Cyber Security Threats to the United States Power Grid

Posted on March 21, 2018

Introduction

The dawn of the 21st century and modernization have brought advanced technologies that are aimed to help improve the quality of life of human beings. However, adverse use of the same technology can hurt the quality of life, too. According to the Associated Press, there have been many cyber-attacks by foreign hackers on the power grid of the United States. In one such attack, Russian hackers spied on many US energy companies with the help of malware on the computers. Similarly, in another such cyber-attack, some Iranian hackers remained successful in stealing information about the details of a power plant and passwords. Such cyber-attacks put a huge question on the cyber security of the United States Power Grid. The Power infrastructure and energy system of the United States was given a D-plus ranking by the American Society of Civil Engineers. The Society has noted that the energy system of the United States, power grids, and pipelines were built more than a century ago.

The energy system has not been upgraded as it should have been which poses serious security threats. This inherent weakness in the power infrastructure of the United States is very much in the knowledge of anti-state elements and terrorists. The FBI has shown its concern over the possibility of cyber-attacks on the power grid by the Islamic State through specialized software that may destroy the electrical equipment. Concerned division of the FBI has also indicated ISIS may be recruiting hackers to plan and execute a cyberattack on the power grid of the United States. It is pertinent to mention the extent of difficulty in carrying out a cyber-attack on the American power grid. The national power grid has 55000 power substations, which route the electricity produced by power plants. According to the Wall Street Journal, terrorists need to destroy only 9 out of 55000 power substations to cause a national blackout. Such an attack will shake the entire power grid. Such an attack is quite capable of causing nationwide rolling blackouts which may last more than a year. Similarly, if the terrorists can utilize an electromagnet pulse, it can disrupt all the electronic equipment and harm the national power grid.

EM pulse use against the power infrastructure of the country can cause one to two trillion dollars' loss, and full recovery may take decades. There are many solutions to the cyber-security threats to the power grid. This paper will give a brief about the cyber security threats to the country's power grid.

Vulnerability

There are many approaches used in cyber security that are used in protecting the data and network systems. As such, cyber security is an important part of the information system that allows it to become a tool of the future (Draffin, 2016). It was also found that cybersecurity was one of the biggest concerns in the electric utility sector, and it was only behind environmental, and economic regulation. The main goal of electric utilities is to avoid any failure and breaches in cyber security in the future that may require costly recovery. There are many financial incentives for investing and maintaining cyber security; these are limited because the business model does not provide enough bonuses to spend on boosting the infrastructure. Many challenges are faced in addressing the many electricity up-downs. There are many complexities of the cyber security vulnerabilities as shown in the table below (Draffin, 2016):

Source: (Draffin, 2016)

It was also reported that there are numerous and growing attacks on the North American grid and that the issue is international and national. The Federal Bureau of Investigation also considered the terror activities that are likely to impact America. These attacks are becoming more common, and the energy system will be centrally targeted. The branches of the US Department of Homeland Security have been preparing to respond to these cyber-attacks. Many attackers are seen in the form of other nations, terror cells and organizations, firms, and external hackers that aim at stealing important information damaging the electricity infrastructure and the various grid operations. It is more than possible that many of these attackers are using electricity wires and lines to target the military and industrial settlements. It is also possible that the electricity lines may provide a place for the attackers to gain crucial military information.

It is important to note that cyber-attacks can happen due to the following:

- They can happen from any direction.
- There is no elimination of the attacks, and they can only be mitigated.
- The mitigations will cost a lot of funds to be used, and the benefits may be hard to outweigh the amount of money being used. Moreover, the long-term costs cannot be predicted.
- Cybersecurity should be one of the topmost priorities for the government and the utilities.

The risk has increased, with the utilities moving to the interconnected digital devices from the analog and electromechanical devices. These threats are masked, sophisticated, and very persistent. With new information technology, there are a lot of products that increase the attacks on surfaces.

The smart grid is used in the delivery of electricity to the consumers from the suppliers and uses digital technology that saves energy, and also lowers the cost of electricity, and increases transparency and reliability. The following are a few features of the smart grid:

- It heals after any disturbance in the power events.
- It allows the participation of the consumers and responds to any demands.
- There is a resilience to the cyber and physical attacks.
- The smart grid provides power to the 21st-century needs of the population.
- There are accommodations in the storage and generation options.
- There are new services, products, and markets.
- There is efficiency in the operation and optimization of the assets.

