Cyber Security of the SMART Grid

Katherine Sugely Arriola

What is the Smart Grid according to Google definition is the electrical supply network that uses digital communications technology to detect and react to local changes and usages? Smart Grid increases power reliably, availability and efficiency that work contribute to the economic and environmental factor. There are benefits to using the Smart Grid such as improved efficient transmission of electricity, quicker restoration of electricity after power disturbance. Improved integration of customer owner power systems, including renewable energy systems. (United States Department of Energy, n.d.)

Coals and fossil fuels have been used by power plants to produce the electricity we use every day the gird is a network of power lines and substations that delivers electricity from power plants to homes and businesses. The modern grid usually depends on one main power sources which don't provide enough detail information on usage which will make managing electricity. the most common solution was to build more power plants. In attempts to improve sustainability by decreasing the use of fossil fuels by implementing that Smart Grid. The Smart grid will provide sensors and software to the existing grid that will give utilities information and understand and follow proper procedure to react immediately. For instance, if there is physically damage to a power line due to a natural disaster. (EPCEenergyeducation, 2011)

The software would detect and reroute the power around the problem area. There is also a financial benefit to the smart grid. The price of electricity changes throughout the day but this will not be seen on current meters on the homes. The price of electricity depends on the time of day. It usually more expensive doing the day and cheapest during the night. When the smart meter s installed certain appliances can run when power is cheap. This will give customer more control of the energy bill.

To avoid blackouts, the smart grid will be incorporated various sources of energy production to build resilience and allow for easily scale electricity. In the traditional grid, solar and wind energy are difficult to integrate due to antiquated. There is the need to upgrade transformers on the grid to allow for two-way energy distribution, consumers who unitized solar and wind energy can potentially sell energy back to the gird, keeping track of the electrical distribution to the grid through metering. The smart grid also outperforms the traditional electric gird in the ability to rapidly troubleshot and remedy power outages. (O'Connor, Nicholas, Nakamura, & Kaczmarek, June)

The smart grid also way various methods of renewable energy power generation can be distributed by across multiples sources so the system is more stable and efficient. The smart grid is a quality focused project. In the future, there will be a delivery of quality power necessary. To be free of spikes, disturbances and interruptions. To enable real time communication between the consumer and utility so consumers can tailor the energy consumption and to be resilient to attach as its becomes more centralized and reinforced by improving smart grid security protocol. (Energy, 2007) .

Cybersecurity is the state of being protected against an intruder. This intruder can include unauthorized and/or criminal use of electronic data. It is in means to take measures to such an attack. Now that there is a definition, there needs to be a reason. Why would someone have the motive to hack a power grid. Some of the reason may include, however are not limited to gain control of smart grid, collecting valuable data of the grids functions.

As we study about the increasing efficiency of the Smart grid there must be a discussion about the protection of the smart grid. (Pillitteri, 2016) There needs to be advance the development and standardization or cybersecurity including privacy, polices measures, procedures, and resiliency in the electric smart grid by 2016.

Cyberspace is an underlying infrastructure are vulnerable to an attack. The vulnerability of cyber space is not just limited to computer and other typical handheld devices. As time goes on technology is increase integrate with physical infrastructure operations thus leading to increased risk for physical infrastructure operations and high consequences of possible attacks to the complex network.

When the topic of Cybersecurity and the Smart grid comes up there are mixed conceptions of what it. For instance, we need to think of the process of how to smart grid works. It appears engineers are focused on the development of the grid in terms improving economic and power distribution. However, as the development of the grid takes and place even along Electrical Engineering course taught at Universities. Another reason why cyber security of the smart grid is due to the idea that its already safe. The question should be why this topic is not commonly discussed and who and why would someone have the desires to hack or to damage a system like the smart grid.

These are the common reasons why the Smart grid is at risk just as any other system. There are the reasons why some would consider attacking the smart grid system. There are non-malicious attackers who desires to view the security and operation system as a puzzle to be cracked or are curious of how the system works and want explore for personal curiosity. Many hackers are normally driven by the academic, intellectual challenge and curiosity. Another person to hack will be a consumer driven by vindictiveness towards an organization or another consumer and attack the smart grid to figure is to shut down their home's power.

