Western Interconnection Cyber Security and Mission Assurance

Part III: Network Resiliency and Mission Assurance

Jayden Lyons

CYBR370

Norwich University

03/07/2020

The Department of Defense prioritizes mission assurance of critical industrial infrastructure as the ability to provide continuous operation despite cyberattacks, system failures, and other temporary disruptions. Mission assurance in terms of a computer network is defined as resilience and is the primary objective of network security in the corporate world as well. As noted previously, the highest priority cyber threat 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 assure the Western Interconnection continues to operate while controlling systems are sanitized and restored. This process involves designing, implementing, and maintaining network security and resilience through defense in depth and a fault tolerant ICS network architecture. It also involves having a strong set of operational procedures and effective incident response plan. One concern with ICS networks controlling the Western Interconnection is the increasing number of internet connections utilized to manage the production and transmission of electricity. From the perspective of ICS network security, the Internet is an untrusted network and despite all the benefits, more exposure to the Internet expands the attack surface and introduces more security risks.

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) are responsible for managing the Western Interconnection power grid. SCADA systems are composed of distributed PLC devices and can acquire and transmit data with centralized monitoring. The primary function of SCADA 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 is usually a combination of SCADA and DCS systems. The ICS environment controlling the Western Interconnection power grid also contains components of information technology (IT) 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.

Within an effective security framework, network segregation is an important design concept that must be implemented to secure an ICS network. 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). This resiliency and network segmentation can be 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 techniques and technologies include access control lists, application whitelisting, host IDS/IPS, VPN and encryption protocols.

Another factor in ICS network security is managing the human element. 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 employs security technology 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). 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).

Operational procedures supporting ICS security focus on the day to day security activities and ongoing management for 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.

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>