Educational Modules in Industrial Control Systems for Critical Infrastructure Cyber-security

Abstract

The cyber-security of critical infrastructure has gained much attention in recent years due to the effectiveness of such attacks to cause physical harm. Cyber attacks on critical infrastructure, specifically the Industrial Control Systems (ICS) by which critical processes are controlled, affect water, power, critical manufacturing and many other areas vital to society. Therefore, the education of new engineers to mitigate these attacks is also critical. One key problem that has existed for some time is the separation of cyber-security education, in the Computer Information Science (CIS) discipline, from that of ICS education, in the electrical and other engineering disciplines as ICS engineers. This separation results in misunderstanding between CIS and ICS professionals who typically remain divided within the corporate enterprise, which impedes the implementation of cyber-security solutions in critical infrastructure. To address this problem, new educational modules are developed to educate students from both CIS and ICS disciplines in the unique aspects of ICS cyber-security. The modules are designed to be accessible to students of either discipline, which allows this important subject to be included into either curriculum quickly and without the need for developing a new course. The modules explore the unique network protocols and security measures implemented in ICS from the perspective of maintaining reliable process control, including known vulnerabilities and attacks. The modules also explore methodologies for intrusion detection, forensics, and attack mitigation as uniquely applied to ICS. CIS students gain insight into the nature of process control and understanding in how cyber-security policy affects process control. ICS students gain insight of cyber-security concepts, and the importance of these concepts in the corporate enterprise. Finally, a lab scale ICS platform is developed to serve as a cyber-security trainer for students from both disciplines, including sample lab experiments that encourage interdisciplinary cooperation towards achieving the common goal of critical infrastructure cyber-security. In order to assess the impact of these modules on CIS and ICS students, a survey is developed to measure the understanding of the unique aspects of ICS cyber-security both before and after module presentation and lab participation.

1. Introduction

Cyber-security continues to move to the forefront of existing and new technology deployments, as well as the media in general. Recent attacks[1,2] by terrorist groups on critical infrastructure are beginning to exploit the risks and vulnerabilities of Industrial Control Systems (ICS)[3,4]. A Presidential Executive Order has brought priority to the issue[5] and Presidential Directive 7[6] defines such critical infrastructure sectors, the vast majority of which are controlled by ICS. Therefore, there remains a critical need to educate students in the concepts of cyber-security with respect to such systems, and to be inclusive of students not only in disciplines specializing in cyber-security, such as Computer Information Science (CIS), but for students in engineering who utilize ICS as a tool to control a physical process, e.g. critical infrastructure.

2. Integration into existing programs

Cyber-security concepts are at least generally addressed in CIS and related disciplines such as Information Technology (IT) and Computer Science (CS), if not specifically addressed in cyber-security concentrations within these. What is missing from these is an understanding of real-time control systems as they are deployed in industry, and their associated industrial processes, as these tend to be addressed in the electrical, mechanical, and chemical engineering programs. Subsequently, concepts of cyber-security rarely are included in electrical, mechanical, and chemical engineering programs unless there is a specific need or desire by the student to pursue. While this has improved in recent years, there is still much lacking in common ground[7,8]. This has resulted in the existing, siloed attitude taken in industry in the past as CIS is responsible for security and engineering is responsible for industrial process reliability. When these two responsibilities conflict, the solutions are often delayed or less than optimal, specifically due to a lack of common understanding between these groups on cyber-security.

3. Previous educational work

The University of South Australia was among the first to implement a SCADA systems security course within a systems engineering program[8]. The goals of this paper were to illustrate the role of SCADA in Australia's critical infrastructure and demonstrate the need for SCADA systems security in their curriculum. In their approach, the technical details of SCADA systems, the concepts of cyber-security, and the implications for critical infrastructure installations and society are all studied in concert.

For some time, the Idaho National Laboratory and Sandia National Laboratory have collaborated on the National SCADA Testbed Program[9] to provide workshop-style training in ICS cyber-security for students and professionals. While this program continues to be of high value, it is difficult for some students to attend, thus the need for such concepts to be included at engineering and CIS institutions.

Some texts and supplements have also started to become available for reference to students and educators[10,11]. These texts could be included in textbooks for the respective course and shared among both engineering and CIS students alike.

Additionally, previous work[7] supported by the Department of Homeland Security National Institute for Hometown Security has included the development of a curriculum model, which introduced two educational tracks to accommodate the missing components, or gaps, for each student group, i.e., a track for CIS students to cover engineering gaps, and a track for engineering students to cover CIS gaps.