They can be attacker with terrorist intent and who views the smart grid as an attractive target as it affects millions of people making the terrorist cause more visible. There could be employees disgruntled on the utility/customers or ill trained employees causing unintentional errors. It also can be competitors attracting each other for the sake of financial benefits and potential monetary gain. The reason the smart grid is prone to attacks dur to the smart grids ability increased communication capabilities make it more vulnerable to cyber-attack. The smart grid is a critical infrastructure, all vulnerabilities should have identified and sufficient solutions must be considered to reduce the risk to an acceptable sure level. (Smart Grid Awareness, 2015)

As previously discussed the smart grid is seen as a fundamentally change the electrical grid from the centralized utility-centric gird to a distributed consumer-centric gird. The growing amount of attacks on electric grid by cyber-attacks are slowly growing. There are several documented events. For instance, in January 2003 a computer worm infected a computer network at the David-Besse nuclear power plant in Oak Harbor, Ohio. This lead to the to the disabling a safety monitoring system and the plants process computer for several hours.

In August 2003, the alarm processes of FirstEnergy were prevented monitoring of the grid and as several transmission lines tripped for various reason. This failure caused in disabling power plants through various reason eventually lead to an extended black out. There was an incident in August 2006 the circulation pumps at the Brown Ferry nuclear plant in Alabama failed because of excessive traffic on the control system network. There was investigation later that year revealed that the hackers were able to penetrate the plant's control system and to steal power by hacking into the smart meters than change the power consumption reading. Along with that discovery Phishing incidents were also detected at an electric bulk provider and malware samples were detected that indicated a targeted.

As there is a reveal about the rise of cyber-attacks there is also an increasing concern on security. It's clear that Smart grids consists of a complex network of sensor, monitors, devices and computer for data collection and analysis. Both engineers and analysist have identified the major challenges faced of computerized security systems related to smart grid. This includes the high volume if sensitive customer information, distributed control devices. This leads to a lack of physical protection, weak industry standards and there are also large number of stakeholder who depend on the smart grid.

There is also a concern of smart grid security as with typical systems are confidentiality, integrity and availability. The confidently entails protected both consumer and operation data integrity. It also required both at the consumer level for metering and billing and at the operational level to ensure stability of the gird. It's clear that the smart gird faces the same security challenges like any other complex computer network and security. One of the first major cyber- warfare attach that attacked a critical infrastructure in the country by using the worm. The delivery of the infection started via USB drives of nuclear inspectors.

There might a be a question on whether the SCADA systems are designed with inadequate security; or instance some organization used hard coded passwords are often pre-coded and never changed from the original settings. (Hong & Goel, 2009)

To think about the cyber security aspect of Smart grid one need to dissect about what makes the smart grid itself. The Smart grid is a complicated system. The smart grid system includes distribution systems, smart metering, and appliances. Each of these devices created and manufactured different vendors. Each of those components contain many layers of connections with different kind of functions. (Chan & Wong, 2015)

The smart grid is a wide and complicated system. It is a combination of devices related to energy resources, distribution systems, smart metering, appliances and more. These devices were developed and manufactured by different vendors, with multiple layers of connections with different kinds of proprietary or open standard protocols used for communication between these devices. Although security measures such as industrial grade encryption or multiple levels of authentication could be employed, they are not the only target of hackers. (Chan & Wong, 2015)

It is argued that there is strong security such as the security measuring the industrial grade encryption. There is also the monitorization of each compete to make sure it is up to standard to support the smart grid. However, hacking is a creative art form and hackers are trained find the weakest and most vulnerable point of a system. This is usually the part of the system that most engineers and manufacture do not consider.

This is a concern as when engineer's discuses about the smart grid. They talk about increasing efficiency and the economic benefit. But there is not an open discussion about the cybersecurity and the possible weak points of the smart grid. There can also the argument that the major and most important components of the smart grid According to Chan and Wong:

"*Traditional cyberattacks are attempts made by hackers for sabotaging computer systems and networks, and they are in a different domain from the power grid. However, if it is possible for hackers to alter the expected behavior of a power system or compromise sensitive information, minor consequences would incur instability of demand-response systems, while major catastrophes could be financial losses, physical destruction to the power systems and even human injuries.* " (Chan & Wong, 2015)

This leads to the argument that because of the lack of discussion from engineers about the risks of the smart grid being hacked. To gain a better understanding of possible cyber-attack as we must consider the possible threats and their propriety.

