IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Strategic Integration of Cybersecurity in Power Transmission Systems for Enhanced Grid Resilience

Suman Mysore
Independent Researcher, Pittsburg, USA

Abstract: *As the role of power grids in society increases, cyber threats targeting them are also surging. Thus, power grid companies must enhance the cybersecurity status of their power supply systems. This writing asserts that comprehensive power grid cybersecurity must have prevention mechanisms, detection technologies, and response strategies. These mechanisms can be implemented at four levels: device and application security, network security, physical security, and policies, procedures, and awareness.*

Keywords: power grid, power supply system, cybersecurity, hackers, security

I. INTRODUCTION

The role of power transmission systems in society is widening day by day. Today, it is virtually impossible for people in the developed and semi-developed world to live without electricity. As more technologies rely on the grid, the role of power transmission systems become even more pronounced. While the increased reliance on power supply systems is occasioned by eco-friendly benefits, it comes with cybersecurity costs.

Cybercriminals prefer targeting high value systems. With increased dependence on the grid, power supply systems are among the most essential infrastructures in the community. Consequently, hackers prefer attacking them to compel respective governments to pay ransom. State-sponsored hackers may also target the grid to cripple economic activities of targeted states. Warring countries may also target each other's grid systems to disrupt communication and coordination efforts of enemy state. For example, in 2022, at the height of Russia-Ukraine conflict, Russia targeted Ukraine's power grid to sabotage their war efforts and dispirit the public [1]. China is another country that has been accused of using state-sponsored hackers to attack other countries' power grids [2].

Increased reliance on the grid creates new attack vectors for power supply systems. For example, introducing EV charging ports on the grid exposes the grid to cyber attackers in two ways. Modern electric vehicles are connected to the internet and are part of the Internet of Things (IoT). These vehicles are vulnerable to hackers on the internet who can use them as mediums to infect grids when they connect to charge [3]. EV charging stations use computerized systems to control charging load and prevent battery overcharging. These systems are usually networked over the internet. Their access to the internet exposes the grid to cyberattacks.

It’s not just the grid that is a victim of cyber criminals; the grid can also be used as a conduit for hackers to harm users. With the computerization of the grid, it is viable for hackers to use the grid as a channel to distribute malware to users [4]. For instance, with the increased use of power supply systems for EV charging, cybercriminals can use the grid to steal EV owners’ data such as addresses, social security numbers, and financial information. Some attacks are even designed to malfunction EV systems, causing damage to EV batteries or even locking owners from accessing their cars.

Increased reliance on power supply systems exposes both the systems and users to cybersecurity risks. Increased grid usage elevates its relevancy in the country, making it an ideal target for state hackers. On the other hand, as more people use the grid, hackers are finding it a viable attack interface to target the public. Therefore, it is integral grid operators safeguard the grid from cybersecurity threats.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

DOI: 10.48175/IJARSCT-15332

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

II. ATTACK TYPES

Some of the common types of cyberattacks on the grid include;

A. Physical attacks

These are direct attacks on power supply systems. They involve destruction of equipment, and their primary goal is to disrupt the availability of service to other consumers. Physical attacks are a type of denial of service (DoS) attack and can become distributed denial of service (DDoS) if conducted at a large scale [5].

B. Attack on access control

Access control manages how data is accessed in a system. It ensures all authorized persons in a system access data and resources required to complete their job while preventing them from accessing data and resources not needed for their job. Hackers may attack access control to masquerade as genuine users and access data in the system [6,7].

C. Attacks on cryptography

Data in transmission and at rest in power supply systems is given an additional protection layer through encryption. Attacks that attempt to illegally decrypt data in grid systems are classified as cryptography attacks. These attacks target public key infrastructure (PKI), which is commonly used in grid systems.

D. Attacks on firmware/software policy

Firmware and software programs in grids are usually programmed to upgrade to the latest versions autonomously through online updating. While this mechanism ensures systems are always up to date, it is vulnerable to attacks. Hackers can utilize this scheduled event to load a malicious version or software into the grid [8].

E. Software input validation

These are attacks that target underlying grid systems. These attacks include SQL injection, cross-site scripting, and cross-site request forgery. Espionage attacks/man-in-the-middle attacks are another form of attacks that target power grids.

III. INTEGRATION OF CYBERSECURITY IN THE GRID

Cybersecurity measures can be implemented anywhere in power supply systems. For example, they can be deployed in endpoint devices such as meters, network components such as transformers, and control systems such as software responsible for managing sub-stations. Though different types of cybersecurity measures are applicable in the grid, a well-secured power supply system must have three types of cybersecurity services: prevention, detection, and response services [8].

