Relevance of Cybersecurity in Smart Grid

MANGALA DEVI

Abstract

Cybersecurity has its relevance in today's smart grid. IOT enabled devices and equipments, smart substations and feeder automation, all are an integral part of smart grid. Thus hacking and other cyber attacks have to be taken into consideration in designing and maintaining a smart grid. Effort is made here to highlight the relevance of cyber security in a smart grid and the regulations made by various countries to take care of these threats.

Keywords : Cyber security, Smart grid

Introduction

Cybersecurity is related to making the systems secure against malicious attacks. Cyber attacks on Information Technology systems may be considered as different when compared to those on smart grids. This is because in the case of smart grids, these attacks are going to affect the critical infrastructure of a country.

In simple terms, a smart grid is a traditional electric grid plus information technology plus two way communications. The traditional electrical grid is getting automated with smart substations, Intelligent Electronic Devices and IOT enabled devices. For example, consider a house of a householder with smart meter installation and the electricity usage is being tracked using the mobile phone. The user if needed, can reduce the electricity consumption during times when the tariff is high, and increase the consumption during off peak hours. This is a simple example, but one can envisage the magnitude of the control possible in a smart grid consisting of sensors and actuators, automatic fault detection and control and Advanced metering Infrastructure, to name a few.

The figure below shows the interaction of actors in different smart grid domains through secure communication flows and electrical flows. [1]

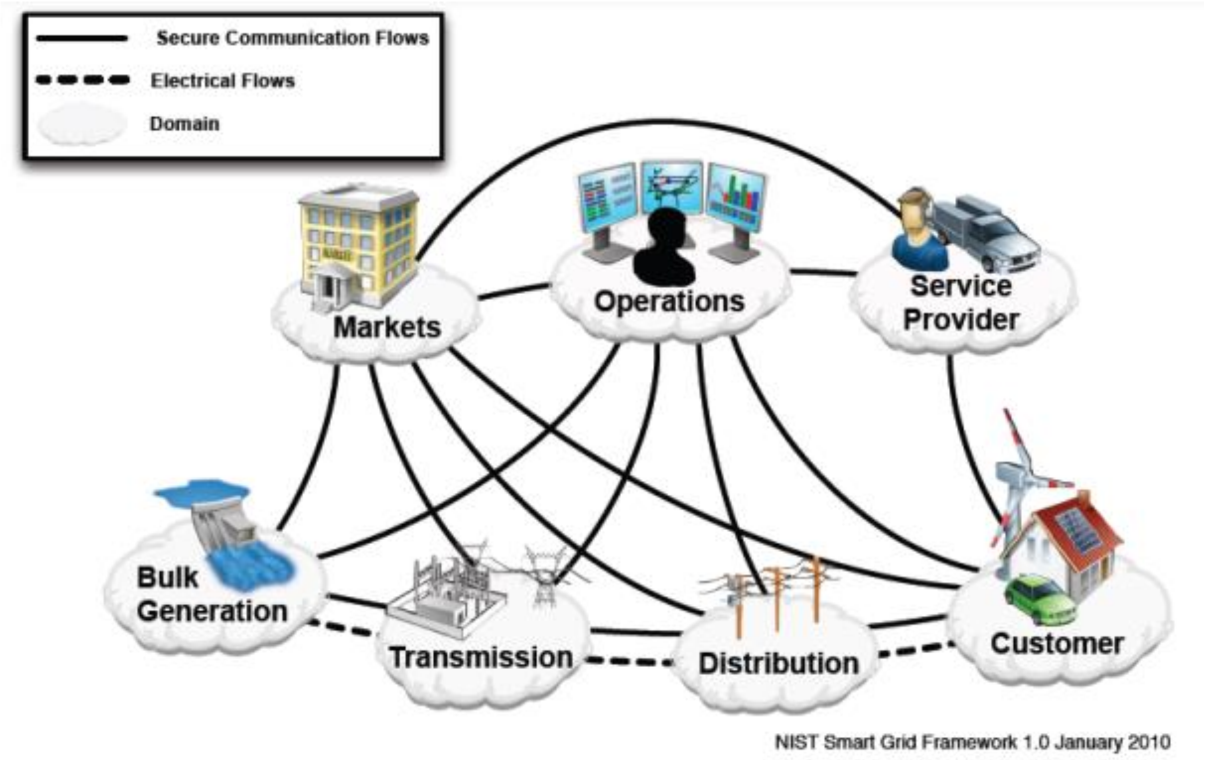

Figure 1: Interaction of actors in different smart grid domains through secure communication flows and electrical flows

Main Areas of an Electrical power system, where things are getting automated

The various areas in Electrical power systems where the devices are getting automated include Electricity metering, Fault monitoring and control, Grid operation and Control, Distribution management, Substation operation, IOT enabled devices and control etc. to name a few. The data generated can be used for analytical purposes and taking proper control decisions.

Types of Cybersecurity issues in Smart Grid

The table below shows the basic types of cyber security attacks in a smart grid. [3]

Table 1 : Basic types of Cybersecurity attacks in a smart grid [3]

Name	Description
Device attack	It aims to compromise (control) a grid device. It is often the initial step of a sophisticated attack.
Data attack	It attempts to adversarially insert, alter or delete data in the network traffic so as to

	mislead smart grid to take wrong decision.
Privacy attack	It aims to learn/infer the private information of the users by analysing electricity usage data.
Network availability attack	It aims to use up or overwhelm the communication and computational resources of smart grid and to result in delay or failure of communication.