Metering Infrastructure Attacks

A very complex configuration is seen in the smart grid and is known as the Advance Metering Infrastructure. The AMI shares information related to the communication between utilities and smart meters regarding outages. Numerous smart meters are connected with mesh networks that open new opportunities for communication interference and utility assets that will release customers' private information. In many cases, the attackers can send attack packets, which exhaust the node energy and the communication bandwidth.

Hackers may attack the US or European utility grids, affecting the network's control and generation. Hacking the meters is quite possible by evaluating the onboard memory and reading the network interfaces and the diagnostic ports (Ghansah, 2012). Most of the tools that hackers use are open-source or hardware tools that can be purchased. There are examples of both, and these are known as "Terminator" and "OptiGuard" (Lopez et al., 2015). Both are Python-based and are designed to provide full functionality according to the communication protocols (C12.19 and C12.18 ANSI) (Lopez, Sargolzaei & Huerta, 2015). The C12.18 is used in two-way communication between the optical serial ports and meters. In this, the communication is done with the ANSI type 2 optical probe. The intruder is seen to take full advantage of opening the port and allowing the C12.19 to pass through it (Lopez et al., 2015). This protocol allows the meter data table to be viewed and the data includes the measurements, state, and configuration mode.

The NAN sniffing breaks the network encryption and captures the smart meter consumption. By this, the attackers are made to learn the communication protocols by the state that is being used in the meter. The information that is obtained would allow the introduction of false reports that can set up larger attacks. Any minor attacks that would have occurred in the past would have undermined the security efforts. In most cases, the outside party monitors the traffic in the network and obtains information on the control structure, and power consumption in the future (Lopez et al., 2015).

Jamming attacks are used to prevent meters and their connection with the utility organization by stuffing the wireless media with noise. There are two modes in which this can be utilized; the first is the response to sensing normal radio signals and having noise signal emitted; the second it the continuous noise signal emission that results in the channel being blocked. The channels in these cases are always blocked and are hence not received. An attack that restricts the operations can also

take place. In such cases, the attacker prevents the initiation of MAC address operations that cause collisions in the data packet (Lopez et al., 2015). Such attacks are classified according to the target communication, and the preference is not given to legitimate meters but is given to adversarial signals (Ghansah, 2012). Jamming can lead to disastrous effects on the infrastructure and components of the grid.

The next most important and eminent attack can be seen by bad data injection. Such attacks mimic the receivers and senders and obtain illegitimate access to wireless networks. As soon as access is given, the person is overwhelmed by the numerous fictitious messages that are placed on his network. The data attacks can be divided into two subcategories (Lopez et al., 2015): strong and weak. The primary difference between the two is the number of meters one can take control. A strong attack is when the attacker has gained a hold of many meters when launching the attack.

There are other modes of attack such as spoofing, that is related to the impersonation of the network by taking over the identity. The Man in the Middle attacks are also executed by the adversary plugging itself between the communicating gadgets and examining the various types of traffic (Lopez et al., 2015). In this, there is spoofing and injection. The outer party keeps a connection to two devices, while keeping updated with the traffic, and directs any communication between them. The MITM attack can use the fake encryption key to mitigate the encryption and take the place of an original one (Lopez et al., 2015).

There is also a concept of energy theft. In this, the attacker can interrupt the development of a measure even before it comes into existence. There may also be tampering with the demand data of any measurements in the meter. The attacker will be able to modify the network properties during the time that the meter is logging that data (Ghansah, 2012).

Source: (Ghansah, 2012)

Monitoring and Control Attacks

The Fieldbus is an industrial network protocol known as the IEC 61158. These include Modbus, DNP3, CIP, and also PROFIBUS. The components above are designed to follow the communication model. Many protocols lack authentication and encryption procedures. The system that contains Fieldbus is left relatively susceptible to threats and a wide range of attacks. That is when sending illegitimate data that causes protocol failure, the protocol can force these devices to be no longer operable. The interruption of industrial processes can be seen when the protocol commands that the force restart, and, as a result, interrupts the processes. The data from the diagnostics can be erased with the codes, and business and user information can be retrieved. The service can also be denied to many devices at once by rejecting the broadcasting to devices. In these cases, the devices are made to configure the settings.