4. Course modules

The course modules are designed for easy integration into existing courses for students in various programs. For example, a course in information assurance could include the topics for CIS students to acquaint these students with aspects of ICS. Likewise, a course in industrial control could include the topics for engineering students to acquaint these students with principles of cyber-security. These courses would be recommended at the senior or graduate level in order to best accommodate alternative thinking and application. The modules advance the mutual understanding of ICS cyber-security concepts so that when encountered in industrial settings,

both corporate CIS and engineering professionals will have a common vocabulary by which to meet security challenges. Outlines of the modules with respect to student groups are as follows.

A. Topics for CIS students:
    1. ICS hardware
        a. Programmable Logic Controller (PLC) processor architecture
        b. PLC real-time operating systems
        c. Sensory input and actuator output buffers and interfaces
    2. ICS software
        a. Human Machine Interfaces, GUI
        b. PLC programming languages, overview
            i. 981 ladder logic
            ii. IEC 61131-3
    3. ICS networks
        a. Ethernet considerations in real-time networks
        b. Modbus/TCP and serial links
            i. RS-232 and RS-485
        c. Proprietary protocols
            i. Allen Bradley Data Highway
            ii. Emerson WDPF
            iii. Siemens Simatic Net
        d. Other serial links, utilization of telephone modems
        e. Existing commercial solutions in ICS intrusion detection and firewall routers
    4. The industrial environment
        a. Reliability of industrial processes, costs of downtime
        b. Hardware, software selection criteria
        c. Role-based access and use cases in industrial settings
        d. Software patch management, why patches cannot always be installed
        e. Industry specific policies for security
            i. North American Electric Reliability Corporation Critical Infrastructure Protection standards[12]
        f. ICS-specific malware
            i. Stuxnet model
        g. Engineering goals and responsibilities

B. Topics for engineering students:
    1. Principles of core concepts of cyber-security
        a. Encryption basics
        b. Authentication methods
        c. Security-aware network protocols
            i. Ethernet TCP/IP
            ii. DNP3, OPC
        d. Types of attacks
            i. DoS, spoofing, privilege escalation
        e. Intrusion detection and prevention
        f. Malware

        i. Stuxnet model
    g. Network traffic analysis
    h. Forensic analysis and recovery
2. Commercial solutions for network security
    a. Ethernet switch management
    b. Principles of firewall routers
    c. Configuration of operating systems
    d. Password management policy
    e. Software tools
        i. Wireshark, Snort
3. Security principles in corporate environments
    a. Corporate policies in cyber-security
        i. Password management policy
        ii. Software patches, updates
        iii. Hardware, software selection criteria
    b. Liability in corporate networks
        i. Auditing of network transactions
        ii. Assessing risks and vulnerabilities
        iii. Legal aspects of cyber attacks
    c. Threat actors, methods and motivations
    d. CIS goals and responsibilities

Sample learning modules are scheduled for dissemination via WWW through Intel Corporation's University Program Office on or after May 2015 for public use.

5. ICS hardware lab system

In order to test some theoretical principles and provide practical experience, a physical laboratory facility is valuable. These include ICS components such as PLCs, Input/Output devices (I/O), and network hardware as well as computing platforms and software used in industrial settings. While most engineering schools will have some facility that includes these, it is beneficial for a dedicated system to be used such the cyber-attacks and mitigating approaches can be freely exercised without concern to shared experiments for other courses.

Figures 1 and 2 illustrate an ICS platform for cyber-security training. The system consists of two Allen Bradley PLCs for simulation and control, associated I/O, networking hardware, and Windows®-based Virtual Machines (VM) to serve as Human Machine Interfaces (HMI) for operator and engineering (ENG) functions in ICS. Additionally, an ICS-specific Tofino® Xenon firewall has been incorporated to enable experiments with commercial ICS cyber-security solutions, which provides detailed traffic analysis and signatures specific to ICS protocols, such as the Allen Bradley EtherNet/IP® used here.

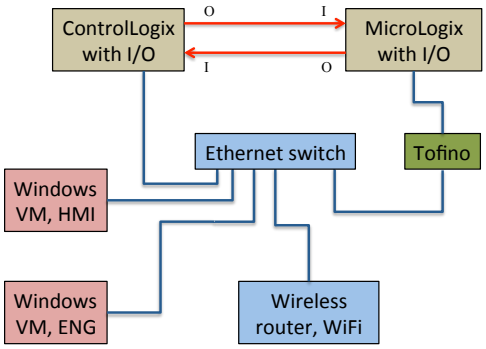

Figure 1 – ICS cyber-security trainer block diagram.

