Smart Grid Cybersecurity

Matthew N. O. Sadiku
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
sadiku@ieee.org

Mahamadou Tembely
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
mtembely@student.pvmau.edu

Sarhan M. Musa
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
smmusa@pvamu.edu

Abstract— **The smart grid is the next generation electric power system that depends on modern communication networks and supports electricity generation, transmission, and consumption. Potential threats from a broad range of cyber attacks on the smart grid have become a serious concern. Cybersecurity is critical to sustainable modern grid. This paper provides a basic knowledge for smart grid cybersecurity.**

Keywords—smart grid, cybersecurity, cyber-crime, information warfare, cyberwar

I. INTRODUCTION

The North American power grid is one of the most complex and largest systems in the world. It is now aging and evolving into a smart grid, which is a power grid with intelligence [1]. With the heavy reliance on computer communication networks to manage its energy usage, a smart grid becomes exposed to vulnerabilities and cyber attacks. The potential impact of cyber attacks is vast.

Security is a crucial attribute of the smart grid. It is the degree of protection provided by the grid against potential loss or damage. Security issues arise as smart power grids become targets of cybersecurity threats. With the rapid expansion of the Internet of Things, the potential for malicious attacks on the smart grid is on the increase. A breach in the security of the smart grid can be fatal for its reliability.

II. SMART GRID ARCHITECTURE

Over the years, the power industry operated their own communications infrastructure to control power grids. The trend has shifted toward using shared public communication networks. The power and communication systems are becoming more and more interdependent. Smart grid is the emerging intelligent power systems that depend on Information and Communication Technology (ICT). Smart grid enables integration of smart appliances, transmission and distributed systems, and energy management. It integrates renewable resources, such as wind and solar power, with conventional grid.

The smart grid architecture has two components: power architecture and communication architecture [2].

Power Architecture: Generation, transmission, and distribution are the three main subsystems of the electric power system. The power grid physically connects power generation and power consumers. Transmission is the bulk transfer of electricity from power plants to substations. Distribution delivers electricity from the substations to consumers. The smart grid utilizes several technologies to produce, distribute and monitor energy usage of customers. Energy from distribution substation is received by the Home Area Network (HAN) and distributed to all home appliances.

Communication Architecture: This includes the physical network architecture and network protocols. All components are connected by the several communication technologies such as Wide Area Networks, WiMax, and HAN. The communication infrastructure controls the power infrastructure and makes it intelligent, efficient, and reliable. It is vital that communications are secured, devices are protected, and privacy is respected. The communication system measures, collects, stores, and communicates between all devices. The Advanced Metering Infrastructure (AMI) includes Supervisory Control and Data Acquisition (SCADA) Center, smart meters, and Wireless Sensor Networks. This allows for automatic reading of power consumption of the customers. Utilities can automate billing from a centralized interface.

III. SECURITY REQUIREMENTS FOR SMART GRID

The smart grid has unique security requirements or objectives [3]. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity.

Availability: This refers to the ability of the smart grid to maintain correct operation even during adverse conditions. This usually gets the highest priority when it comes to power. Access to the smart grid should be available and reliable to all users. Power systems should be available 100% of the time. Attacks targeting availability of service generally leads to Denial of Service (DoS).

Authentication: This usually involves using username and password to validate the identity of the user. Authentication and integrity can help the smart grid protect against common cyber attacks such as impersonation, forgery, and man-in-the-middle.

Confidentiality: Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings. Confidentiality ensures that information in smart grid is restricted only to authorized people.

Nonrepudiation: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Integrity: This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.

IV. SECURITY THREATS FOR SMART GRID

Security threats within the smart grid usually attempt to compromise one or more security objectives. As the smart grid depends on computer networks, it is vulnerable to various security and privacy issues. A cyber attacker can penetrate a smart grid using variety of attacks. The physical layer security for smart grid deals unauthorized access, with malicious attacks, privacy issues, and voltage regulation.

Unauthorized Access: This broad threat covers a wide range of issues including access to data, devices, systems, and networks. Access control should include authentication, network access, and device authentication.

Malicious Attacks: Individuals can attack the communication infrastructure and cause damages to the smart grid. Malicious attacks can be classified as eavesdropping, jamming, and injecting [4]. A malicious, unauthorized individual can eavesdrop on the data transmission and access critical information, thereby violating the confidentiality requirements. Jamming blocks the information flow. An injecting attack inserts bad data into the network with the intension of misleading the control center.

Privacy Issues: Any personal information that may be available through the smart grid should be secured. This includes personal name, address, account number, bill history, the IP address of the meter, and service provider. We must strike a balance between security and privacy.

