RESEARCHERID
THOMSON REUTERS

[Reetu, 6(6): June 2019]
IDSTM-2019

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A REVIEW STUDY ON CYBER SECURITY REQUIREMENT IN POWER GRIDS

Miss Reetu
Assistant professor, CSE Department GTC Soldha, Bahadurgarh, Haryana

ABSTRACT

Cyber Security is the protection of internet connected systems, including hardware, software and data from cyber-attacks. Many security methods and schemes could be applicable to the smart grid, especially in domains that interact with customers (Markets/Customers/Service Provider Domains). While in the Generation/Transmission/Distribution domains, which are responsible for the process of power delivery, attack detection, mitigation, authentication and key management. In this paper some cyber security, Authentication of data, Malware scanners, Firewalls, Anti-virus are studied.

Keywords- *Cyber Security, Malware Scanner, Firewall, Smart Grid.*

I. INTRODUCTION

Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks. To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), recently issued updated guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessment. The voluntary cyber security framework, developed for use in the banking, communications, defence and energy industries, can be adopted by all sectors, including federal and state governments. President Donald Trump issued an executive order mandating that federal agencies adopt the NIST Cyber Security Framework in May 2017 The voluntary cyber security framework, developed for use in the banking, communications, defence and energy industries, can be adopted by all sectors, including federal and state governments. President Donald Trump issued an executive order mandating that federal agencies adopt the NIST Cyber Security Framework in May 2017. As a result of security risks, investments in cyber security technologies and services are increasing. In 2017, Gartner predicted that worldwide spending on information security products and services would reach $83.4 billion -- a 7% increase from 2016-- and that it would continue to grow to $93 billion by 2018.

II. ELEMENTSOFCYBERSECURITY

Cyber security requires the coordination of efforts throughout and information system, which includes

- Application security.
- Information Security
- Network Security
- Disaster Recovery/Business Continuity Planning
- Operational Security.

III. TYPES OF CYBER SECUTIRY THREAT

- Ransom ware: is a type of malware that involves an attacker locking the victim computer system files -- typically through encryption - and demanding a payment to decrypt and unlock them.
- Malware: is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- Social Engineering: is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

- Phishing: is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources;
- however, the intention of these emails is to steal sensitive data, such as credit card or login information

IV. TECHNOLOGY FOR CYBER SECURITY

- Cryptographic systems: A widely used cyber security system involves the use of codes and ciphers to transform information into unintelligible data.
- Firewall: Use to block traffic from outside, but it could be also used to block traffic from inside.
- An Intrusion Detection System (IDS): IDS is an additional protection measure used to detect attack.
- Anti-Malware Software and scanners: Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called anti Malware tools are used to detect them and cure an infected system.
- Secure Socket Layer (SSL): It is a suite of protocols that is a standard way to achieve a good level of security between web browser and websites.

V. CYBER SECURITY APPROACHES

A. System Model

A smart grids consist of four components: generation, transmission, distribution, and consumption. In the consumption component, customers use. electric devices (e.g., smart appliances, electric vehicles), and their usage of electricity will be measured by an enhanced metering device, called a smart meter. The smart meter is one of the core components of the advanced metering infrastructure (AMI). The meter can be collocated and interact with a gateway of a home-area network (HAN) or a business-area network (BAN).

B. Cyber Security Requirements

In this section, we analyse the information security requirements for smart grids. In general, information security requirements for a system include three main security properties: confidentiality, integrity, and availability. Confidentiality prevents an unauthorized user from obtaining secret or private information. Integrity prevents an unauthorized user from modifying the information. Availability ensures that the resource can be used when requested. The most important requirement for protecting smart grids are outlined below.

- Confidentiality of power usage: Confidentiality of meter data is important, because power usage data provides information about the usage patterns for individual appliances, which can reveal personal activities through nonintrusive appliance monitoring.
- Integrity of data, commands, and software: Integrity of price information is critical. For instance, negative prices injected by an attacker can cause electricity utilization spike as numerous devices would simultaneously turn on to take advantage of the low price. Although integrity of meter data and commands is important, their impact is mostly limited to revenue loss. Availability against DoS/DDoS attacks: Denial-of-service (DoS) attacks are resource consumption attacks that send fake requests to a server or a network, and distributed DoS (DDoS) attacks are accomplished by utilizing distributed attacking sources such as compromised smart meters and appliances. In smart grids, availability of information and power is a key aspect.
- Availability against DoS/DDoS attacks: Denial-of service (DoS) attacks are resource consumption attacks that send fake requests to a server or a network, and distributed DoS (DDoS) attacks are accomplished by utilizing distributed attacking sources such as compromised smart meters and appliances. In smart grids, availability of information and power is a key aspect [20]. More specifically, availability of price information is critical due to serious financial and possibly legal implications.