A. Prevention strategies

These are strategies that are put in place to proactively detect and thwart threats. Prevention strategies are core to the triad of confidentiality, integrity, and availability since they do not allow threats to gain access to systems. Typically, prevention strategies focus on preventing user processes from accessing privileged resources in the grid, such as grid servers and server configuration files [8]. Some of the most used models in prevention strategies include;

Access control

This strategy focuses on controlling how system users access data and how resources are assigned to them. Through authentication and authorization, access control ensures users are who they say they are and can only access resources required to accomplish their roles. Besides limiting access to system data and resources, access control plays an integral role in managing the spread of threats in a system. For example, if a hacker compromises a grid operator's account, the attack is limited to data accessible to the operator only. Access control is an integral strategy that can be deployed to prevent and contain the spread of attacks in power grids [9].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Firewalls

Firewalls are barriers between two networks that monitor traffic and only allow trusted traffic to cross over. Firewalls work based on the established security policies that define secure traffic and suspicious traffic [10]. In power grids, firewalls can be implemented in interfaces where internal networks communicate with external networks. For example, systems that connect to the internet should be fitted with firewalls. Similarly, endpoints such as EV chargers should be equipped with firewalls to block unwanted traffic.

Geofencing

Geofencing is a novel cybersecurity measure that leverages geographical locations of threats to block them. Geo-fencing technology detects the location where traffic is emanating and grants or rejects the connection. Geo-fencing is particularly useful for power supply systems since it can help track and block state-sponsored attackers. For example, why would traffic from Asia attempt to connect to Canada's power grid network? Geofencing can detect such traffic and plug it in real-time.

Penetration testing

Penetration testing is a security exercise in which white hat hackers attempt to find and exploit vulnerabilities in a system. The primary goal of penetration testing is to find and mitigate vulnerabilities before adversaries can exploit them. Penetration testing can also help cybersecurity experts prepare to respond to security eventualities in grid systems [11].

Threat intelligence

Threat intelligence is evidence-based information about cyberattacks. This information includes attack mechanisms, strategies for detecting the attacks, the impact of the attack on the grid, and strategies for defending against the attacks. Security experts use insights from threat intelligence to proactively protect their systems and defend them promptly in case of an attack.

B. Detection strategies

These are strategies for flagging specific actions and signatures and monitoring the whole system for suspicious processes. The primary goal of detection strategies is to identify threats timely so that security teams can respond before significant damage is orchestrated in the system. Some of the detection strategies that can be employed in power grid systems include;

AI monitoring

One of the core applications of AI in the grid is threat detection. AI-powered cybersecurity systems can detect cyber threats in grid systems and report them in real time, allowing cyber teams to respond quickly. Besides detecting threats, AI cybersecurity systems can autonomously respond to threats by blocking them or recommending mitigation strategies to security teams [12, 16].

Threat hunting

As per the name, threat hunting is the practice of proactively searching for threats in a network that may be undetected. Threat hunting is suitable for searching stealthy attacks capable of manoeuvring conventional security defences and remaining in the network for long-term data collection. Grid operators can enhance their system's cybersecurity by hiring professionals who can regularly scan their networks to identify potential ongoing attacks.

Intruder traps

This is an emerging technology in cybersecurity. Intruder traps are virtual replicas of burglar detection motion sensor systems. They work by deceiving and luring attackers to reveal themselves before they can access actual data and system resources. Fake assets and data are scattered throughout the IT environment [13]. System administrators are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

informed when attackers interact with these baits, allowing them to kick intruders out or monitor them to gather intelligence.

C. Response

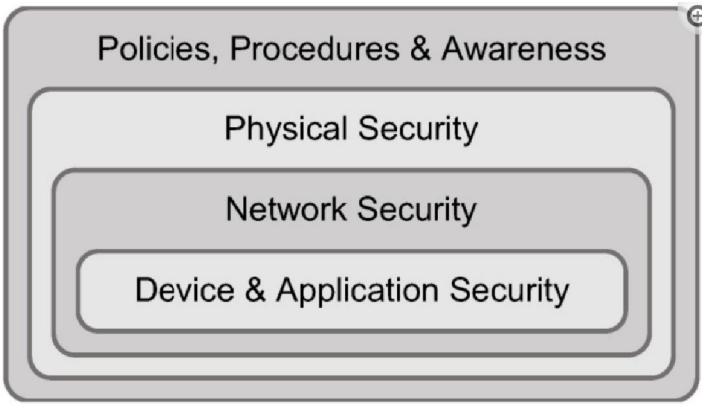
The last aspect of comprehensive cybersecurity in power grid systems is containing threats and recovering. Containing an attack involves stopping it from spreading in the network and further siphoning off data. This process may involve taking some components of the systems offline and only reintegrating them after the threat is cleared. The recovery process involves reversing the impact of a threat in the system. This may include data recovery for corrupted files and resolving jammed networks. A comprehensive response should include mitigation of vulnerabilities that allowed the attack.