Is the most commonly known threats and is an umbrella term for a malicious software designed by hackers to run a target system. Some of the most common forms of malware include worms, spyware, Trojan horse. The most common malware that can potentially be used to attack a sophisticated system like the smart grid is Stuxnet. Potential hackers can use Stuxnet to attach certain components of the grid. Such as the industrial supervisory control and data acquisition.

SCADA is a system that is used to monitor and control a plant and the its equipment's. If there is damage to the SCADA, the grid will not be able to detect any damages or carryout out the necessary actions and control. This well lead the Smart grid to become more vulnerable. This potential treat may happen in industries such as waste management/control, oil and in this case electrical energy the smart grid. The Stuxnet computer worm and cyber weapon that is claimed to created jointly by the United State and Israel. However, no nation or organization

had officially claimed responsibility. Threats using this malware started in June of 2010 a 500-kilobyte computer worm that infected industrial site in Israel.

One of the reason worm is so threating to the power grid is that it doesn't require a complicated process to install it. It usually takes an unwitting victim to install it. Once the cyberweapon is installed its wine and often over a computer network. For instance, a employee can simply install to using a USB. Once the worm is installed it starts to infect all the machines. It does so by brandishing a digital certificate that seems to show that it comes from a reliable company.

The cyber weapon is able to evade automated-detection systems. The Stuxnet worm then checks whether a given machines are part of the targeted industrial control system are deployed in Iran to run high-speed centrifuges that helps to enrich nuclear fuel. If the system is not a target, Stuxnet does nothing: if it is, the worm attempts to access the internet and download a more recent version of itself. The worm then compromises the target system's logic controllers exploiting "zero day" vulnerabilities software weaknesses that haven't been identified by security experts. In the beginning, Stuxnet spies on the operations of the targeted system. Then it used the information it has gathered to take control of the centrifuges, making them spin themselves to failure. It then sends a false feedback to outside controllers, ensuing that they won't know what's going wrong until it's too late to do anything about it. (Kushner, 2013)

Another method hacker can attack the system is damaging the programmable logic control of the grid or the PLC. This cyber weapon is used for such action. The reason behind attacking the PLC of the gird. The PLC is the industrial digital computer which is the typically used in many machine industries. The PLC is machine has input line that are connected to sensors are connected events taking place within the system. It performs many functions which includes but it is not limited to executing the control instructions contained in the user programs. It communicates with the devices of the grid, this includes programming devices, Networks and over PLCs.

Another method of attack, advanced persistent threats are another common form of hacking. It's a method usually done on by professional hackers use to target a system continuously over a long period of time. This technique includes using malware social engineering and custom made exploits. Advanced persistent threats are attack carried out usually by a group with the capability an intent to persistently target a specific entity undercover. (Skopik, Friedberg, & Fiedler, 2011)

As previously mentioned some attacks can be done with non-malicious intent. The method of using APT is a common method for intellectual curiosity for how a system works. A curious hacker will want to enter the system and be able to observe how the system and work. The benefit of APT is that it can be limited to a mission for observation. However, this method give hacker more option on what they want to do once the gain access.

Since this method is not a method of an immediate attack rather a long term its designed to remain undetected as long as possible. This will makes detecting and combating this attack

even more difficult and will potentially take more time and resources to reverse the damages. Again, the most common section of the smart grid the hacker using this method by taking control of the supervisory control and data acquisition domain.

This method can be combined with Zero day, Stuxnet and Distributed Denial of Service. The attacker usually tries to intrude into the web server which enables SQL injection. This kind of attack gives the intruder elevate permissions and the chance to take over the web server for his own purposes. They usually take the intrusion detection system. The object is to gain ongoing access to target system. The APT attacker often used spear fishing a type of social engineering to gain access to the network through legitimate means and once access has been achieved the attacker establishes a back door. These mean hackers can install fraudulent utilities.

