, it should be noted that the Smart Grid should adopt other secure methods of HMI web browser interaction such as private VPN tunneling, secure HTTPS, and firewall configurations to not divulge information about target machines in plaintext.

The issues for the deterministic browser is the Javascript time execution. All operations conducted through Javascript calls have to be considered to predict the time the process will take and the resultant confusion for the attacker. Javascript and its now popular superscript Typescript will introduce new synchronous and asynchronous functions that will break compatibility with this deterministic browser. Also, any calls to the performance API in Javascript will break compatibility with the deterministic browser and revert back to regular true system time. Many HMIs might require access to these APIs and functions.

C. Privacy attack

In the Smart Grid, there are more than just computers controlling each realm. The advancement of technology has allowed for a wide range of new technologies in the last few years. Due to this, NIST and other proponents of the Smart Grid are providing a flexible, adaptable plan that will allow for new, unpredictable technologies to connect to the Smart Grid system.

However, attacks on the Smart Grid with these new technologies are not limited to security attacks, but privacy ones too. Privacy focuses on the compromising of information through means of linkage. Instead of focusing on the technical aspect of cracking cryptosystems, privacy researchers use networks of people to see whether people have a relationship.

In the *privacy attack* of the Smart Grid, the attacker uses the Smart Grid itself to divulge information about its users to compromise confidentiality and conduct reconnaissance. With modern technology, smart vehicles with electric power sources will be targeted as well as networks based around individual homes. Both forms of privacy invasion include aspects of Geo-Locational Privacy in which location provides a key aspect for the attacker to track on a person or device.

1) Tracking activity

As previously seen in the discussion about the deterministic browser, timing attacks have a significant factor when tracking the activity of devices within the Smart Grid. The same happens outside of a web browser to the smart meter. In [8], the authors theorize a model of privacy capture by making a procedure to track, wait, and analyze targeted meters to see what activities go on. This mainly involves a process where the attacker snoops information on the meter and see the changes of kwH used over time. Afterwards, a profile of devices that draw continuous power or only at peak times can be inferred and mapped. Plotting out the energy use over time provides a map of what a person does inside the building and significant tracking abilities to the attacker.

When correlated with other defining features common in privacy research such as gender, age, or weight, the energy profile of individuals is compelling data to sell to data brokers. [8] describe various privacy-invasive questions that could be answered through this method of attack. They also address the protections provided in countries that seem to not take the detailed reporting of the attack into account.

Another method of privacy invasion is the smart vehicle. The Smart Grid will almost assuredly take into account of smart vehicles traveling within cities in order to shift energy to and from the home and work place. As a result, the smart grid will track vehicles and their drivers in order to see which vehicles will probably stay or leave in power consumption areas. If an attacker gains access to the Smart Grid, individuals can be tracked via their vehicles' unique power consumption and cross referenced with other privacy variables like makes and models. The idea of tracking power usage from the home smart meter is now extended to a city-wide region.

2) Preventing privacy loss

Protecting the privacy of users can be done through the use of privacy preservation algorithms. These algorithms are built with an inherent tradeoff between privacy and utility of data, so data collectors and producers can control how much data is anonymized for levels of service quality. In the Smart Grid, this data protection should be

considered only for the bottom space of the end user and service provider since metrics for power generation and consumption should be accurate as to not cause unintentional data loss or even unintentional false data injection. However, future solutions should consider privacy algorithms for smart meters and vehicles.

In [9], smart devices report metrics to the service provider that are protected by differential privacy. Differential privacy means the values of the data are obfuscated enough so the data has the same probability of being one value as another. For example, a spike in power load has an equal chance of being either a computer being turned on or a fridge creating ice. Due to this probability, the attacker or untrusted data collector has no ability to determine useful information on the statistics of the power load.

In [11], the authors provide a privacy preserving algorithm for smart vehicles within a city-space. The process of the algorithm ensures that every vehicle has a set of pseudonyms and their location data that can be obfuscated with privacy parameters set by the user. By exchanging pseudonyms consistently, reporting back obfuscated location data by groups of neighboring vehicles, and providing defense techniques in regards to specific adversaries, the protocol can deter privacy and utility loss until a significant amount of vehicles are deemed unsafe to exchange pseudonyms with.

While both of these approaches have the benefit of providing the user with privacy guarantees and the data provider with utility guarantee, it will have an affect on the SCADA core of the Smart Grid. As privacy-utility tradeoffs decrease with the increase of records within the system, an attacker with nation-state resources could use the privacy preservation against the Smart Grid. Even with the solution proposed by Chen et al. that provided a parameter to control the rate of false positives, that value scaled with a privacy parameter would eventually compromise the Smart Grid system.

At least with regard to the power generation realm, a better implementation of privacy preserving algorithms are required to find a balance between not only privacy and utility, but false positive rates in IDS as well. A privacy preserving algorithm that takes into account privacy obfuscation and state estimation will be a contender for the Smart Grid.

IV. Conclusion

With the ongoing development of the Smart Grid, multiple considerations must be taken into account for both old and new threats. Looking at false data injection reminds of the previous era of Modbus and BACnet where unencrypted communication played a huge role in the idea of the Smart Grid. By following standards and adopting new IDS's with modern technology we can prevent calculations for power consumption and production from being incorrect. The HMI as a primary issue across the realms of Smart Grid security is now solvable with the creation of the deterministic browser. However, the one thing the Smart Grid needs to focus on is the privacy of its data and users. With the interconnected Smart Grid and new technology innovations, the security of the power grid can be assured from the bottom to the top.

References

[1] Cao, Y., Chen, Z., Li, S. and Wu, S. (2018). *Deterministic Browser*. Available at: https://arxiv.org/abs/1708.06774

[2] Chen, P., Yang, S., McCann J., et al. (2018). Detection of false data injection attacks in smart-grid systems - IEEE Journals & Magazine.

[3] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). *Cyber-security in smart grid: Survey and challenges.* Computers & Electrical Engineering, 67, 469-482.

[4] Halim, F. Yussof S., and Rusli E. (2018). *Cyber Security Issues in Smart Meter and Their Solutions.* IJCSNS International Journal of Computer Science and Network Security, Vol.18 No.3, March 2018

[5] Ken Curtis. *A DNP3 Protocol Primer*. (2005). DNP3 Primer, Revision A, 20 March 2005

[6] Krebs, B. (2017). *FBI: Smart Meter Hacks Likely to Spread.* Available at: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/comment-page-1/

[7] Liu, Y., Ning P. and Reiter, M. (2011). *False data injection attacks against state estimation in electric power grids*. ACM Transactions on Information and System Security, Vol. 14, No. 1, Article 13, Publication date: May 2011.

[8] Quinn, Leake, *Privacy and the New Energy Infrastructure* (2009). Available at SSRN: https://ssrn.com/abstract=1370731 or http://dx.doi.org/10.2139/ssrn.1370731

[9] T. T. Nguyˆen, X. Xiao, Y. Yang, S. C. Hui, H. Shin, and J. Shin. *Collecting and analyzing data from smart device users with local differential privacy*. arXiv:1606.05053, 2016

[10] Wang, W. and Zhuo, L. (2018). *Cyber Security in the Smart Grid: Survey and Challenges.* Computer Networks: The International Journal of Computer and Telecommunications Networking. Volume 57 Issue 5, April, 2013. Pages 1344-1371

[11] Yu, R. (2016). *MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks* IEEE Transactions on Dependable and Secure Computing. Vol. 13, No. 1, January/February 2016.