INL/CON-09-16096
PREPRINT

Cyber Security and Resilient Systems

Institute of Nuclear Materials Management 50th Annual Meeting

Robert S. Anderson

July 2009

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

CYBER SECURITY AND RESILIENT SYSTEMS

Robert S. Anderson
Idaho National Laboratory
1765 North Yellowstone Hwy, MS 3790, Idaho Falls, ID 83415

ABSTRACT

The Department of Energy (DOE) Idaho National Laboratory (INL) has become a center of excellence for critical infrastructure protection, particularly in the field of cyber security. It is one of only a few national laboratories that have enhanced the nation's cyber security posture by performing industrial control system (ICS) vendor assessments as well as user on-site assessments. Not only are vulnerabilities discovered, but described actions for enhancing security are suggested – both on a system-specific basis and from a general perspective of identifying common weaknesses and their corresponding corrective actions. These cyber security programs have performed over 40 assessments to date which have led to more robust, secure, and resilient monitoring and control systems for the US electrical grid, oil and gas, chemical, transportation, and many other sectors. In addition to cyber assessments themselves, the INL has been engaged in outreach to the ICS community through vendor forums, technical conferences, vendor user groups, and other special engagements as requested. Training programs have been created to help educate all levels of management and worker alike with an emphasis towards real everyday cyber hacking methods and techniques including typical exploits that are used. The asset owner or end user has many products available for its use created from these programs. One outstanding product is the US Department of Homeland Security (DHS) Cyber Security Procurement Language for Control Systems document that provides insight to the user when specifying a new monitoring and control system, particularly concerning security requirements. Employing some of the top cyber researchers in the nation, the INL can leverage this talent towards many applications other than critical infrastructure. Monitoring and control systems are used throughout the world to perform simple tasks such as cooking in a microwave to complex ones such as the monitoring and control of the next generation fighter jets or nuclear material safeguards systems in complex nuclear fuel cycle facilities. It is the intent of this paper to describe the cyber security programs that are currently in place, the experiences and successes achieved in industry including outreach and training, and suggestions about how other sectors and organizations can leverage this national expertise to help their monitoring and control systems become more secure.

INTRODUCTION

Not long ago, the systems and tools that helped us manage our lives, provide for our families, and create rewarding careers were primarily physical in nature. They utilized the ingenuity of machines to simplify the work of tens or even hundreds of people. These machines were isolated, powerful, and helped the world become an advanced society where no task was too difficult and no idea was too obscure. With the invention of the computer and the networks that tie them together, these isolated, powerful machines were united to form efficiencies never before seen. Productivity was exponentially expanded and the cost of doing business decreased. Electronic communications became the core technology for all transactions, whether helping to produce the service or product or the data necessary to conduct business.

NATURAL EVOLUTION

Today, computers are integral to every aspect of our lives, including cell phones, laptops, electronic billing, banking, social networking, entertainment, and the control and monitoring systems that provide constant and reliable energy for the nation's critical infrastructures and key resource sectors. Along with the sheer number of electronic processing transactions and shared communications taking place each day is a wealth of information that, if breached, could cause catastrophic consequences for business, infrastructure, and national defense. Inquisitive hackers seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions can be benign and motivated solely by curiosity, their actions typically violate the intended use of the systems they are exploiting. The results can range from mere mischief to malicious activity.

EXAMPLES

Cyber attacks have been taking place for many years. Most have originated within information technology organizations because of their connectivity to many local business systems as well as the internet. The trend over the last decade to network our once isolated industrial control and monitoring systems has placed our national assets, including critical infrastructure and nuclear safeguards activities, at a much higher risk. Examples of recent cyber attacks on these systems lends credibility to the realization that unless government and industry begin immediately to correct the software deficiencies created from decades of nonsecure development practices, the business risk to their enterprise will increase. The Wall Street Journal posted an article "Electricity Grid in U.S. Penetrated By Spies"[1] speculating that cyber spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. The article suggests that foreign countries are on a mission to navigate the U.S. electrical system and its controls. Other articles describe an e-mail message addressed to an executive containing a shopping list sent over by the Pentagon of weaponry another country wanted to buy. Lurking beneath the description of aircraft, engines, and radar equipment was an insidious piece of computer code known as "Poison Ivy" designed to suck sensitive data out of the $4 billion consulting firm's computer network. Had the executive clicked on the attachment, his every keystroke would have been reported back to a mysterious master server, which was registered through an obscure company headquartered outside the United States.[2] Such examples, which prove that cyber hacking penetrates control systems and corporate e-mail servers, are becoming more and more frequent.