After gaining the initial access to the system, the hacker gather valid and personal user information. Then the hackers create a ghost infrastructure for distributing malware that can remain hidden in plain sight. As previously mentioned Apt are often extremely differ cult to identify in plain sight, the action of theft of data can never be complete hidden. A method to detect any anomalies in outbound data is the best way for an administrator to discover that his networks has been the target of APT attack.

Another method of as cyber hack that can be done is a denial of services attack. The attacker is trying to prevent legitimate users from being able to access the information of services or to use the service. This is done by targeting the computer and the network connection or the computers and network of the sites the users are trying to use, an attacker may be able to prevent you from accessing email or other services that rely on the affected computer.

The technique can be done by flooding a network with information. A common example is when someone types s URL for a particular website into your browse you sending a request to that sites computer severe to view the page. The sever can only take a certain number of requests at once, so if an attacker overloads the sever with the requested of the service, since you cannot access that site.

What was previously stated it how the process would take place for the standard personal computer and how the attacker would act on it. If someone were to attack the smart using the same technique the process would be executed differently. DoS attacks disrupting the Interest traffic, so as the increasing usage of power grid systems of DoS attack to the grid infrastructure causing a major power failure becomes quite possible.

Distributed denial of service is when the attacker can use your computer to attack another computer. It's by taking advantage of security vulnerabilities or weaknesses. An attacker could take control of a computer. The attacker will then force the system to send large amounts of data to a website or send spam to particular email addresses. When the attack is distributed because the attacker is using multiple computers and launch. (McDowell, 2009) the denial of service attack.

In the case of the smart grid the object would be to bring down a large portion or even he whole targeted network. DDoS attacks exploit numerous attacks sources, spreading using

multiple hosts which effect amplifies the attack power and makes defense more complicated. DDoS presents vulnerabilities.

In vulnerability attacks, malicious packets exploit network protocol and application fault that exists at the target network. The malicious packets exploit vulnerable software installed at the target network. The malicious packets exploit vulnerable software installed at the target host, trigger hosts, triggering excessive CPU utilization increasing memory demand halting the hots operations or other general systems breaking.

It will allow vulnerabilities may allow an attack and penetrate a system get access to control center and modify the load conditions to destabilize a critical infrastructure in unpredictable ways leading to serious results or disaster for example brownout or even a catastrophic blackout. (ASRI, Satin and PRANGGONO, Bernardi, 2015)

A zero-day attack is an unpatched computer system vulnerability that is not yet disclosed to the public. The vendor of the affected computer system having zero days to fix it after the vulnerability has been disclosed. This security hole is then exploited by hackers before the vender becomes aware and hurries to fix it. It refers to the unknown nature of the hole to those of the hackers, especially for the developer.

The treats of malicious attacks against the security of the Smart Grid infrastructure cannot be overlooked. As the smart grid is expanding nature of the smart grid user base implies that a larger set of vulnerabilities are exploitable by the adversary class to launch malicious attacks. There is currently extensive research had been conducted to identify various threats against the Smart grid and to propose counter-measures against these potential attacks. As it was previously discussed it can be concluded that that most common compensate of the smart grid the hacker tend to take control of are the following: The Supervisory Control and data Acquisition, the Smart Meter attacks and the Physical Layer attacks.

According to the National Institute of Standards and Technology, there are three standard cybersecurity for the Smart Grid which area availability integrity and confidentiality. There attacks the compromise the standards: Denial of services and distributed Denial of services. As mentioned the objective of such attack is to diminish the availability of the Smart grid by preventing messages delivery between the Smart Grid devices.

Identifying spoofing attacks allows the hackers to impersonate authorized Smart Grid users. Network spoofing are examples of identity spoofing attack includes Password guessing, social engineering dictionary attacks and sniffing. Eavesdropping attacks affect data confidentiality of the Smart gird communications channel through sniffing of IP packets on the intercepting wireless transmission on the home area network. This intrusion happens when an illegitimate user gains access to a cyber -system and obtain unwanted access to critical back-end servers.

