INL/CON-12-24615
PREPRINT

Cyber Security Testing and Training Programs for Industrial Control Systems

PBNC 2012

Daniel Noyes

March 2012

PBNC 2012-FA-0081

CYBER SECURITY TESTING AND TRAINING PROGRAMS FOR INDUSTRIAL CONTROL SYSTEMS

Daniel Noyes

Idaho National Laboratory, Idaho Falls, Idaho, United States

daniel.noyes@inl.gov

Abstract

Service providers rely on industrial control systems (ICS) to manage the flow of water at dams, open breakers on power grids, control ventilation and cooling in nuclear power plants, and more. In today's interconnected environment, this can present a serious cyber security challenge. To combat this growing challenge, government, private industry, and academia are working together to reduce cyber risks. The Idaho National Laboratory (INL) is a key contributor to the Department of Energy National SCADA Test Bed (NSTB) and the Department of Homeland Security (DHS) Control Systems Security Program (CSSP), both of which focus on improving the overall security posture of ICS in the national critical infrastructure.

In support of the NSTB, INL hosts a dedicated SCADA testing facility which consists of multiple control systems supplied by leading national and international manufacturers. Within the test bed, INL researchers systematically examine control system components and work to identify vulnerabilities.

In support of the CSSP, INL develops and conducts training courses which are designed to increase awareness and defensive capabilities for IT/Control System professionals. These trainings vary from web-based cyber security trainings for control systems engineers to more advanced hands-on training that culminates with a Red Team / Blue Team exercise that is conducted within an actual control systems environment.

INL also provides staffing and operational support to the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Security Operations Center which responds to and analyzes control systems cyber incidents across the 18 US critical infrastructure sectors.

1. Introduction

The cyber security landscape for critical infrastructure is changing rapidly. Critical infrastructure installations rely on industrial control systems (ICSs) to be safe from cyber events so that they can operate as they are designed. However, with technological advances and upgrades in ICSs and greater connectivity to the Internet, the cyber threat to critical infrastructure has never been greater.

> The ability to identify and directly access controllers and industrial software applications can be as simple as knowing how to search for control systems, then clicking on hyperlinks. Researchers often use

freely available search engines, such as SHODAN (basic SHODAN is still free, enhanced tools version requires subscription service fees), Every Routable IP Project (ERIPP), and Google, to locate SCADA and ICS assets (ICS-CERT, 2011).

Regulations exist to protect against the cyber threats that exist, especially for the nuclear power industry. For example, the US Government's 10 CFR 73.54(a)(2) "requires the licensee to protect such systems and networks from those cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, services, or data; and impact the operation of systems, networks, and equipment."

A regulation however, does not guarantee security. In 2003, the Davis-Besse nuclear power station near Oak Harbor, Ohio was infected with the Slammer worm which resulted in a temporary loss of safety monitoring. In 2008, the Hatch Nuclear power plant near Baxley, Georgia went into automatic shutdown due to a software upgrade on a business system. These events, along with the 2010 discovery of the Stuxnet malware are all examples of how even the nuclear industry cannot guarantee protection from cyber-related events (Kesler, 2011).

Even if nuclear plants are using analog technology, and their control network is completely air gapped from the business network, it doesn't mean it will stay that way. The operational environment is changing. Operational equipment is moving to digital and wireless technologies. The benefits are great, but risks are ever prevalent.

An attacker only needs one success out of a thousand to succeed. On the other hand, defense must have one hundred percent success rate to protect against all threats. This is an impossible situation. The threat landscape is too vast and widespread to guarantee success. However, it is critical for a nation to do everything possible to protect against the existing and emerging threats to its critical infrastructure. This requires a holistic approach to security and involves all stakeholders whether they are in the public or private sector.

In this paper, an overview of the programs is discussed in which INL is dedicated to improving the cyber security posture of the US critical infrastructure. These programs include the DOE National SCADA Test Bed (NSTB), Department of Homeland Security (DHS) Control Systems Security Program (CSSP) ICS Cyber Security Training Program, and DHS CSSP ICS-CERT.

