International Journal of Scientific Research and Engineering Development-– Volume 3 Issues 1 Jan- Feb 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Smart Grid Cyber Security

Amogha A K
Department of EEE

----------**********----------

Abstract:

This paper is about the cyber security in smart grid . Here, there are highlights of the complexity of smart grid network , vulnerabilities and threats specific to this huge heterogeneous network. The challenges that exist in securing the smart grid network and how the current security solutions applied for IT networks are not sufficient to secure smart grid networks. We conclude by over viewing the current and needed security solutions for the smart grid precisely during all time.

Keywords **—Cyber Security, vulnerabilities, threats**

----------**********----------

I. INTRODUCTION

The traditional electrical power grid is currently evolving into the smart grid. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers, improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. A smart grid is a huge complex network composed of millions of devices and entities connected with each other. Such a massive network comes with many security concerns and vulnerabilities. Smart Grid is a developing network which is a new technology that includes equipments and control working together. In addition, it has a cyber security system to protect Smart Grid from hackers .

II. PROBLEM STATEMENT

In this highly modern technological world , Smart Grids are susceptible to cyber attacks.Hence, smart grid cyber security has become essential to protect the system.

III. WHAT DOES CYBER ATTACK MEAN?

A cyber attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Cyber attack is also known as a computer network attack (CNA).

IV. WHAT IS A SMART GRID ?

Smart grid has a digital technology which improves reliability, and efficiency of the electric system in real-time.

V. WHAT IS CYBER SECURITY ?

It is a practice which intends to protect computers, networks, programming & data from unauthorized access to change or destruction.

VI. OBJECTIVES OF SMART GRID SECURITY

- Data Availability
  - It refers to timely & reliable access to the use of information.
- Data confidentiality
  - It refers to protecting personal privacy information from an unauthorized access.
- Data integrity
  - It refers to preventing or detecting the modification of information by unauthorized persons or system.

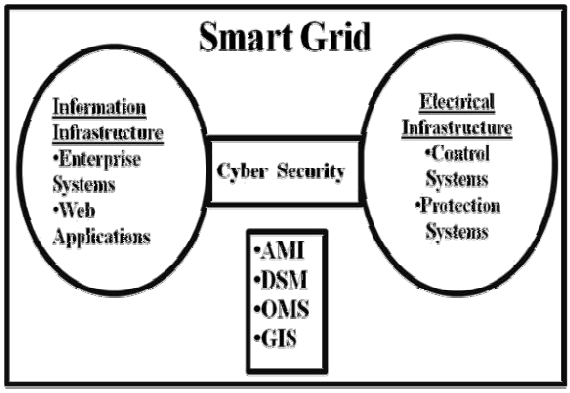


Fig.(i): Smart Grid Technology

VII. NEED OF CYBER SECURITY IN SMART GRID

Previously power Grid automation system were isolated from public network .Later, it became essential to utilize public network. This has increased the vulnerability of power grids to Cyber attacks by exposure to networks.

VIII. CYBER THREATS IN SMART GRID

There is a possibility of a security breach due to frequent exchange of sensitive information. To avoid unauthorized access of smart grid data, there is a necessity of shielding the important data. Hackers have a tendency to take control of smart grid application of server for accessing confidential information.

Types of Cyber Attacks

1.Web-based Attacks
2.System-based Attack

Web-Based Attacks

1.Injection Attacks:

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection can be disastrous.

2.File Inclusion Attack:

A file inclusion attack is a type of vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time.

3.Cross Site Scripting:

Cross-site scripting (XSS)is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

4.DNS Spoofing:

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

5.Brute –Forced Attack:

A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible

passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

6.Dictionary Attack:
It is for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

7.Buffer
Overflow:
In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Buffers are areas of

memory set aside to hold data, often while moving it from one section of a program to another, or between programs.

8.Session Hijacking:
Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to
maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

9.URL Interpretation:
In a URL interpretation, a client manually adjusts the parameters of his request by maintaining the URL's syntax but altering its meaning.

10.Social Engineering:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information that may be used for fraudulent purposes.

11.Man in Middle Attack:
A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

12.Phishing:
Phishing is the fraudulent attempt to obtain sensitive information such as usernames, password, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

13.Virus:
Vital Information Resources Under Seize is a computer virus that is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

14.Worms:
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

Worms almost always cause at least some harm to the network. Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through.

15.Trojan Horse:
In computing, a Trojan horse, or Trojan, is any malicious computer program which misleads users of its true intent. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a

routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else .

16.Backdoors:
Entering a protected system using a password can be described as going through the front door .Companies may build backdoors 'into their systems'. However, so that developer can bypass authentication and dive right into the program . Backdoors are usually secret , but may be exploited by hackers if they are revealed or discovered .

17.Bots:
An internet bot, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering (web crawler), in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human. More than half of all web traffic is made up of bots.

18.Sniffing:
It is an interruption or capturing of network data packets which are unencrypted to gain the information and to crash the network.

System Based Attacks
1.Component-Wise
2.Protocol-Wise
3.Topology-Wise

Details of System based Attacks
1.Component-Wise:

It includes all the types of Field Components like RTU i.e. Remote Terminal Units etc are attacked through remote access.

2.Protocol-Wise:

Using the communication protocols available in the public domain, an intruder can hack the data acquisition protocols and exploit them.

3.Topology-Wise:

Network topology vulnerability is

exploited . Ex.: DoS i.e. Denial of Service

Attack **Consequences – Component Wise**

- Mislead data presented to control system operator.
- Damage to field equipment if operator performs supervisory control operations based on inaccurate field Data.
- Loss of service due to intruder shutting down the device.

