INL/JOU-15-36770
Accepted Manuscript

Cyber Hygiene for Control System Security

David Oliver

October 2015

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Prepared for the U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyber Hygiene for Control System Security

By: David Oliver, Control Systems Researcher, Idaho National Laboratory

Cisco is projecting that by 2020, 50 billion devices will have web connections[1]. At the same time, network intrusions are on the rise and the annual global cost of digital crime exceeds $445 billion[2]. Companies across the globe are facing the reality that their data, intellectual property, and control systems are at risk. Once a rarity, incidents of hackers compromising high-profile companies are becoming commonplace.

In 1997, the President's Commission on Critical Infrastructure Protection issued a report that said, "We found no evidence of an impending cyber-attack which could have a debilitating effect on the nation's critical infrastructure"[3]

Seventeen years later, in 2014, Admiral Michael Rogers stated in testimony before the House Select Intelligence Committee that, "There shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability to do that, to enter our systems, to enter those industrial control systems, and to shut down, forestall our ability to operate our basic infrastructure"[4].

BlackEnergy is a recently discovered malware that specifically targeted a known vulnerability in the human-machine interface (HMI) applications of three major control systems vendors. The active malware became public knowledge a year after the vendors had patched their software and three years after attackers had been using it to gain access to victim networks[5]. BlackEnergy attacked computers running the software with a direct connection to the Internet[6]. The 88 known variants of the Havex malware infected victim machines using a watering hole attack, an infected website, to gain a network foothold[7]. Another attack vector from recent headlines, this one from the Target hack involved compromised credentials from an HVAC control systems vendor which allowed the attackers to pivot into their network[8]. There are many ways to compromise a network. IT staff at companies everywhere must perfectly defend every path into their respective networks, whereas attackers need only exploit a single weakness.

A quick comparison of the urgency conveyed in the quotes above reveals a growing concern for the security of our nation; especially with regard to critical infrastructure. Securing our nation's critical infrastructure those structures, goods, and services we rely on to make modern life possible is a hot-button issue from corporate boardrooms to the floors of Congress. The problem is significant. With hundreds of thousands of assets spread across 16 critical infrastructure sectors including millions of miles of pipelines, communication and power lines, roadways and railways, identifying the scope of the problem is difficult. To further complicate matters, an estimated 85% of US critical infrastructure assets are owned by the private sector[9] where a business case must be made for every dollar devoted to security.

The Internet of Things

Prior to the advent of the Internet, little thought was paid to securing the data connection to the components of a water treatment plant or power transmission substation. Money and manpower were expended to secure the space those components occupied. Guns, guards, and gates were the main focus. Today, while it is still important to secure the physical location of these components, attackers realize that targeting a company's network is easier and less expensive than a physical attack. Physical guns, guards, and gates are bypassed by hackers and attacks can come from any direction and any distance. Increasingly, the biggest weakness to a company's network comes from inside that network. A recent study by CompTIA an IT trade association cited that while human error was the cause for 52 percent of all security breaches, only 54 percent of companies offer any training in cyber security[10].

As we move toward the Internet of Things, with sensors and machines talking to each other and making decisions without human interaction or oversight, the number of devices available for attack is growing exponentially. Many of these devices employ embedded systems running third-party software. Often hundreds of vulnerabilities discovered in these systems each year remain unpatched due to the difficulty in updating the device. The recent Heartbleed vulnerability found in the SSL algorithm manifested in thousands of devices running the software and persists in unpatched devices.

Control systems have been communicating this way for years. Long-distance monitoring of substation equipment or remote wells by a central command center has been the accepted practice at many companies. To assist companies with keeping costs down while maintaining connectivity to remote equipment, manufacturers have begun releasing network-enabled devices, often with built-in web servers and human-machine interface (HMI) applications. While these devices help to keep operating costs low, too often security is implemented as an afterthought or left off completely leaving them vulnerable to exploitation. Using the Internet as a transport mechanism for control systems data often translates the vulnerabilities in the device into access to the larger company network. Specialized search engines such as SHODAN supply a ready-made listing of internet-facing devices that attackers can query as part of their attack research[11].

Control Systems Cyber Hygiene

As part of an effort to engage control systems owners and operators across the 16 critical infrastructures sectors, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) recently delivered a presentation at the May 2015 Industrial Control Systems Joint Working Group Spring Conference in Washington, D.C. Listed below are the top ten NIST categorized vulnerabilities[12] and recommended mitigations for each, taken from that presentation based on data from assessments conducted during the first two quarters of fiscal year 2015:

10. Least Privilege (AC-6) - Also called Least User Access, this vulnerability group deals with users having more security privileges than absolutely necessary. End users with local administrator accounts and widespread use of Domain Administrator accounts allow attackers

to exploit additional machines with higher privileges. To reduce this risk, establish user accounts for administrators and only use those accounts when necessary.

9. Configuration Change Control (CM-3) - Not involving the critical parties in making changes to the control systems network as well as not keeping records of changes made will render any knowledge of how the control systems operate obsolete. An established and enforced change control process will ensure that the control systems operations and maintenance staff know how the system is configured resulting in reduced diagnostic times as new system problems arise. A known configuration will also provide a baseline of what “normal” traffic looks like on the network.

