Western Interconnection Cybersecurity and Mission Assurance

Jayden Lyons

CYBR370

Norwich University

Executive Summary

Due to an ominous escalation in cyberattacks targeting vital industrial infrastructure, ensuring the safety and security of the Western Interconnection power grid represents an increasingly critical priority for U.S. national security. Significant cyberattacks on vital industrial systems around the world in recent years have raised the stakes for industrial control systems cybersecurity in America. Enemy attacks on the Western Interconnection power supply can be initiated as a direct physical attack against the grid or in the form of a sophisticated cyberattack exploiting the digital systems controlling the Western Interconnection. Cybersecurity concerns regarding the Western Interconnection also include new vulnerabilities introduced with the integration of evolving technologies, IT-integrated operational technology, poorly configured software, supply chain technology, and insecure IoT devices significantly expanding its attack surface. This report explores the current cyberthreat landscape for the Western Interconnection and provides guidance and recommendations for an effective cybersecurity architecture to protect the Western Interconnection power system.

1

I. Western Interconnection Cyberthreat Landscape

The Western Interconnection power grid is one of three main interconnections that supply electricity to the continental United States. Nearly 20% of the entire North American population rely on electricity generation and transmission from the Western Interconnection. The Western Interconnection operates independently and facilitates the distribution of electric power to 14 states on the west coast, serving a U.S. population of over 80 million. The Western Interconnection is a complex physical grid consisting of 136,000 miles of transmission lines, operated and controlled by 34 balancing authorities and 500 companies in the U.S., providing all of the electric, natural gas, hydroelectric, nuclear, wind, and solar power for the Western region. Industrial Control System (ICS) networks manage the production and distribution of electricity through a network of power plants, distribution substations, and electronic devices and controls (Congressional Research Service, 2018). Though the Western Interconnection is historically reliable, the network is vulnerable to significant failures due to natural, operational, or man-made events and evolving cyberthreats (Congressional Research Service, 2018). A sophisticated cyberattack via malware disseminated in its ICS network may result in catastrophic loss of life, damage and destruction of a public utilities system, and remote control of critical system operations of the Western Interconnection by foreign adversaries.

Adversarial threats to the ICS network managing the Western Interconnection power grid may arise from a plethora of sources from terrorist groups to disgruntled employees to foreign state-sponsored hackers. The Western Interconnection is an extremely ambitious target for any bad actor and would most likely require a threat agent to have nation-state level technical skills, an in-depth understanding of ICS engineering and processes, and considerable confidence to even attempt to compromise the system. Therefore, the Western Interconnection would not be an attractive target for opportunistic hackers or attackers seeking to steal data, spy on communications, or leverage monetary payment. Without an obvious financial or cyberespionage angle, the most likely objective of a threat agent targeting the Western

2

Interconnection is to disrupt, destroy, manipulate, or control an ICS process thereby compromising the grid’s operation. The targeting of critical infrastructure to disrupt, degrade, or destroy systems is consistent with numerous attacks engaged in by Russian, North Korean, and Iranian nation state actors, and intrusions of this nature may be with immediate intent or in preparation for a contingency (Johnson et al, 2017). Considering the high level of expertise and resources required to successfully execute a cyberattack of this nature, an advanced persistent threat (APT) group with unlimited financial resources and full support of a foreign nation-state represents the highest priority adversary and threat to ICS systems and national security.

APT groups are highly skilled in deploying both traditional and advanced malware, social engineering attacks, and strategic web compromise. APT groups are the most dangerous type of adversary because they are prepared to invest an unlimited amount of time and resources to develop the necessary sophisticated attack tools and to achieve the objective mandated by their government (Chapple & Seidl, 2015). APT groups also have little risk aversion because they are essentially carrying out the orders of their government with the expectation they will be protected by their nation-state and thus are confident in their ability to avoid detection and prosecution.

A state-sponsored APT group is certainly capable of carrying out an attack on the Western Interconnection power grid by deploying, for example, Industroyer, a devastating new strain of ICS malware specifically designed to target power grids. Cybersecurity experts suspect Industroyer code was utilized in a 2016 cyberattack on an electrical substation in Ukraine (Paganini, 2017). Analysis of Industroyer code revealed an advanced malware featuring multiple backdoors enabling remote control and execution, at least 4 payloads enabling circuit breaker control, a denial of service (DoS) attack against protection relays, and a wiping tool to cover their tracks and make it difficult to restore systems (Paganini, 2017). The creators of Industroyer are cunning and went to great lengths to create malware capable of directly controlling ICS switches and circuit breakers (Paganini, 2017). Industroyer malware can be installed in a network covertly via phishing or social engineering lure, human error, malicious insider,

3

security gap, or remote access trojan among other methods. Upon accessing the network, a launcher is installed through a backdoor, which initiates the malicious payloads and wiper while the command and control server is hidden in the Tor network on the dark web.