A few of the study on the disruptions that can be caused due cyber attacks, as found in the literature are given in the table below.

Table 2 : Disruptions that can be caused due cyber attacks, as found in the literature

Sl. No	Study Area
1	Reliability impacts from cyber attack on the performance of the grid and the development of power grid finite-state abstraction (FSA) models that preserve the dynamic behavior of the modeled systems [4]
2	Smart Grid Resilience Under Remote Meter Disconnect Attack [5]
3	Risk-based approach to security that has been used for years in protecting physical assets, and how it could be modified to help secure the digital aspects of the smart grid and control systems in general. [6] The smart grid has been said to be vulnerable because mass load fluctuations could be created by quickly turning off and on large quantities of smart meters. [6]
4	At the end of December, 2015 as many as 80,000 residents in Western Ukraine lost power. Subsequent investigation into the incident indicated that coordinated cyber-attacks contributed to the power outages by disrupting control systems and flooding call centers. [7]
5	On Friday 12 May 2017 a global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. In the UK, the attack particularly affected the NHS, although it was not the specific target. At 4 pm on 12 May, NHS England declared the cyber attack a major incident and implemented its emergency arrangements to maintain health and patient care.

	[9]

Cyber Security standards for Smart Grid

1. The IEC 62443 series was developed to secure industrial automation and control systems (IACS) throughout their lifecycle [2].
2. NIST has identified cyber security standards that support smart grid interoperability and has issued a cybersecurity guideline.

Cyber security laws in various countries

AEMO(Australian Energy Market Operator) submitted Australia's 2020 - Cyber Security Strategy AEMO is shared the view of the Australian government that cyber security and the safety of the internet is important to protect the essential services, such as energy, water and transport. The pervasive use of information and communications technology and its convergence with operational technology renders critical systems and infrastructure vulnerable to cyber-attack. [12]

On June 1, 2017, China's Cybersecurity Law went into effect, marking an important milestone in China's efforts to create strict guidelines on cyber governance. Long before the Cybersecurity Law took effect, China had already made some efforts to strengthen information security. [11]

In the EECSP Report: Cyber Security in the Energy Sector February 2017, the two main objectives are 1. To secure energy systems that are providing essential services to the European society and 2. To protect the data in the energy systems and the privacy of the European citizen. [15]

Central Electricity authority, Govt. of India, has issued CEA (Cyber Security in Power Sector) Guidelines, 2021, for compliance by the entities concerned. Government of India has set up the Indian Computer Emergency Response Team (CERTIn) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats. [10].

In 2015, the Cyber Security Agency of Singapore (CSA) was formed as the central agency to oversee and coordinate all aspects of cybersecurity for the nation [13].

The Singapore Cybersecurity Strategy 2021, outlines Singapore's updated goals and approach to adapt to a rapidly evolving strategic and technological environment. Threat actors are becoming more sophisticated and taking advantage of increasingly ubiquitous connectivity to launch more cyberattacks. Singapore thus reviewed and refreshed its cybersecurity strategy, which was first launched in 2016 [13].

Conclusion

Cybersecurity issues of smart grid are going to be of great concern, considering the reliability aspects of this critical infrastructure. The various standards related to cyber security issues in smart grid and some of the various government initiatives to address the same are consolidated here.

References :

1. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0
2. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443 . [Accessed: 05-Apr- 2022].
3. X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," in *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38-45, August 2012, doi: 10.1109/MCOM.2012.6257525.
4. E. Stamp, R. A. Laviolette, L. R. Phillips, and B. T. Richardson,"Sandia Final Report: Impacts Analysis for Cyber Attack on ElectricPower Systems (National SCADA Test Bed FY08)," Tech. Rep., 2009
5. William G. Temple, Binbin Chen, and Nils Ole Tippenhauer, " Delay Makes a Difference: Smart Grid Resilience Under Remote Meter Disconnect Attack", In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm'13) Vancouver, Canada, October 2013
6. S. Clements, H. Kirkham, M. Elizondo, and S. Lu, "Protecting the smart grid: A risk based approach," in IEEE Power and Energy Society General Meeting, 2011
7. [Online]. Available: https://www.sans.org/webcasts/analyzing-ukrainian-power-grid-cyber-attacks-102007/ . [Accessed: 05-Apr- 2022].
8. [Online]. Available: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20. [Accessed: 05-Apr- 2022].
9. [Online]. Available: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. [Accessed: 05-Apr- 2022].

10. [Online]. Available: https://cea.nic.in/wpcontent/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf. [Accessed: 05-Apr- 2022].

11. [Online]. Available: https://www.protiviti.com/HK-en/insights/china-cybersecurity-law-and-impacts#:~:text=On%20June%201%2C%202017%2C%20China's,efforts%20to%20strengthen%20information%20security. . [Accessed: 05-Apr- 2022].

12. [Online]. Available : https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-138.pdf. [Accessed: 05-Apr- 2022].

13. [Online]. Available : https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021. [Accessed: 05-Apr- 2022].

14. [Online]. Available : https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf. [Accessed: 05-Apr- 2022].

15. [Online]. Available : https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf. [Accessed: 05-Apr- 2022].

16. [Online]. Available : https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. [Accessed: 05-Apr- 2022].