Western Interconnection Cyber Security and Mission Assurance

Part II: Western Interconnection Defense in Depth Architecture

Jayden Lyons

CYBR370

Norwich University

03/07/2020

ICS networks control the electric production, transmission, operation, monitoring and reporting for the Western Interconnection power grid. Insider threats, malware, ransomware, social engineering, mobile devices, IoT devices among others represent vulnerabilities in an ICS network. An enterprise computer 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. Multiple security measures implemented in each logical layer constitutes a defense in depth architecture.

Security controls are ineffective if an attacker can gain physical access to network computers, servers, and system devices. 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. Weak network 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 is also vulnerable to manipulation creating an access point for ICS network intrusion within the computer and application layers. Security protocols including antivirus software, host and wireless IDS/IPS, port management, 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). 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. The most pervasive vulnerability is malware being deployed in the computer and/or application levels and persisting undetected in the network. Device level apps, however, are becoming more of an appetizing target as well with the expansion of IoT devices and integration of IT and OT in industrial environments. These devices are manufactured with minimal to no embedded security, which creates an additional security vulnerability.

An important factor to consider in our approach to harden the security of ICS networks 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 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 paramount. 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 cyber security 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. ICS networks make thousands of decisions in real time to ensure the safe and reliable operation of the Western Interconnection power grid. Therefore, an optimal security architecture for ICS networks is one that significantly improves security and ensures integrity and availability without hindering production or distribution from the Western Interconnection grid.