2. National SCADA Test Bed

Since 2003, the NSTB has completed many vulnerability assessments on major energy control systems and recommended security enhancements to the vendors. The vendors have adopted many recommendations, developed next-generation systems, and worked with end-users to implement upgrades in legacy systems.

The need for such an evaluation program becomes even more apparent as time passes. ICS equipment, such as Programmable Logic Controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, and more, is continually being modernized and adapted to match up with 21st century technological capabilities. This includes transforming analog to digital, including wireless capabilities and giving individual devices the ability to connect to the Internet via various technologies. Many of today's RTUs and other equipment are being developed with embedded web servers to aid in widespread Internet connectivity. While technology modernization allows for greater convenience and lower costs, it also creates potential security risks. Whereas many legacy ICS networks were once not connected to the Internet, this is not the case today.

All an attacker needs to compromise a system is one access point. Even though a SCADA system may not have a direct connection to the Internet, indirect connections may exist, which an attacker could target. Perhaps the SCADAs are connected to the corporate network for business functions; connected to peers (i.e., ICCP connections); or connected to remote sites, vendors, system administrators, operators, or field equipment (INL, 2011). It is critical to consider all possible access paths, not just the obvious routes.

Through the work of the NSTB, control systems in use today have many vulnerabilities that could be exploited if they are not addressed. The most recent report, released in September of 2011, lists the most common vulnerabilities discovered from 2003 to 2010 by INL and provides recommendations to SCADA vendors and owners to identify and reduce the risk of these vulnerabilities in their systems.

Table 1. Ten common vulnerabilities identified in NSTB assessments (INL, 2011)

Common Vulnerability	Reason for Concern
Unpatched published known vulnerabilities	Most likely attack vector
Web Human-Machine Interface (HMI) vulnerabilities	Supervisory control access
Use of vulnerable remote display protocols	Supervisory control access
Improper access control (authorization)	SCADA functionality access
Improper authentication	SCADA applications access
Buffer overflows in SCADA services	SCADA host access
SCADA data and command message manipulation and injection	Supervisory control access
SQL injection	Data historian access
Use of standard IT protocols with clear-text authentication	SCADA host access
Unprotected transport of application credentials	SCADA credentials gathering

The vulnerabilities listed in the table above were routinely discovered in NSTB assessments using a variety of typical discovery and exploitation methods to manipulate or disrupt system operations. For more information regarding these vulnerabilities and the recommendations on how to reduce the risk of these vulnerabilities, see the full report (INL, 2011).

2.1 Vendor Support

The need for the NSTB is easily demonstrated by the products and services it provides. However, establishing the environment for such a successful program requires time, expertise, and trust. Since the equipment being tested is developed by private companies and operated largely by private companies, legal agreements for cooperative work have to be established by the stakeholders involved. Before the program was well known, equipment vendors were unsure about granting permission to “hack” into their systems for the purpose of finding as many vulnerabilities as possible while paying for a portion of the cost involved. However, these companies began to see how having their equipment evaluated in an ethical way would benefit them in the long run, and they began to actively and willingly participate in the program.

2.2 Assessment Prioritization

The personnel involved in the assessment process had to determine which systems to evaluate first and develop rigorous methodology by which they would assess these systems. Through risk and consequence analysis, it was determined that the focus for assessment would be on SCADA equipment used for electricity transmission in the power grid. Because four primary vendors made up the vast majority of the market share of SCADA equipment used for electricity transmission, that was the equipment that took priority for assessment.

2.3 Assessment Team Composition

Because SCADA software and equipment differ from traditional IT software and hardware, unique skill sets are required to perform an assessment. The team composition for each assessment is usually composed of four or five personnel and includes a control systems engineer, a lead cyber security researcher, and two or three junior cyber security researchers. Among other duties, the control systems engineer acts as the lead for the assessment. The control systems engineer is responsible for configuring the equipment to match operational configuration to the extent possible, working with the lead cyber security researcher to perform a risk and consequence analysis to develop targets for the assessment, and overseeing the assessment process and development of the final report. The lead cyber security researcher is responsible for the technical assessment work performed and directs and assists the junior cyber security researchers in conducting the assessment and providing input for the final report. On average, each assessment generally takes 3 months from beginning to end to complete, and approximately 1000 hours of technical assessment are performed on each assessment.