INDUSTRIAL CONTROL AND MONITORING SYSTEMS[a]

Industrial control and monitoring systems are one subset of these computer systems that are subject to cyber exploitation. They operate within a complex environment. Organizations are increasingly sharing information between business systems and locally and geographically remote control systems. Security breaches can cause the loss of trade secrets and/or interrupt information flow resulting in the loss or destruction of services or products. Even more devastating consequences can be categorized as potential loss of life, damage to the environment, violations of regulatory statutes, and the compromises to operational safety. Threats to these systems can come in many forms, not only through outside terrorist or clandestine organizations, but through insiders with a great amount of knowledge about the systems. What makes control systems vulnerable to cyber security attacks?

a. The term "industrial control and monitoring systems," as used throughout this paper, includes Supervisory Control and Data Acquisition Systems (SCADA), Process Control Systems (PCS), Distributed Control Systems (DCS), and other control and monitoring systems.

To answer this question, a brief dialog of historical control and monitoring systems must be discussed.

The first industrial control systems were created with the objectives of availability, integrity, and confidentiality. These systems were designed to perform a function using these objectives with no thought to implementing secure standard software programming practices or policies. The motivation behind code development was primarily minimal cost and functionality. Since these systems were created with proprietary applications, unique communications protocols, obscure operating systems that were isolated, and had limited processing capabilities, the risk of a cyber breach was low. However, as the information technology business grew with the use of Ethernet and TCP/IP protocols, the original industrial control and monitoring devices were continually being replaced with less expensive commercial off the shelf (COTS) networking equipment. The asset owners took note, and made the business decision to replace aging proprietary equipment with industrial control and monitoring devices that could be connected with COTS equipment, thereby decreasing the plant's installation and operating costs. COTS equipment was now available for use with standard operating systems and communications protocols to bind control system equipment together with business applications for easy data retrieval. The business case for this transition included increased efficiencies, inventory control, marketing, forecasting, plant health—remote monitoring, increased analysis, lower production costs, quicker responsiveness, and a host of other engineering and business reasons. However, this networked environment provided a remote pathway for the attacker to exploit the poor coding practices, particularly in the industrial control and monitoring systems application software.

RISK

Risk has been defined as "…the threat or probability that an action or event, will adversely or beneficially affect an organization's ability to achieve its objectives."[3] Quantitatively, the risk equation can be defined as the combination of threat, vulnerability, and consequence.[4] So what is the risk of a cyber attack on an industrial control and monitoring system?

The risks to industrial control and monitoring systems are real, based on the information reported that vulnerabilities continue to be identified. Once these vulnerabilities have been disclosed, any number of attacks can be considered for exploitation. These exploits range from the simple denial of service attacks, to those where root access is obtained. When an adversary obtains control of an industrial control and monitoring system, data can be added, removed, or manipulated without being detected by the end user. When the industrial control and monitoring system does not indicate any signs of penetration or manipulation, the attacker can essentially perform any scenario possible within the operating limits of the system. These vulnerabilities exist primarily because of weak or nonexistent secure coding practices formed over many years. For most vendors, the cost of completely rewriting large installed software bases is prohibitive. However, these systems can and are being patched as vendor paradigms shift to mitigating the vulnerabilities that are discovered and reported.