The way the smart grid considered a risk for a cyber-attack is complicated in terms of the various ways it could happen. There is a concern about how can affect those who are in

working in the smart grid but also the clients who directly benefits from smart grid. This should be considered when stopping a cyber-attack and most importantly preventing it. Some common examples of such attacks are: switching off the device, jamming communication channel, Denial-of-Service against domain name servers (DNS) at the corporate network, and spoofing. This may disabled in a smart meter, it is possible to invoke a remote switch off request, to demand a smart meter be shut down. Consequently, the household electricity usage is unreported until the smart meter is restarted. Jammed communication channels will have similar consequences as the previous attack. Modifying the secret keys stored within a smart meter will prevent decryption of secure messages transmitted by the meters to the data concentrator units and end-servers.

One of the methods is to reconfiguration/resetting to remove the traits of the malicious attacks, including secret key resetting, and replacing the actual effected device. The privacy of user data is the most important concern in the smart grid.

The electricity usage pattern of a given household may lead to disclosure of several sensitive parameters; consumer habits (invariably sellable to marketing and spam operators), whether the consumer is at home or away traveling. Such information can expose information to competitors of the utility service. The competitors of course will use this information for their benefits

An attack against a smart meter's integrity takes place when legitimate data of the smart meter is tampered with, replaced, or deleted, before its transmission to the data concentrator unit of a neighborhood area network. The data is manipulated by the adversary either locally I for instance within the victim's computing resource or memory, or remotely through forging/injection/deletion of messages. Cyber security should be seen and is the essential element of the smart grid. It includes the protection needed to ensure the confidentiality and integrity of the digital overlay which is part of the Smart Grid.

The adversary may inject fictitious data into the smart meter communication channel to either portray increased electricity consumption of a household, or to reduce it. In both cases, the loss is bore by the legitimate end-users and/or the utility provider. Message replay attacks may be launched with one of two intentions. The utility provider may receive the same smart meter readings from a household, as previous ones.

As a result, the increased usage of electricity of a household may go unrecorded. Similarly, a forging attack to reduce the reported electricity usage data from a household may benefit the end users, at the cost of loss to the utility provider. Several techniques exist to reduce the effect of smart meter integrity attacks. The most common approach being to generate and maintain secret keys of reasonable length (based on current technological trends) between the sender and receiver of the electricity usage data.

Such an approach will help ascertain that a message authentication code (MAC) will verify the message integrity at the receiver's end. Availability A smart meter is also vulnerable to attacks against its continuing availability.

For all three scenarios, the availability of the smart meter is affected. For instance, a compromised smart meter may transmit an incorrect reading to the utility provider, and claim to have not done so. If the smart meter is using a secret key for data encryption, non-repudiation is enforced inherently, as no other entity is expected to possess a copy of the same secret key. On the contrary, the lack of a secret-key based mechanism will burden identification of such an attack. A common reason for attacks against the smart meter is manipulation of the meter configuration. The meter must therefore be secure enough to withstand both hardware as well as software-based attacks, that attempt to modify its configuration.

The can effect an area that is supported by line a metropolitan city large-scale deployment of smart meters (Number of smart meters = Number of households), in a metropolitan city, demand enough security, to prevent a large-scale catastrophe through such attacks.

Security measures must be considered at all protocol layers and the Time critical messages must be protected through a deployed security mechanism, and 3) All wired communication paths must be leveraged to strengthen security of the wireless communication networks. The authors identify threats against the SDG from the wireless channel as follows: 1) Jamming, 2) Eavesdropping by nodes from outside the channel, 3) Eavesdropping by malicious nodes.