D. Physical security

Grid cybersecurity is not just about virtual security; it also entails aspects of physical asset security. Most energy companies use power cables for process control networks (PCN)communications. While this mechanism enhances the cybersecurity status of their networks, they can easily be compromised when attackers gain access to physical network devices [14]. Thus, the cybersecurity of power grid systems should include strategies such as tamper detection, video surveillance, monitoring of critical components such as transformers and substations, and physical access control to vital areas such as server rooms. Other strategies, such as burying electric cables underground or hoisting them very high above the ground, can be used to enforce physical security in grid networks.

IV. CONCLUSION

To comprehensively safeguard power grids from cyber threats, security is implemented at four levels: device and application security, network security, physical security, and policies, procedures, and awareness [15].



Device and application security is implemented in individual applications and devices on the grid network. Network security focuses on protecting communication pathways in the grid. Network security entails methods such as network separation and intrusion detection systems. As aforementioned, physical security constitutes measures that protect and detect physical assault on grid infrastructure. The last layer, policies, procedures, and awareness, focuses on controlling the impact of human behaviour on grid security. Policies and procedures dictate how grid resources and devices should be handled to reduce risk. Awareness educates grid workers on impeding cybersecurity risks and how they can help minimize their impact on the grid

REFERENCES

[1]. Reuters, Russia hits Ukraine power grid and gains ground in east. Retrieved From: https://www.reuters.com/world/europe/zelenskiy-vows-changes-will-bolster-ukraine-amid-defence-minister-uncertainty-2023-02-06/ ,(2023)

[2]. Wired, China-Linked Hackers Breached a Power Grid—Again. Retrieved From: https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/, (2023)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

[3]. Acharya, Samrat, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. "Cybersecurity of smart electric vehicle charging: A power grid perspective." IEEE Access 8 (2020): 214434-214453.

[4]. Energy5, Cybersecurity Threats to EV Charging Stations. Retrieved From: https://energy5.com/cybersecurity-threats-to-ev-charging-stations, (2023)

[5]. McCary, Eric, and Yang Xiao. "Smart grid attacks and countermeasures." EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 2, no. 2 (2015).

[6]. Cheung, Helen, Alexander Hamlyn, Todd Mander, Cungang Yang, and Richard Cheung. "Strategy and role-based model of security access control for smart grids computer networks." In 2007 IEEE Canada Electrical Power Conference, pp. 423-428. IEEE, 2007.

[7]. Chen, Xinyi, and Hyun Sung Kim. "RBAC for home area network based smart grid." 한국정보기술융합학회논문지 3, no. 2 (2010): 95-101.

[8]. Young, E. Attacking the Smart Grid, (2011)

[9]. Ruj, Sushmita, Amiya Nayak, and Ivan Stojmenovic. "A security architecture for data aggregation and access control in smart grids." arXiv preprint arXiv:1111.2619 (2011).

[10]. Rao, Umesh Hodeghatta, and Umesha Nayak. The InfoSec handbook: An introduction to information security. Springer Nature, 2014.

[11]. Atalay, Manolya, and Pelin Angin. "A digital twins approach to smart grid security testing and standardization." In 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, pp. 435-440. IEEE, 2020.

[12]. Ruan, Jiaqi, Gaoqi Liang, Junhua Zhao, Huan Zhao, Jing Qiu, Fushuan Wen, and Zhao Yang Dong. "Deep learning for cybersecurity in smart grids: Review and perspectives." Energy Conversion and Economics 4, no. 4 (2023): 233-251.

[13]. Bushby, Andrew. "How deception can change cyber security defences." Computer Fraud & Security 2019, no. 1 (2019): 12-14.

[14]. Xie, Jing, Alexandru Stefanov, and Chen‐Ching Liu. "Physical and Cybersecurity in a Smart Grid Environment." Advances in Energy Systems: The Large‐scale Renewable Energy Integration Challenge (2019): 85-109.

[15]. Krause, Tim, Raphael Ernst, Benedikt Klaer, Immanuel Hacker, and Martin Henze. "Cybersecurity in power grids: Challenges and opportunities." Sensors 21, no. 18 (2021): 6225.

[16]. Mysore, Suman, "Role Of Artificial Intelligence In Grid Modernization: Exploring How AI Can Enhance Grid Management, Predict Energy Demand, And Optimize Renewable Energy Usage." International Research Journal of Modernization in Engineering Technology and Science 6, no. 1 (2024): 1776-1780.