SCADA systems are widely used in critical infrastructure sectors to provide remote control and

supervision. In the smart grid, the systems are used in the automation. SCADA security is crucial, yet there are vulnerabilities online. There is a wide network of strategies that are vulnerable to electronic attacks. It is also important to take into account that SCADA is exposed to many threats today. The following will discuss the SCADA system and security issues that are faced. SCADA itself stands for Supervisory Control and Data Acquisition System and is an amalgamation of systems that report, measure, and change the remote and local distribution processes. The system itself was designed to operate in an isolated environment, and there is a typical connection with the corporate network for business purposes. The goal and purpose of designing these systems was to make them efficient and not secure. There are communication protocols that allow the remote control of SCADA devices, but they do not focus on security. There are many impacts of the SCADA systems, and these results can be seen in the economic, physical, and societal atmosphere.

The first type of attack is G-SCADA. There are generation-level attacks in which SCADA generation is controlled. In this case, there is a high range of vulnerability to the controller, which results in the controlling of the codes; these codes are overwritten in a harmful manner with programmable logic controllers. Systems such as SCADA and HMI are used to set up external controls for stealing data. In this, HMI is used in accessing the portions of the control process that can be overridden. The process of accessing via HMI is by attacking the Ethernet network and altering the I/O flow of the network between the logic controllers and HMI. The reading and the writing are controlled and henceforth changed with the man-in-the-middle attack.

The second type of attack is the transmission level attack, T-SCADA. The monitoring of the outputs and inputs is done via these standards by the transmission system. An example can be seen in that the inputs and output values are changed, and the attacker shifts the value as desired; the result of the change is the compromise in the T-SCADA server.

Inputs include:

- Line voltages.
- Phasor measurements.
- Load values.
- Transformer settings.

Outputs include:

- Breaker controls.
- Capacitance load adjustments.

The I/O values are targeted, when attacking the T-SCADA server is compromised. The examples can be seen when the misrepresentations are seen in the centralized SCADA console. In other cases, there may be a substation of the gateways' TLS and SSL certificate-based protocols due to the manipulation of the secure channels. Moreover, malicious data can be written to the main controller, and in these cases, the unauthorized devices with the certification will lead to a major compromise in the area

network.

The third type of attack is D-SCADA, which is the distribution level attack. The attackers can access the systems of power output, generation systems, and the AMI head-end systems. At the most basic device level, there is a breach seen in the field controller, and this may result in many consequences that vary from the false reporting of data to the operations inadequacies. An example is seen in the autorecloser, which is a type of remote terminal unit that acts as the breaker to protect against power surges. It also allows the recovery mode to start after the conditions are returned to normal. More often than not, the correct manipulation will result in the tripping of the recloser, which will have a cascading effect on the distribution of the systems. The hacker or attacking nation group will be able to have complete and dominant control over the RTU; it is in a position to insert malicious code or logic into the controller of the RTU. Any malware in the RTU can cause many system faults. There can also be the reporting of nominal conditions in the utility centers. Many disruptions in the targeted area resemble service rejection.

Another attack is the time delay switch. There is a wide variety of attacks that can be introduced into the data stream during the various points at the power plant; these delays in the data stream during the measuring points were proven to be very effective when applied to the station levels. The work mostly focuses on the intrusion in the communication channels in the sensing loop and the automatic generation of control signals. The signals exist between the control area of the plant and the IT layer. It is shown that the TDS attacks sabotage the whole power system by forcing destabilization. The systems are built using public communication protocols, and there is a communication level between the RTU and the MTU. In this case, the SCADA protocols provide specifications for the interconnected computers, IEDS, RTUs, and the master station. As such, the most common protocol that is used is the DNP3.

It is important to note that the data and meter collection unit in the power grid makes it susceptible to cyber-attacks and any other malicious measurements. There have been many cases of cyber hacking in the past, and the loss of data in this manner compromises US safety. The data obtained can lead to economic losses and result in the faulty pricing of the products; there may be chances of blackouts that bar any likelihood of the occurrence in the power grid.

The Generic Issues in the Smart Grid

Many critical security issues are not exactly related to the logical aspects of communication. These issues are associated with any component of the grid, and the reference is made to the actual field cases. Many issues have also been addressed in the NIST smart grid analysis document.

There is a problem in the authorization and authentication of the users in the IEDs for the maintenance personnel; the problems are in a way targeted at the user and are concerned with the authentication of the user by obtaining passwords, and other information that is not shared by the

user. The management is also done across the IEDs and in the numerous substations that belong to the utility. There are reasonable updates to ensure that only targeted users can authenticate the device. At present, there are many substation IEDs, which have not targeted the “user.” The passwords are stored on the local device, with various passwords that are used in the authorization stages. The role passwords are used by employees, contractors, and vendors on shared devices. There is an increased number of devices, and the passwords are mostly similar in these. As one discusses the role of authenticating and authorizing these users at the substation IEDs, it is important to note that this poses a serious threat to the overall structure. The users and employees, in this case, are the regular utility employees, the vendor support engineers, and the contractors. As mentioned, the role includes the Audit, administrator, user, and security officer. The mentioned devices are accessed locally, and the user is physically present at the various substations. The IED is accessed on the front panel or with a wired network, or a wireless one. The devices can also be accessed at completely remote locations, with a high-speed or low-speed network connection that is done from a remote location. The provision is made to ensure the provided access in any emergency, and it is an important measure taken; it bypasses the regular controls, and it is done with an audit trail.