Secure protocols to prevent inside attacker's A detailed analysis of the physical layer attacks is as the following the action of Eavesdropping includes spying on the wireless signals are carried in open space, and are susceptible to eavesdropping by an adversary. Sensitive information from a smart meter can easily be observed, and assessed through such an attack. Low-cost eavesdroppers exist in the market, to convenience launch of such attacks. Data encryption is an approach towards protecting sensitive information from revelation to the adversary. However, if a certain pattern is depicted by the transmitted data, an intelligent adversary may still be able to decipher the message content. For instance, if a household is unoccupied, the electricity usage will dwindle. If the smart meter is programmed to communicate with the data concentrator unit only when a certain threshold of energy usage is crossed, or if the message length to be transmitted is directly proportional to energy consumption, then a pattern of activity of the household may be construed. Jamming Method is used in DoS attack the goal of this attack is to prevent the smart meters from communicating with the utility provider, through jamming of the wireless medium with noise signals. Such attacks can be classified into two types: Proactive jamming, where in the jammer can emit noise signals continuously to completely block a wireless channel, and Reactive jamming, wherein the jammer first eavesdrops on the radio channel and launches the attack only when signals are sensed on the channel. As a result of such an attack, the legitimate smart meter can be affected into two ways: the channel will be tagged as "busy" for any carrier sensing done by a legitimate smart meter, and the smart meter may be prevented from receiving packets.

targets a multi-user access channel, and the attacker sets its own back off timer to be very short in length, so that the channel prioritizes access to the adversary each time it wishes to communication, denying access to legitimate smart meters of the smart grid.

The reason why this topic was shows was because of the great interest of discussing a topic that is not commonly discussed in terms of the Smart Grid. It's common to believe that system that will support various options of accommodating storage and generation options efficiently. There are currently cyber weapons being developed. There must be consideration of investments for anti-viral software.

Works Cited

McDowell, M. (2009, November 4). *Understanding Denial-of-Service Attacks*. Retrieved from US-CERT United States Computer Emergency Readiness Team: https://www.us-cert.gov/ncas/tips/ST04-015

ASRI, Satin and PRANGGONO, Bernardi. (2015). Impact of Distributed Denial-of-Service Attack on. *Sheffield Hallam University*, 16.

Chan, J. C., & Wong, D. S. (2015, October). *Cyber Attacks and the Smart Grid*. Retrieved from IEEE SmartGrid: http://smartgrid.ieee.org/newsletters/october-2015/cyber-attacks-and-the-smart-grid

Department of Homeland Security. (2016, September 27). *Cybersecurity Overview*. Retrieved from Department of Homeland Security: https://www.dhs.gov/cybersecurity-overview

Energy, U. D. (2007). *The Smart Grid: An introduction.* Litos Strategic .

EPCEenergyeducation. (2011, December 5). *The Smart Grid Explained - An Understanding for Everyone*. Retrieved from https://www.youtube.com/watch?v=4L31dHXP6i0

Ghansah, I. (2012). SMART GRID CYBER SECURITY POTENTIAL THREATS, VULNERABILITIES AND RISKS . *Public Interest Energy Research (PIER) Program INTERIM PROJECT REPORT* , 93.

Hong, Y., & Goel, S. (2009). Security Challenges in Smart Grid Implementation. 39.

Intel Corporation, M. a. (2013). Smart Grid Cyber Security. *Smart Grid Deployment Requires a New End-to-End Security Approach*, 6.

Kushner, D. (2013, Febuary 26). *The Real Story of Stuxnet*. Retrieved from IEEE Spectrum: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

O'Connor, M., Nicholas, M. A., Nakamura, S., & Kaczmarek, T. (June). *Managing Cybersecurity Threats to the Smart Grid.* Syracuse: The Maxwell School of Citizenship and Public Affairs.

Pillitteri, V. (2016, August 31). *National Insistute of Standards and Technonlogy*. Retrieved from Cybersecurity for Smart Grid Systems: https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems

Skopik, F., Friedberg, I., & Fiedler, R. (2011). Dealing with Advanced Persistent Threats in Smart Grid ICT Networks. *Safety and Security Department*, 5.

Smart Grid Awareness. (2015, June 24). *U.S. Power Grid Being Hit With 'Increasing' Hacking Attacks as Smart Meter Deployments Continue*. Retrieved from Smart Grid Awareness: https://smartgridawareness.org/2015/06/24/increasing-hacking-attacks-as-smart-meter-deployments-continue/

United States Department of Energy. (n.d.). *What is the Smart Grid?* Retrieved from www.smartgrid.gov: https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Wang, W., & Lu, Z. (2012). Cyber Security in the Smart Grid: Survey and Challenges. *Department of Electrical and Computer Engineering, North Carolina State University*, 29.

(EPCEenergyeducation, 2011)