C. Attack Model

- To launch an attack, an adversary must first exploit entry points, and upon successful entry, an adversary can deliver specific cyber-attacks on the smart grid infrastructure. Requirement of cyber security in Smart Grids –

- Availability, integrity, and confidentiality are three high-level cyber security objectives for the Smart Grid.
- Attack detection and smooth operations of smart Grid.
- For Identification, authentication and access control.
- For Secure and efficient communication protocols.

VI. LITERATURE REVIEW

1. A study of cyber security challenges and its emerging trends -
This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. The author discusses some cyber security techniques Access control and password security, Authentication of data, Malware scanners, Firewalls, Anti-virus.

2. Study of Latest Emerging Trends on Cyber Security and its challenges to Society [June 2012]- This paper focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

In this paper a list was developed on issue of cyber security by research and survey some issues are Mobile Devices and Apps, Social Media Networking, Cloud Computing Protect systems rather Information, Everything Physical can be Digital. It also discussed some specific cyber security techniques like Access Control and Identity Management, Authentication, Malware scanners, Firewalls, Cryptography.

3. Cyber security in the Smart Grid: Survey and challenges [Jan 2013]- The Smart Grid, generally referred to as the next-generation power system. Cyber security in the Smart Grid is a new area of research that has attracted rapidly growing attention in the government, industry and academia. In this paper, a comprehensive survey of security issues in the Smart Grid is discussed. The communication architecture and security requirements, analysed security through case studies, and discussed attack prevention and defence approaches in the Smart Grid is discussed.
4. Cyber Security of Smart Grid Infrastructure-[Jan-2014]- In this paper Smart Grid and some recent Cyber Security incidents of this critical infrastructure are discussed. The key security requirements of a smart grid, which are 'availability ''integrity', and 'confidentiality', are also discussed.

Based on the existing research, an overview of Smart Grid anomalies is discussed thoroughly. The protection frameworks of smart grid against component-wise, protocol- wise and topology wise cyber- attacks are also reviewed in this chapter.

5. Smart Grid Cyber-Physical Security – [Sep. 2017]
In this paper author discussed the cyber security in power grid in two phases approach. First is "Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid against Internal Adversaries," studies the privacy-preserving data aggregation, an important problem of consumer privacy protection in the smart grid environment. The second is, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," focuses on an emerging category of threats to smart grids, i.e., coordinated cyber-physical attacks. Through analysing the prerequisites of the implementation of the attacks, the corresponding counter measures to detect those threats in both cyber and physical space are proposed. Both the implementation of coordinated cyber-physical attacks.

VII. RESEARCH GAP

As I reviewed, cyber security is still under development in the Smart Grid, especially because information security must be taken into account with electrical power systems. Consequently, the Smart Grid requires fine-grained security solutions designed specifically for distinct network applications, making cyber security for the Smart Grid a very challenging research area in the future.

REFERENCE

1. *A study of cyber security challenges and its emerging trends (June 2010).*
2. *Study of Latest Emerging Trends on Cyber Security and its challenges to Society [June 2012]*
3. *Cyber security in the Smart Grid: Survey and challenges [Jan 2013]*
4. *Cyber Security of Smart Grid Infrastructure-[Jan-2014]*
5. *SmartGrid Cyber-Physical Security – [Sep. 2017]*
6. *Data communication over the smart grid," in Proc. IEEE Int. Symp. Power Line Communications and Its Applications (ISPLC), Mar. 29–Apr. 1 2009.*
7. *Towards a framework for managing information security for an electric power utility CIGRÉ experiences," IEEE Trans.*
8. *Risk assessment of information and communication systems—Analysis of some practices and methods in the electric power industry," CIGRÉ Electra, Aug. 2008.*
9. *Cyber security considerations in power system operations," CIGRÉ Electra No. 218, Feb. 2005.*
10. *On requirements specifications for a power system communications system," IEEE Trans. Power Del., vol. 20, no. 2, Apr. 2005.*