This wicked new class of ICS malware including Industroyer is designed to cause maximum mayhem and destruction of vital industrial systems such as Western Interconnection power grid. Most industrial networks lack even basic security such as access control, network monitoring, threat detection, security logging and auditing, which only magnifies the larger problem facing ICS networks (Perelman, 2018). The figure below applies the cyber kill chain to the Industroyer attack and summarizes the steps an APT group would likely take to intrude on an ICS network to achieve their objectives.

A screenshot of a cell phone

Description automatically generated

Figure 1.1 Industroyer Cyber Kill Chain

4

In order to combat the cyber kill chain and thwart cyberattacks as early in the process as possible, U.S. industrial power systems need to harden ICS security and develop an incident response plan to optimize early detection and restoration of compromised systems to mitigate any potential disruption of the Western Interconnection.

The diagram below illustrates the steps required to eradicate Industroyer malware.

A close up of text on a white background

Description automatically generated

Figure 1.2 ICS Malware Containment and Removal Process

5

II. Defense in Depth Architecture

ICS networks control the electric production, transmission, operation, monitoring and reporting for U.S. energy systems including the Western Interconnection. An ICS network makes thousands of decisions in real time to ensure the safe and reliable operation of the Western Interconnection power grid. A multilayered approach emphasizing a defense in depth security architecture should be implemented to secure ICS networks managing the Western Interconnection in response to an increasing number of cyberattacks targeting critical infrastructure and a rapidly evolving cyberthreat landscape. Hardening systems with defense in depth requires the integration of multiple security protocols implemented in each network layer. Security measures focusing solely on the network perimeter is likely suboptimal considering the evolution of cyberthreats targeting ICS networks and critical infrastructure.

A network can be divided logically in 5 layers from the innermost device, application, and computer layers to the network and physical layers encompassing the logical and physical network perimeter. An ICS network must be secured from the physical layer of infrastructure inward to the core device level. Physical security is paramount because technical controls become ineffective if an attacker can gain physical access to network computers, servers, system devices and components. Physical security including guards, cameras, dogs, locks on doors, gates, keycards, etcetera is always the first line of defense against intrusion and physical access to facilities.

Within the network layer, weak security protocols and suboptimal network configuration and segmentation are vulnerabilities attackers can exploit to gain access through the network layer. The network perimeter should be secured with technology including firewalls, network access controls, intrusion detection and prevention systems (IDS/IPS), zoned LANs, VLANs, demilitarized zones (DMZ), and secure routers and switches. Software code vulnerable to manipulation may create an access point for intrusion and compromise within the computer and application layers. Security protocols including antivirus software, host and wireless IDS/IPS, port management,

6

secure patches and updates should be implemented to secure the computer level within an ICS network. Software and firmware integrity and authenticity should always be verified, and vendor risk management controls established (Congressional Research Service, 2015). According to a Kapersky lab report, the main source of infection on ICS computers is the Internet with 27% of attacks received from web sources, 8.4% from removable media, and 3.8% from email attachments, including employees attempting to access known malicious and phishing web pages (Seals, 2018). Thus within the application layer, security measures such as access control mechanisms, packet firewalls, user authentication, secure passwords, content filters, and application whitelisting should be implemented to help protect against malware injection through Internet web apps and other attacks. The most pervasive vulnerability is malware being deployed in the computer and/or application levels and persisting undetected in the network. However, due to the expansion of IoT devices and integration of IT and OT in industrial environments, device level attacks are on the rise as well. IoT devices are manufactured with minimal to no embedded security, inevitably creating additional security vulnerabilities when utilized in ICS networks. Therefore, hardening ICS network security with a well-designed defense in depth architecture is the most effective method to safeguard the security and reliability of the Western Interconnection.