Consequences –Protocol Wise

- Financial loss if the attack leads to Excess generation output.
- Safety vulnerability if a line is energized while line men are in the field servicing in the line.
- Equipment damage it control commands ascent to the field resulting in over load conditions.

Consequences-Topology Wise

- Delay or inhibition of real time data exchange.
- As a result control centre operators may fail to have a complete view of electrical power grid system status, leading to incorrect decision making.

Types of Damages

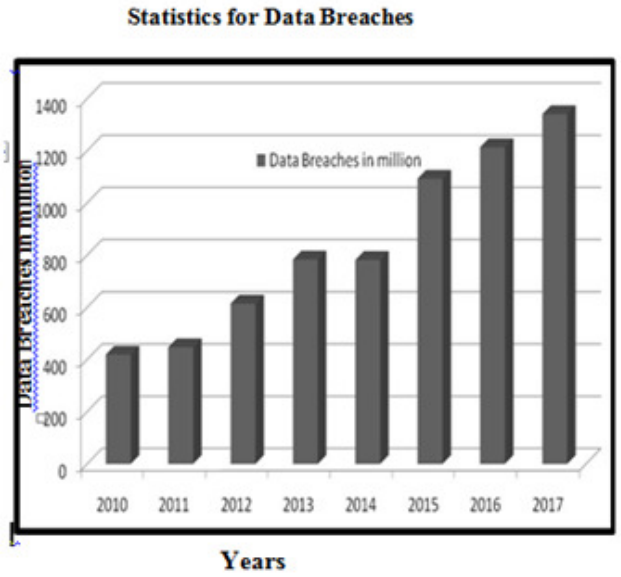
(1) Cyber Fraud :
It is done for Monitory Gains.

(2) Cyber Spying:
It is done for Gaining Information .

(3) Cyber Assault:
It is done in order to Damage the Information of the networks .

(4)Cyber Warfare:
Cyber warfare is responsible for Damaging Infrastructures Facilities in the system network components .

This affects the functioning of the entire system network. There will be improper operations of the components or equipments or the devices present in the smart grid .This will lead to the destructions in the smart grid which is dangerous .



Benefits of Cyber Security :
1.Strengthening system against security attacks.
2.Guarding of data.
3.Shielding of Software.
4.Unauthorized access.
5.Smooth functioning of grid.
6.Security alarming in case of cyber attack.

Security Features :
- Human safety
- To ensure that system runs under normal operating conditions .
- To protect the equipments and power lines.
- Security Requirements
- Maintain up to date software, vulnerability and penetration testing .
- Training for employees keeping emails secure.
- Maintain backup diligently.

Security Solutions
- Encryption software
- Data backup solution
- Password security software
- Anti-Virus software
- Firewalls

IX. CONCLUSIONS

With the broad range of opportunities that internet has opened for everyone also comes the risk of Cyber attacks it is time to fight this attacks.As most of such cyber attack can be prevented or detected with basic security practices intelligent about cyber security at the substations can make an enormous different towards efficient cyber resilience.

X. FUTURE SCOPE

Research should be made for the provision of robots in smart grids to avoid manual errors and human loss .Cyber security in the smart grid is still under research and needs more investigation to overcome the vulnerabilities and threats.

REFERENCES

1. www.smartgridcybersecure.net
2. www.paloalto.edu
3. https://heimdalsecurity.com
4. https://securityinyelligence.com
5. https://cyber.fiu.edu

6.Cisco White Paper. [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/white paper c11539161.pdf
7. Metke AR and Ekl RL. Security technology for smart grid networks. IEEE Transactions on Smart Grid, 2017
8. Tehopedia.com
9. en.wikipedia.org/wiki/Code_injection
10.en.wikipedia.org/wiki/File_inclusion_vulnerability
11.en.wikibedia.ru/wiki/Local_File_Inclusion
12. slideshare.net/SiddharthBezalwar/secure-coding-in-c
13. en.wikipedia.org/wiki/Cross-site_scripting
14.code.tutsplus.com/tutorials/cross-site-scripting-in-wordpress-what-is-xss--wp-30430
15. en.wikipedia.org/wiki/DNS_spoofing
16. gateoverflow.in/55536
17. en.wikipedia.org/wiki/Brute-force_attack
18. youtube.com/watch
19. en.wikipedia.org/wiki/Dictionary_attack
20.scribd.com/document/223688503/Smart-Grid-Security
21.smartgridawareness.org/privacy-and-data-security/smart-grid-vulnerabilities-a-more-detailed-review/smart-grid-security-threats-vulnerabilities-and-solutions
22. link.springer.com/10.1007/978-3-642-40675-1_73
23. phoenixnap.com/blog/cyber-security-attack-types
24. en.wikipedia.org/wiki/Social_engineering_(security)
25. en.wikipedia.org/wiki/Man-in-the-middle_attack
26. en.wikipedia.org/wiki/Computer_worm
27. quizlet.com/202996905/exam-3-flash-cards
28. en.wikipedia.org/wiki/Trojan_horse_(computing)
29. en.m.wikipedia.org/wiki/Computer_trojan
30. motherboard.vice.com/read/hacking-glossary
31. linkedin.com/pulse/what-difference-between-troll-internet-bot-jarrett-potts
32. en.wikipedia.org/wiki/Internet_bot
33. scribd.com/document/231143864/An-Integrated-Security-System-of-Protecting-Smart-Grid-Against-Cyber-Attacks

XI. AUTHOR PROFILE

Amogha.A.K. received Bachelor's Degree in Electrical & Electronics Engineering in the year 2017. She has completed post graduation M.Tech in Electrical Power Systems in the year 2019. She has presented her various technical papers in Seminars, Conferences as well as in many International journal publications. Her area of interest is Power Systems.