Consequences are calculated based on the application and its physical, virtual, or economical effects on people and the surrounding structures. Damage can be quantified to include such individual things as lost business or transaction time during a period of downtime, lost productivity, or lost business opportunities. Other damage can be as catastrophic, such as losing the operating

capabilities for extended periods of time, which would include the loss of communications, banking, and impacting other critical infrastructure or key resource sectors. The worst case scenario would be the loss of life from an explosion at a hazardous processing plant or the use of a nuclear weapon created with nuclear material stolen from a rogue state.[4]

Threat is the frequency of potentially adverse events. This factor is difficult at best to determine because of the variables that it presents in any thorough analysis. The key to thinking about threat is to determine, or at least estimate, the rate of whatever threats face your organization, keeping in mind that many threat rates change constantly, particularly those driven by humans.

This discussion about risk leads to a directed question: Why be concerned about cyber security? The answer comes in many forms, but the following responses may best answer this question:

- Cyber intrusion and attacks continue to grow in both severity and frequency against information technologies systems
- COTS and the use of internet communications protocols are exposing control systems
- Hacker tools are increasing and available to anyone (open source)
- Clear text industrial control and monitoring system software remains dominant, allowing multiple pathways for exploitation
- The number of public disclosures of vendor equipment vulnerabilities is increasing.

MITIGATION

The world faces unique challenges to protect the lifestyles of their citizens from attack via a new battlefield that utilizes cyber terror to incite fear, uncertainty, and doubt, but also has the potential of catastrophic destruction. To meet these unique challenges, governments must identify the critical infrastructures and key resources that are susceptible to cyber attack and protect them in the most cost effective and efficient manner that maintains business continuity. Strengthening the cyber security posture of critical infrastructure and key resources will assist in the task of protecting both individuals and the world's environments.

Because of the laboratory's 60 year experience in nuclear, chemical, and industrial engineering, INL is uniquely qualified to provide relevant input to the mitigations and risk reduction efforts of industrial control and monitoring systems. As a result, INL's cyber security research team members have extensive knowledge of nuclear/industrial facility design and operation as well as insight into the numerous attack surfaces available to the adversary.

INL supports two primary U.S. industrial control cyber security programs: the DHS Control Systems Security Program (CSSP) and the DOE National SCADA Test Bed (NSTB). These two programs emphasize vendor assessments and mitigation, both in the laboratory and at user facilities, address outreach to increase awareness, and support standards bodies and organizations in accelerating standards that address the industrial control and monitoring systems environments.

INL PROGRAMS

INL has been recognized as a center of excellence for cyber security in critical infrastructure protection. Working in partnerships, INL provides mitigation information on discovered vulnerabilities that include specific actions for enhancing security on a system-specific

basis. These efforts also include addressing the general industry concerns of identifying common weaknesses and their corresponding corrective actions that can be used by all critical infrastructure and key resource sectors. These cyber security programs have funded over 40 assessments to date, which have provided robust, secure, and resilient industrial control and monitoring systems for many sectors, including energy, nuclear, chemical, and transportation. As a result of this work, INL has some of the top cyber and industrial control systems experts, allowing the laboratory to leverage this talent toward many applications.

DHS CONTROL SYSTEMS SECURITY PROGRAM (CSSP) AND THE DOE NATIONAL SCADA TEST BED (NSTB)

The DHS CSSP and the DOE NSTB were established in 2004 as a result of the United States indentifying the importance of control systems security in securing the nation's infrastructure. The CSSP program focuses on addressing the cyber security posture of all critical infrastructure and key resource sectors, while the NSTB focuses on the Energy Sector. When looking at the expansive infrastructure controlled by computer systems and their networks, protecting industrial control systems that operate critical infrastructure and key resource sectors from cyber attack is of great concern.

The primary mission of the CSSP and NSTB programs is to reduce the risk to critical infrastructure and key resource sectors by coordinating between government and industry to enhance the cyber security posture. This mission results in the mitigation of vulnerabilities while responding to the threats associated with the industrial control and monitoring systems that operate the nation's critical infrastructure and key resource sectors. These programs leverage the expertise at other DOE laboratories whose emphasis is on near term products usable by industry.