In addition to the IED equipment, there is also the smart meter deployment that makes use of the passwords in meters that are not related to those of the users. These passwords are used throughout the meter development and are shared among the users. Similar to the IED, the problems faced by the smart meter are numerous. In the case of the smart meter, the access can be through the optical port, and local; there may also be remote access with the AMI, or with the HAN gateway. These meters do have some level of connectivity to the AMI head end, and the level can be as low as 1200 baud, or also lower in some cases where the power line carried device has data rates that are measured in mill baud.

There are threats seen in the authorization and authentication of the people in the outdoor field equipment. The equipment can support Bluetooth or 802.11 for local access from the maintenance truck. There is a problem seen in the authorization and authentication of the users for the devices in a way that the access is targeted at the user, information (passwords), and that is also specific to the user. There are a few problems faced in this, one of which is the breach of the security of the wireless channels. The other problem is that of how these users can be authenticated. Research has been carried out, and results have been targeted at the smart meters and the IEDs, with the passwords in the field device, being the same in the thousands of devices that are not specific to the user and are not changed. Access is granted only via a wired connection, and with the short-range radio, some devices allow remote access.

Consumer and meter authorization and authentication are also issues. The meters are the home area network gateways that transfer information to the customers. If the customers are authenticated to the meters, the authorization procedures ought to be carefully monitored. The authentication from the AMI head-end ensures that no adversary can control the meter. The AMI head end and the authentication of the meter are important as the users’ information is obtained from the meter and is used for billing purposes; the commands ought to be assured of the delivery to the meter.

The HAN devices must be authenticated in a secure manner to the gateway. It is also crucial for the HAN device for it to be authenticated about the command and the demand-response from the head end of the DR, to secure control. The HAN device ensures the commands are delivered, and the responses from the correct device are not forged. In the case of the HAN device failing the authentication, it will be unable to respond to the demands of the response signals. There may not be a possibility for the DOS attack to result in the failure of the HAN device's authentication.

There are many distributions in the communication systems that use the serial links for many purposes including SCADA communications with the distribution field and control center equipment. Many other protocols are used that do not offer protection of the confidentiality of the messages that are sent and received in the text form. There are solutions that use protocols like the IPSEC or SSL, that wrap the serial link over PPP, and that suffer unduly. There are solutions that relate to the addressing of bandwidth and security issues in the environment.

There are a few other management systems in the meters. The meters contain cryptographic keys for authentication and encryption of operations. There are also cryptographic operations that are used in management schemes, and they provide key diversity. The devices have unique materials and diversity, and the compromise of one device does not affect other devices. There are also other cases of the meter bases where the symmetric keys are the same across many different states, and the compromise of only one network can result in the compromise of all the networks and meters. There is also an inability to perform the updates on the meters, which allows the development of the applications without any expensive physical visits to the equipment. It is also important to make sure that the firmware mechanisms are not used in the installation of any malware. It is in the best interest to deal with such issues.

The integrity of the meter repairs and updates is essential in the prevention of any malicious threats. The availability and number of hours are also important. Confidentiality is not absolutely essential unless there is a relation to the maintenance of personal information.

References

Baumeister, T. (2010). Literature review on smart grid cyber security. *Collaborative Software*

Development Laboratory at the University of Hawaii.

Ghansah, I. (2009). Smart grid cyber security potential threats, vulnerabilities, and

risks. *California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047*.

Lopez, C., Sargolzaei, A., Santana, H., & Huerta, C. Smart Grid Cyber Security: An Overview of

Threats and Countermeasures. *Florida International University*.

Martellini, M., Abaimov, S., Gaycken, S., & Wilson, C. (2017). Vulnerabilities and Security

Issues. In *Information Security of Highly Critical Wireless Networks* (pp. 11-15). Springer International Publishing.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Cyber Security for Smart Grid

Communications. *IEEE Communications Surveys and Tutorials*, *14*(4), 998-1010.