An important factor to consider in our approach to harden the security of ICS networks, however, is the impact on speed and performance. Defending today’s power systems is challenging because ICS networks typically use communication protocols optimized for bandwidth and efficiency (Carullo, 2019). ICS communication is not encrypted, thus, all network traffic travels in plain text and is potentially vulnerable to data leaks. However, encryption and additional security protocols may create latency and hinder the time-sensitive ICS processes controlling the power supply from the Western Interconnection. Encryption, in fact, may not be necessary in an ICS environment because integrity and availability are the primary concerns. However, if deemed necessary, encryption technology such as virtual private networks (VPN) with IPsec and SSL/TLS can be implemented safely in specific areas to provide an additional

7

layer of defense. Encryption in the data link layer should be considered rather than in

the network layer to reduce encryption latency (Stouffer et al, 2015). Cryptographic hashes can also be incorporated safely in an ICS environment according to NIST guidelines (Stouffer et al, 2015).

Malware technology seems to be advancing more rapidly than cyber defense technology. The NSA’s Information Assurance defense in depth strategy provides a three-pronged holistic approach to cybersecurity to optimize network security against rapidly evolving cyber threats. The first component in the NSA model is people. The NSA’s people-focused approach emphasizes hiring talented staff, training, and rewarding them, and penalizing unauthorized and unacceptable behavior (Chapple & Seidl, 2015). Robust multilayer security will falter if employees, managers, operators, and administrators have no idea how to properly utilize and maintain the security protocols and procedures in place. Proper training of all employees regarding their role in maintaining network security and following best practices for securing all devices connected to an ICS network is essential to ongoing security maintenance. This includes basic workstation security such as not clicking on links from unknown sources, not installing rogue access points, avoiding policy or procedure breaches, removing unnecessary apps, and keeping computers and servers clean and up to date with approved patches and updates.

The second component of the NSA defensive model focuses on technology and how technology is configured, implemented, and monitored within multiple network layers to achieve defense in depth. The objective in layering security technology is to create a resilient network, so the power supply from the Western Interconnection is not interrupted when adverse events occur. The third component of the NSA cybersecurity framework is operations. Operational security includes daily activities, security policies and procedures, security monitoring and management, key management, testing configurations, software patches and updates, incident response and recovery planning. Therefore, an optimal security architecture for ICS networks is one that significantly improves security and ensures integrity and availability without hindering production or

8

distribution from the Western Interconnection.

III. Network Resiliency and Mission Assurance

The Department of Defense (DOD) defines mission assurance of critical industrial infrastructure as the ability to provide continuous operation despite cyberattacks, system failures, and other temporary disruptions. For an enterprise network, this concept is defined as resilience and is the primary objective of network security in the corporate world as well. As noted previously, the highest priority cyberthreat to the Western Interconnection power grid is a sophisticated and targeted attack attempting to manipulate ICS networks. Therefore, worst case scenario, the DOD mandates a process be in place to ensure the Western Interconnection continues to operate while potentially compromised controlling systems are sanitized and restored. Achieving mission assurance for the Western Interconnection involves designing, implementing, and maintaining network security and resilience through defense in depth and a fault tolerant ICS network. It also involves having a strong set of operational procedures and an effective incident response and disaster recovery plan.

An ICS is a collection of control systems, networks, electronic controls, and devices used to digitally manage industrial processes. There are 2 types of ICS, SCADA systems and distributed control systems (DCS). Together these systems are responsible for managing the Western Interconnection power grid. SCADA systems are composed of computers, data communications, graphical user interfaces and other peripheral devices for supervisory management of industrial processes and can acquire and transmit data with centralized monitoring. The primary function of a SCADA system is to provide automated data acquisition and long-distance monitoring and control of field sites through a centralized control system. A DCS controls an industrial process in a single location by managing local controllers and devices. An ICS environment for power systems is usually a combination of SCADA and DCS systems.

The ICS environment controlling the Western Interconnection power grid also

9

contains components of information technology and operational technology (OT), which is the hardware, software, or firmware that controls physical devices in the field. The integration of IT and OT enhances visibility of the supply chain and operational processes, but also introduces a new security vulnerability in grid management by increasing the number of internet connections used to manage the production and transmission of electricity. Internet of Things (IoT) devices connected to ICS networks represent a growing security vulnerability as well. Attackers are increasingly targeting IoT devices to gain access to ICS networks to inject malware and malicious payloads, launch denial of service attacks, and other malicious attacks. The introduction of digital smart grid technology developed to modernize grid operations is another potential ICS security vulnerability. Along with the proposed benefits of advanced OT and improved grid efficiency comes the potential risks associated with increasing the number of IT controls connecting industrial processes to the Internet. From the perspective of network security, the Internet is an untrusted network and despite all the perceived benefits, more exposure to the Internet expands the attack surface exponentially and creates more security risks for the Western Interconnection.