Both programs focus on assessments in the laboratory and in the field. The objectives of the assessments are multifaceted. Program goals include the following:

- Identify and mitigate cyber vulnerabilities in hardware and software at the component and system levels of industrial control systems
- Develop mitigation strategies and communicate this information to both industrial control system vendors and critical infrastructure and key resource sectors
- Work in partnership with system vendors to share enhanced security programs with end users, such that end users receive more secure systems and training about how to implement cyber security within their operating environments
- Provide cyber security risk mitigation tools that allow end users to perform self assessments and mitigate vulnerabilities
- Provide subject matter experts in support of standards organizations whose task is to address industrial control systems by developing security standards and best practices.

Assessments are performed in a collaborative and structured sequence that includes: selection and establishment of an industrial control system vendor impacting infrastructure and key resource sectors; legal contracts, including nondisclosure clauses; test plans; system installation and configuration; and system assessments and reports, both protected and releasable to the public. Once the programs issue the report to the industrial control system vendor, mitigation efforts that support patches and bug fixes can be incorporated into future modifications. As this assessment

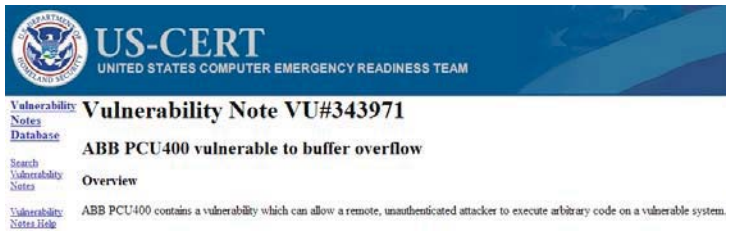
cycle continues and end users incorporate cyber security updates, facilities become more resilient to cyber attacks.

Onsite assessments are performed on a less frequent basis to determine if vulnerabilities and mitigations identified in the laboratory are relevant in actual installations. Another objective is to review policies and procedures. The advantages of performing onsite assessments include gaining additional insight into site-related vulnerabilities and providing mitigations that are facility specific. Assistance can be provided to the industry partner to improve security while encouraging the sharing of lessons learned among industry peers. Typical assessment teams include control system engineers, cyber researchers, and network specialists.

Outreach and awareness activities are an important element because many organizations are not cognizant of their cyber security risks and what mitigation measures are available. Industrial control system access once thought to be impossible has now been demonstrated numerous times using readily available open source tools. Outreach and awareness objectives are achieved when participants are educated and trained about what cyber security products and services are available. Training workshops have been provided at industry events and conferences to help improve understanding and support development of a business case for improving security policies and programs. These courses are developed on the basis of observations found during cyber vulnerability assessments. The CSSP and NSTB programs conduct two-, four-, and eight-hour courses tailored to educating the industrial control system and information technology stakeholder. An advanced course provides user–intensive, hands-on training for protecting and securing control systems from cyber attacks. In a one-week course, participants practice their skills and put their knowledge to the test through a Red Team/Blue Team exercise. Actual industrial control systems are used in the exercise and supported by a real-time scoring system that displays network activities of both teams. More than 3,800 critical infrastructure and key resource sector personnel have participated in these workshops and training activities sponsored by DHS and DOE.

Documents and tools are developed under both programs that help the end user understand the importance of cyber security, provide baseline security postures, provide recommended practices to improve security posture, support procurement language, create forensic plans and programs, and provide a host of other relevant cyber security information. Instrumentation, Systems, and Automation (ISA); the National Institute of Standards and Technology (NIST); and the International Electrotechnical Commission (IEC) are examples of standards organizations that are supported.

The DHS CSSP also provides an operational Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for the U.S. Computer Emergency Readiness Team (US-CERT). The US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry, and international partners. US-CERT interacts with federal agencies,


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Vulnerability Notes Database
Search Vulnerability Notes
Vulnerability Notes Help
Vulnerability Note VU#343971
ABB PCU400 vulnerable to buffer overflow
Overview
ABB PCU400 contains a vulnerability which can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.

industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. The ICS-CERT works to reduce the industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments and control system owners, operators, and vendors. The ICS-CERT coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.[5] A recent article in *Information Week* reported that federal agencies reported to US-CERT that they experienced 18,050 cyber security attacks in fiscal year 2008, three times the number from 2006.[6]