8. Physical Access Control (PE-3) - Unsecured doors at the main office as well as at remote sites, as well as improper management of physical keys provide an easy entry point for attackers without requiring any advanced “hacking” skills. Implementing a security plan using access alarms and video surveillance will inform security personnel when an area has been breached. Utilizing electronic magnetic or RFID cards assigned to each user and deactivated as the user leaves the organization will help ensure that the areas are inaccessible to unauthorized persons.

7. Audit Generation (AU-12) - As mentioned in Configuration Change Control above, understanding normal network traffic patterns allows automated processes to identify anomalous traffic for review by cyber security analysts. Often control systems network traffic is not logged or reviewed in a timely manner. Logging traffic and collecting those logs in a central repository will enable analysts to identify a breach while making it more difficult for attackers to hide their activities by erasing log entries.

6. Security Awareness Training (AT-2) - Cyber security topics are often very technical and discussing them amongst users on the company’s network often results in confusion and mis-information. A standardized training program geared toward the layman users, those without extensive cyber security training will allow everyone in the organization to speak the same language with regard to computer security and will raise the overall security posture of the organization.

5. Authenticator Management (IA-5) - Long-term passwords and passwords of insufficient length or complexity make exploiting systems easier for an attacker. Establishing and enforcing password policies and processes such as requiring complex passwords over 12-15 characters be changed regularly strengthens security by invalidating passwords that may have been compromised previously.

4. Allocation of Resources (SA-2) - Economic times are tough and many companies are being forced to ask their IT staff to do more with fewer resources. Some companies are outsourcing their security altogether. These may be financially sound decisions in the moment but open security holes. Overworked IT personnel have a higher probability of missing an intrusion and outsourced staff may not be properly vetted resulting in an increased insider threat. As

resources permit, employing a dedicated, trained, on-site staff of appropriate size reduces the organization's overall attack surface.

3. Least Functionality (CM-7) - Many times when a device is installed, ports not required for it to operate on the network are left open, protocols are enabled and services are left available. This allows an attacker to exploit the default configuration of that device as a means of ingress into the network. The time taken as a device is installed to understand the default configuration and disable or close unnecessary ports, protocols and services will restrict their unauthorized use during an attack.

2. Identification and Authentication (IA-1) - Closely related to Authenticator Management, many organizations do not encrypt their password storage or require multi-factor authentication for external access to network resources. Often these situations are viewed as unlocked doors to attackers who, when entering the network have easy access to credentials for all of the users of that network. Strong encryption of stored credentials and employing systems that encrypt passwords before transmitting them are best to deny attackers access to additional credentials. Multi-factor authentication for access to the network from the outside further reduces the risk of compromise.

1. Boundary Protection (SC-7) - The most cited issues with network security come from the network architecture employed by many companies. Large, flat networks lacking internal boundaries enable attackers to move among all of the devices on that network without having to compromise additional nodes. Lack of traffic monitoring, especially of outbound traffic restricts analysts ability to identify data exfiltration, a major indicator of compromise. Re-architecting the network to group devices with similar traits or uses into logical groups using firewalls to route or deny traffic will restrict malicious movement through the network. Logging traffic for review and denying traffic by default will help analysts identify a breach and will help reduce data loss if a breach occurs.

There are many resources from government and private industry available to assist organizations in reducing their attack surface and enhancing their security posture. Standards are being written and improved upon to make the practice of securing a network more manageable. While the specifics of network security are complex, most system vulnerabilities can be mitigated using fairly simple cyber hygiene techniques like those offered above.

---

[1] "Hacking the Planet." The Economist. July 18, 2015. Accessed September 29, 2015. http://www.economist.com/news/leaders/21657811-internet-things-coming-now-time-deal-its-security-flaws-hacking.

[2] "Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies. June 9, 2014. Accessed September 29, 2015. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[3] Marsh, Robert. "Critical Foundations: Protecting America's Infrastructure." October 1, 1997. Accessed September 29, 2015. https://fas.org/sgp/library/pccip.pdf.

[4] Rogers, Michael. "Cybersecurity Threats: The Way Forward." Hearing of the House (Select) Intelligence Committee. November 20, 2014. Accessed September 29, 2015. https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.

[5] Lucian, Constantin. "Attack Campaign Infects Industrial Control Systems with BlackEnergy Malware." PCWorld. October 29, 2014. Accessed September 29, 2015. http://www.pcworld.com/article/2840612/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware.html.

[6] "Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)." ICS-CERT. December 10, 2014. Accessed September 29, 2015. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[7] Walker, Danielle. "Havex Malware Strikes Industrial Sector via Watering Hole Attacks." SC Magazine. June 25, 2014. Accessed September 29, 2015. http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/

[8] Krebs, Brian. "Target Hackers Broke in Via HVAC Company." Krebs on Security RSS. February 15, 2014. Accessed September 29, 2015. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[9] "Critical Infrastructure and Key Resources." Information Sharing Environment. Accessed September 29, 2015. https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources.

[10] Berr, Jonathan. "Computer Security's Weak Link: Humans." CBSNews. April 6, 2015. Accessed September 29, 2015. http://www.cbsnews.com/news/the-human-element-and-computer-security/.

[11] "The Search Engine for the Internet of Things." Shodan. Accessed September 29, 2015. https://www.shodan.io/.

[12] "NIST Special Publication 800-53 (Rev. 4)." National Vulnerability Database. Accessed September 29, 2015. https://web.nvd.nist.gov/view/800-53/Rev4/home.