Considering an expanding attack surface for industrial systems, effective network segregation is particularly important for securing ICS networks. Network segregation separates an ICS network from corporate and other networks and establishes security domains grouped together based on sharing the same management authority, policy, level of trust, level of function, and communication traffic (Stouffer et al, 2015). The goal of network segmentation and segregation is to restrict access to sensitive information and ensure that an organization can continue to operate effectively (Stouffer et al, 2015). Network segmentation is achieved utilizing security technologies including firewalls, DMZ, VLANs, unidirectional gateways, network, port, and application filters as well as physical network separation. The boundaries between interconnected security domains also need to be protected utilizing firewalls, routers, gateways, intrusion detection systems, managed interfaces, and encrypted tunnels (Stouffer et al, 2015). Computer, application, and data level security technologies supporting network

10

segregation include access control lists, application whitelisting, host IDS/IPS, VPN and encryption protocols.

In addition to traditional technologies, new technologies are being developed to enhance power system resiliency as well. For example, Smart grid technology featuring sensors and automated controls capable of using real-time data to reconfigure a utility network has been proposed for reliability and resiliency (Congressional Research Service, 2018). Managing the human element, however, is perhaps the most challenging aspect of hardening ICS networks to achieve mission assurance. A vast majority of breaches are caused by employees falling victim to phishing and social engineering attacks providing attackers entry into the network. Multifactor authentication is an effective technique to mitigate the human element by requiring two or more credentials to authenticate and gain network access, including biometric and security token technology (Congressional Research Service, 2018). Securing the human element is best achieved through a combination of technology including multifactor authentication, access control, network segregation, account control and monitoring in addition to effective policies and procedures including strong password policies and administrative procedures. Security education for employees including social engineering awareness programs is equally as important and serves to educate employees on the important role they play in maintaining network security.

Operational procedures supporting network resilience and mission assurance focus on the day to day security activities and ongoing management of an ICS network controlling the Western Interconnection. Operating procedures standardize security policy and management, updates and patch management, key management, security audits and assessments, early detection and incident response, recovery and restoration, and administrative privileges (Chapple & Seidl, 2015). Operating procedures should be in accordance with federal industry standards, NSA, and NIST guidelines to ensure the strategic integration of people, technology, and organizational

management achieves mission assurance in the energy sector and preserves national

security. The single greatest threat to U.S. critical infrastructure is a sophisticated

11

cyberattack capable of corrupting safety controls, remotely controlling system

processes, damaging, disrupting, or disabling vital infrastructure in the energy sector.

Therefore, a robust, multilayered security architecture that optimizes the role of people,

technology, and operations to safeguard the Western Interconnection and preserve U.S.

national security is the best defense against evolving cyberthreats in the modern world.

12

References

Carullo, M. (2019). “IEC 62351 Standards for Securing Power System Communication.” Web. Retrieved from <https://www.nozominetworks.com/blog/iec-62351-standards-for-securing-power-system-communications/>

Chapple, M. and Seidl, D. (2015). Cyberwarfare: Information Operations in a Connected

World. Burlington, MA: Jones & Bartlett Learning.

Congressional Research Service, (2018). “Electric Grid Cybersecurity.” Web. Retrieved from <https://fas.org/sgp/crs/homesec/R45312.pdf>.

Johnson, Caban, Krotofil, Scali, Brubaker, Glyer, (2017). “Threat Research: Attackers Deploy New ICS Framework ‘Triton’ and Cause Operational Disruption to Critical Infrastructure.” Web. Retrieved from <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>

Paganini, P. (2017). “Which Malware are Specifically Designed to Target ICS Systems?” Web. Retrieved from <https://resources.infosecinstitute.com/malware-specifically-designed-target-isc-systems/#gref>

Perelman, B. (2018). “The Rise of ICS Malware: How Industrial Security Threats are Becoming More Surgical.” Web. Retrieved from <https://www.securityweek.com/rise-ics-malware-how-industrial-security-threats-are-becoming-more-surgical>

Seals, T. (2018). “Threatlist: Attacks on Industrial Control Systems on the Rise.” Web. Retrieved from <https://threatpost.com/threatlist-attacks-on-industrial-control-systems-on-the-rise/137251/>

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). “NIST Special Publication 800-82: Guide to Industrial Control System Security.” Web. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

13