PROGRAM IMPACTS

The cyber security programs at INL have had a tangible impact on the nation's critical infrastructure and key resource sectors and continue to forge ahead as a national resource in industrial control systems cyber security. With the co-sharing of resources and expertise between the programs, a tremendous efficiency has been realized by the end user. Benefits of these efforts are shared amongst all parties, including DOE laboratories, industrial control system vendors, and end users who are providing critical resources and services. Through advances in technology, INL continues to expand its understanding and knowledge base of cyber security requirements and the impacts to critical infrastructure and key resources. Vendor partners use the assessment results to integrate security into their systems. Owners (end users) are responding with a higher level of cyber security awareness and education and implementing improvements into their systems, thus reducing the cyber risk to their facilities. Other benefits include the development of self-assessment tools by the CSSP and other educational documents. Both programs supported by INL continue to receive requests from industry stakeholder groups to participate in vulnerability assessments, provide training, and participate in standards organizations. The program's recognition and industry support continue to build within industrial control system vendor and user communities. As an example, end users are requiring third-party cyber assessments for their new systems and requesting that vendors adhere to the CSSP procurement language that is now written into purchase requirements documents. The DHS and DOE understand the importance of cyber security awareness and education, which is continually being enhanced as a direct result of the efforts by those individuals supporting these programs.

RESILIENCE

In order for industrial control systems to perform their intended purpose and be reliable during operations, systems must be designed to operate safely during equipment malfunction, human deficiencies, design errors, or from a malicious actor. Industrial control systems must provide a level of state awareness such that decisions can be made to implement coordinated actions resulting in clear recoveries that serve the customers of the end product or process. A resilient control system can be defined as one that maintains state awareness at an accepted level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature.[7] While resilience encompasses many aspects, cyber attacks present a complex set of conditions that cannot always be predicted. Human nature is defined by unpredictability of both objectives and motives. Even though control systems provide complex networks, they generally have a standard and ordered reproducible set of conditions that an adversary can count for higher probabilities that exploits will be successful. Added to this is the fact that typical industrial control systems rarely change architecture, creating a very consistent target. Challenges to the control system engineer for mitigating these threat vectors

include a high degree of defense-in-depth strategies. Defense in depth is the cornerstone concept to good cyber security practices.

Cyber forensics plays a key role in achieving the mitigations needed for the control systems domain, but the uniqueness and disparity of control system configurations make the performance of cyber forensics difficult and complex. The goal of cyber forensics is to support the elements of troubleshooting, monitoring, recovery, and protection of sensitive data. Moreover, in the event of a crime being committed, cyber forensics is also the approach for collecting, analyzing, and archiving data as evidence in a court of law. Programs therefore need to be in place with a guide to configuring control systems with forensics in mind, as well as guidelines on performing forensics in the event of a cyber attack. Given the nature of industrial control systems, where up-time is an important consideration (i.e., systems cannot be taken offline), real-time and off-line forensics are essential components in the control systems domain. Real time forensics can help to quickly differentiate between a cyber-incident and a system failure.[8]

INL AS A RESOURCE

INL has subject matter experts in cyber and control systems security who maintain the skills necessary to address the risk reduction requirements necessary for industrial control systems. This knowledge, expertise, and experience in cyber security control system assessments is shared with critical infrastructure and key resource stakeholders through industry outreach, training, and education events. To date, DHS and DOE are the primary sponsors, but INL has been asked by other organizations, including foreign governments, to help in both the assessment of their critical systems and the development of programs that are similar to those described in this paper. As a Federal Funded Research and Development Center (FFRDC), INL can provide services as long as basic requirements are met; primarily, that no other domestic or foreign entity can perform the same level of service or expertise, thereby competing with industry.