For more information on the NSTB assessment methodology, see Appendix A of the latest report (INL, 2011).

2.4 SOPHIA

Researchers at INL have also worked through the NSTB to develop a passive, real time tool for interdevice communication discovery and monitoring of the active elements in a SCADA system. With a Greek translation meaning “wisdom,” this tool is aptly named Sophia.

Sophia has several features designed to increase the ability of ICS network administrators to detect and respond to possible cyber security events. Sophia is a “hacker-based” tool designed to identify what’s on the network, thus increasing defensive capability. Sophia can passively identify hosts, ports and services, server/client relationships, and networks.

Because ICS networks are generally static, have limited applications, and few specialized users, they differ greatly from the traditional IT network that generally has opposite attributes in those respects. However, with this ICS network focus, Sophia makes it possible to create effective white lists based on the network attributes it is able to characterize and map out. These white lists serve as the basis for detecting unauthorized communications and alerting network administrators. Because Sophia is entirely passive, it will not cause ICS networks to crash when in use.

Along with the white listing capability, Sophia also has the following uses.

- Configuration Management
  - Alarm may indicate the addition of a new component
- Fielding new systems
  - Identify differences between factory acceptance test (FAT) and site acceptance test (SAT) installation
- Firewall rule validation/development
  - Only allow what is needed for ICS operations
- Switch and router configuration
  - Easily create access control lists
- Component hardening
  - Unnecessary ports identified should be disabled or blocked
- Patch testing
  - Quickly identifies communication changes

A proof-of-concept report (INL, 2010) for Sophia has been published by the INL and can be found online. The program is currently soliciting applications for Beta testers from US Energy Companies and is planning for a commercialization release in October 2012.

3. CSSP Training Program

In order to increase the cyber security posture of critical infrastructure, it is imperative that owners, operators, and other stakeholders have increased awareness, training, and education with regards to ICS cyber security.

INL has worked with both the US DOE and DHS in addressing critical infrastructure awareness, training, and education. Currently, the training INL conducts is on behalf of the DHS CSSP.

> The goal of the DHS National Cyber Security Division's CSSP is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments, as well as industrial control systems owners, operators and vendors. The CSSP 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 (US-CERT, 2012).

As part of this goal, DHS contracts with INL to host courses to train stakeholders in ICSs cyber security. INL has developed three series of classes that begin at an introductory level and conclude with an advanced hands-on training course designed to teach advanced technical level skills in ICS cyber security.

The primary focus of the introductory course is on theory rather than practice and is typically covered in one 8-hour session. This course provides for easy customization for sector-specific training as well as the creation of derivative 2 or 4-hour classes. It is typically conducted at industry and government venues.

The lecture-only intermediate course takes the students from a basic understanding presented in the introductory class and builds on the theory with practical tools. Trainers provide specific instruction on offensive and defensive themes, using actual examples and exercises to illustrate how cyber security theory can be used in real world scenarios. This course is typically conducted in one 8-hour session at industry and government venues.

The hands-on intermediate course revisits some of the more common themes from the lecture-only course, but also provides a forum for the students to experiment with and use cyber security technologies within a control system domain. This course requires students to bring their own laptops as the materials will be delivered via hands-on exercises and is typically covered in one 8-hour session at industry and government venues for a maximum of approximately 40 attendees.

The advanced course is the capstone course that includes 5 days of intensive cyber security for control systems training, cyber security presentations, and a 12-hour Red Team / Blue Team exercise. Although it is recommended that students progress through the beginning and intermediate courses before attending the advanced course, it is not required.

Because having the prerequisite courses is not required, the first portion of the advanced course covers course material presented in the beginning and intermediate courses, albeit in a more condensed fashion. Throughout the remainder of the course, students get hands-on training in network discovery, network exploitation, and network defense techniques and practices. This culminates in a 12-hour Red Team / Blue Team exercise where students put their new skills to the test in a hands-on exercise.