Computer networks do not exist in isolation. The human factor plays a unique role in cyber-defense operations. Average hackers, disgruntled former employees, terrorists, and foreign nations could be responsible for cyber attacks. To curb the flow of malicious attacks, analysts must monitor and protect smart grids [5].

V. SECURITY MEASURES

A reliable smart grid must have a protection approach that restricts adversary access and resilient power to operate appropriately during an attack. Efficient security measures should be implemented during the design, deployment, and operation of the smart grid. The cybersecurity controls for protecting the smart grid are shown in Figure 1. To secure a smart grid, it is important to have several mechanisms in place. These include authentication protocols, cryptographic algorithms, and firewalls [6].

Authentication: This confirms the identity of an entity that tries to access the network.

Firewalls: Network firewalls protect the smart grid assets against malicious cyber attacks.

Intrusion detection: Anomaly detection uses event correlation to identify cyber intrusions. The ability to prevent, detect, and tolerate intrusions is necessary in the smart grid systems.

Encryption: Providing encrypted communications among smart grid devices should be a basic requirement.

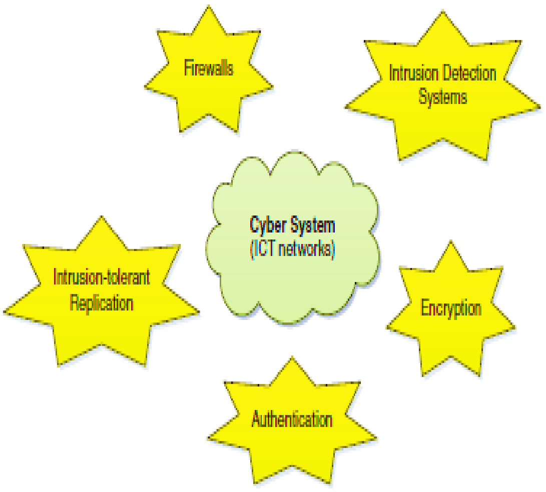
Firewalls
Intrusion Detection Systems
Cyber System (ICT networks)
Intrusion-tolerant Replication
Encryption
Authentication

Figure 1. Cyber security controls for the smart grid [6].

VI. CONCLUSION

Cybersecurity issues are critical for information infrastructure such as a smart power grid. As more and more information is made available on the web, critical infrastructures such as smart grids attract target from adversaries. Advanced network security in the form of intrusion detection system (IDS) and intrusion prevention system (IPS) will protect smart grids from many of the more advanced and emerging cyber threats. Standardization of cybersecurity for smart grid has been slow. The NISTIR 7628 is a comprehensive guideline for designing cybersecurity mechanism for the smart grid [7]. We should do more to protect the smart grid.

REFERENCES

[1] M. N. O. Sadiku, S. M. Musa, and S. R. Nelatury, "Smart grid—an introduction," *International Journal of Electrical Engineering and Technology*, vol. 7, no. 1, Jan-Feb, 2016, pp. 45-49.

[2] E. Y. Dari and M. Essaaidi, "An overview of smart grid cyber-security: state of the art study," *Proceedings of the 3rd International Renewable and Sustainable Energy Conference*, 2015, pp. 1-7.

[3] K. Tazi, F. Abdi, and M. F. Abbou, "Review on cyber-physical security of the smart grid: attacks and defense mechanisms," *Proceedings of the 3rd International Renewable and Sustainable Energy Conference*, 2015, pp. 1-6.

[4] X. Wang et al., "Physical layer security in wireless smart grid," *Security and Communication Networks*, vol. 8, 2015, pp. 2431-2439.

[5] R. S. Gutzwiller, "The human factors of cyber network defense," *Proceedings of the Human Factors and Engineering Society 59th Annual Meeting*, 2015, pp. 322-326.

[6] J. Xie, A. Stefanov, and C. C. Liu, "Physical and cyber security in a smart grid environment," *WIREs Energy and Environment*, vol. 5, Sept/Oct, 2016, pp. 519-542.

[7] NIST, "NISTIR 7628: Guidelines for smart grid cyber security," vol. 1-3, August 2010.

About the authors

Matthew N.O. Sadiku (sadiku@ieee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Mahamadou Tembely (mtembely@student.pvamu.edu) is a Ph.D student at Prairie View A&M University, Texas. He received the 2014 Outstanding MS Graduated Student award for the department of electrical and computer engineering. He is the author of several papers.

Sarhan M. Musa (smmusa@pvamu.edu) is an associate professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.