Based on the laboratory's rich history of supporting the DOE's mission in nuclear and energy research, science, and defense, INL has knowledgeable and experienced control systems engineers with the design and operational experience, cyber security researchers with the experience in finding vulnerabilities and developing exploits, onsite cyber assessments, and test facilities that include the Critical Infrastructure Test Range Complex test bed. The forensics area of CSSP, which can provide needed investigative activities in the case of a cyber event, is gaining additional attention in the control system arena. Any industrial control system that monitors or controls critical functions is a potential candidate for a third party cyber assessment. Cyber attacks can also be used to hide activities from observers. For example, ensuring that transmitted and received data packets have not been compromised is critical to safeguards and security missions.

OTHER APPLICATIONS

Cyber attacks permeate networks and systems that we rely on every day. It is the silent unseen malware that creeps through the networks looking for its next application to devour. The cyber and control systems security resources maintained by INL are available to help with organizations that need educated about cyber security or help in determining levels of defense. The Institute of Nuclear Materials Management supports the continued safekeeping of nuclear material on a global basis and the advancement of nuclear materials management in all its aspects. International safeguards employs unattended monitoring systems to provide continuous monitoring on declared

nuclear facilities around the world as part of its treaty-based mandate to ensure that nuclear material in these facilities is not being diverted from peaceful uses.[9] These systems were originally isolated and independent, relying on inspectors to visit nuclear facilities at a specified frequency, perform specific activities, and draw timely conclusions based on the data collected. Today, more and more of these systems are being connected to remote systems for many reasons, including cost savings, efficient utilization of data for analysis on a near real time basis, and data access by another system within the facility, inspector data review room, or an International Atomic Energy Agency field office such as Toronto, Tokyo, or Vienna. With reliance on these systems for stringent data loss intolerance, cyber security needs to be of utmost importance in addition to the existing fault tolerant designs for both hardware and software.

Governments establish programs that monitor and track cyber attacks need help understanding the breadth and depth of the resources required to handle the increasing frequency of attack attempts. As a FFRDC, INL has already assisted other foreign countries in creating government programs that monitor and analyze the numerous cyber attacks taking place every day. Resources are available at INL to help organizations develop, operate, and identify attacks that have the potential of disabling or disrupting critical infrastructure or missions that cannot afford any loss of or delay in activity.

CONCLUSIONS

Industrial control and monitoring systems are vulnerable to cyber attacks that can have potentially devastating consequences, and the threat continues to grow exponentially every day as cyber security attacks and sabotage continue to penetrate deeper into mission critical systems. Nuclear material must be controlled, accounted for, and protected against unwanted proliferation. Many of the industrial control and monitoring systems used to meet these objectives, were once simple, discrete, and isolated, but are now more sophisticated, perform multiple functions, and are integrated with each other, thereby providing attack surfaces that never existed in the past.

The onus to protect these assets from cyber security attacks is upon each and every organization that controls these critical processes. Doing so will allow them to operate in a safe and secure manner, thereby achieving mission success. DHS and DOE, in concert with the expertise at INL support these efforts by providing cyber security education, creating products that address the processes that must be in place to counter cyber threats, and providing self assessments to existing systems with mitigation strategies useful for immediate implementation.

REFERENCES

1. *Wall Street Journal*, "Electricity Grid in U.S. Penetrated By Spies," April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html.
2. *Businessweek*, "The New E-spionage Threat," April 10, 2008 http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm.
3. *Wikipedia*, "Risk," http://en.wikipedia.org/wiki/Risk.
4. *International Charter*, "The Risk Equation," http://www.icharter.org/articles/risk_equation.html.
5. Department of Homeland Security Control Systems Security Program, http://www.us-cert.gov/control_systems/.
6. *InformationWeek*, "Cybersecurity Balancing Act," April 27, 2009, http://www.informationweek.com/government.
7. Craig Rieger, David Gertman, Miles A. McQueen, *Resilient Control Systems: Next Generation Design Research*, IEEE HSI 2009, May 21-23, 2009.
8. Recommended Practice: Creating Cyber Forensics Plans for Control Systems http://csrp.inl.gov/Recommended_Practices.html#nogo.
9. Schanfein, Mark, *International Atomic Energy Agency Unattended Monitoring Systems: A Brief Overview*, LA-UR-06-4162, Los Alamos National Laboratory.