During the exercise, the Red Team will be attacking a mock chemical company’s network in an attempt to steal data and take control of their batch processing equipment. At the same time, the Blue Team must defend their networks and maintain operations of their equipment to produce the chemicals they are committed to deliver to customers. The entire experience is extremely effective at bringing the cyber security challenges to light and engaging stakeholders in an effective and meaningful way.

Because of the equipment and classroom limitations, the advanced training is restricted to approximately 40 attendees and is conducted on a monthly basis. Each advanced training course requires personnel with expertise in control systems engineering, network discovery, network exploitation, and network defense to oversee and conduct the training. As of February 2012, more than 1,200 attendees have completed the advanced course.

These attendees represent 35 separate countries outside of the U.S. and over 660 owner/operator, utility, vendor, government, and industry agencies.

It is the intent of the DHS CSSP to make the training courses available to other organizations through Training Support Packages (TSP), which have been developed for each course. These TSPs will consist of the following components:

- Instructional Plan
  - Enabling Learning Objectives (ELO)
  - Terminal Learning Objectives (TLO)
- Student Manual
- Instructor Guide/Lesson Plan
- Course Material
  - Slides
- Hardware/Software Guide.

4. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Although the NSTB and ICS Cyber Security Training Programs enhance the cyber security posture of critical infrastructure, threats and compromises still exist. A response capability is required to address these existing threats and compromises. INL plays a major part in the development and execution of the response capability of the CSSP known as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Since the opening ceremony for the ICS-CERT was held at the INL in November 2009, INL has provided the professional and technical support needed to operate the ICS-CERT Control Systems Operations Center at INL.

The capabilities provided by the ICS-CERT include the following:

- Respond to and analyze control systems related incidents
- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The need for the ICS-CERT is easily demonstrated by the metrics shown in Table 2.

Table 2. ICS-CERT metrics (ICS-CERT, 2011)

ICS-CERT Metrics	FY-10	FY-11
ICS Incidents	40	130
ICS Related Vulnerabilities	17	145
Incident Response Fly Away	5	7

> Vulnerability analysis and coordination activities were up over 700% over FY-10, with researchers using ICS-CERT as a conduit to vendors in the ICS space. Many of these issues resulted in advisories and alerts posted to the US- CERT secure portal and the public CSSP website. ICS-CERT published over 150 information products, warning the ICS community of various vulnerabilities and threats impacting control systems (ICS-CERT, 2011).

With increased focus on cyber security for ICSs, a national response capability is critical. The ICS-CERT relies on cooperation from the public sector stakeholders, private sector companies, and law enforcement when necessary for successful resolution of cyber-related events. This cooperation is only maintained by trust, transparency, and a collective dedication to increase the cyber security posture of the national critical infrastructure.

5. Conclusion

The cyber security challenges facing critical infrastructure, including nuclear power generation and transmission, are vast and widespread. It is critical to be aware of and respond to threats and incidents whenever they exist.

In support of DOE and DHS programs, INL plays a major role in increasing the overall cyber security posture of the US critical infrastructure. It is critical to address the various challenges of ICS cyber security in multiple ways. This includes becoming aware of the existing cyber security threats, testing and improving ICS equipment and installations, training and educating stakeholders, and responding to incidents and threats where they are detected.

Developing and operating these programs requires collaborative effort from both public and private entities. Having the appropriate mission, resources, and people with the necessary expertise to carry out the functions of these programs is essential to success.

Acknowledgments

This work was supported by the INL Control Systems Department ICS Mission Support Center.

References

ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct2011.pdf, date last accessed, February 27, 2012.

INL, http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems%202011.pdf, date last accessed, February 27, 2012.

Kesler, Brent, http://www.nps.edu/Academics/Centers/CCC/Research-Publications/StrategicInsights/2011/Apr/SI-v10-i1_Kesler.pdf, date last accessed, February 27, 2012.

US-CERT, http://www.us-cert.gov/control_systems/index.html, date last accessed, February 27, 2012.