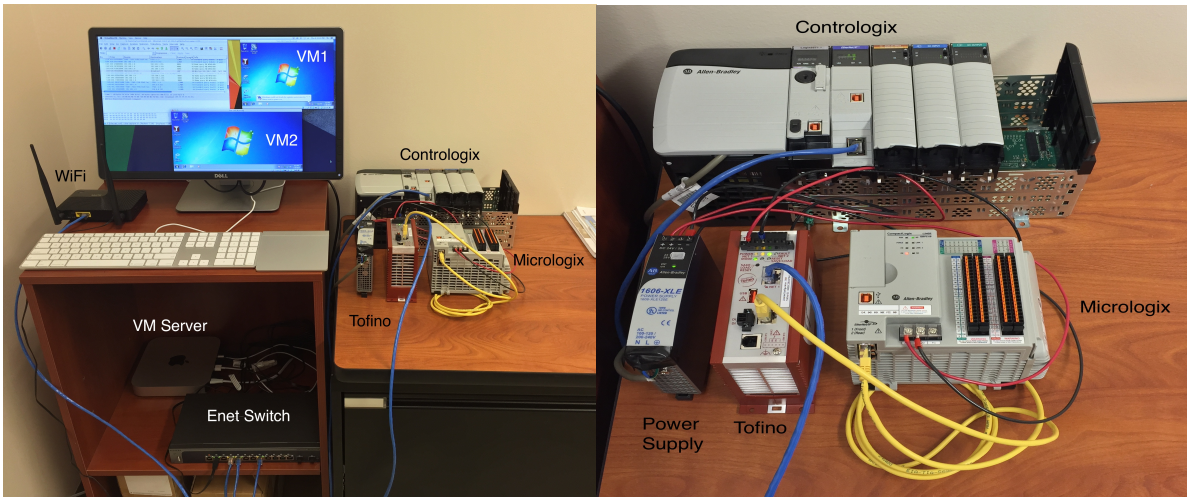

Figure 2 – ICS cyber-security trainer photographs, w/o I/O wiring.

The ControlLogix® PLC simulates an industrial process, e.g., water treatment or power generation, which is controlled by the MicroLogix® PLC by direct wiring, in red, through digital and analog I/O. The use of two different PLCs allows vulnerabilities unique to certain devices to be explored. Alternatively, the use of two different PLC vendors may be recommended. The ControlLogix PLC is placed on the EtherNet/IP network, in blue, with the Windows VMs, which provide operator and engineering functions as typical in the industrial environment. The MicroLogix PLC represents the PLC in direct control of the industrial process, so this is placed behind the Tofino firewall on the network. Finally, a wireless router is included to allow direct remote access by students to attempt to hack into the network, e.g., red team, and perform maintenance and attack response, e.g., blue team. This provides an isolated network to avoid the issues associated with incorporating the system into the university WAN for cyber-attack purposes.

6. Laboratory exercises

Potential laboratory exercises would do best to include student teams that consist of a mix of both CIS and engineering students in order to foster collaboration between these historically siloed groups. A cooperative approach would start with exercises that are familiar to one student

group, allowing the other student group to learn from fellow team members. Once these exercises had been accomplished, exercises that would be more challenging to both student groups simultaneously would serve to engage the team members together. An example outline of this approach is as follows.

A. Preliminary exercises

1. Assembly of the lab training system similar to Fig. 1, allowing each student group to work on their respective area of comfort.
2. Ethernet, WiFi, and VM configuration, allowing CIS students to demonstrate best practices to engineering students.
3. PLC configuration and ICS software configuration of VMs, allowing engineering students to demonstrate best practices to CIS students.

B. Advanced exercises

1. ICS network traffic analysis, allowing engineering students to become familiar with network traffic tools and CIS students to become familiar with normal ICS network traffic.
2. Configuration of the Tofino firewall router to monitor and protect ICS protocol traffic from anomalies utilizing skills learned in the previous traffic analysis exercises.
3. Sample network attacks to gain access, deny service, etc., exercising known vulnerabilities of the hardware and software in the lab trainer. Perhaps some unknown vulnerabilities may be uncovered.
    a. The ICS Cyber Emergency Response Team (ICS-CERT) provides an excellent clearinghouse of existing and newly discovered ICS vulnerabilities at their web site, https://ics-cert.us-cert.gov/. The procedure would be to choose a particular vulnerability and discuss how an attack could be launched on the trainer. How would this vulnerability be mitigated?

C. Final exercise

1. Red team, blue team competition where each team continues to consist of a mix of CIS and engineering students. In contrast to capture-the-flag competitions, this attack should focus on disruption of the industrial process simulated and controlled in the PLCs, requiring both network hacking skills and industrial process knowledge to succeed.

7. Evaluative survey

An evaluative survey is developed to gauge the preconceived notions of students in the subject matter of ICS and critical infrastructure cyber-security. The survey employs a Likert scale metric applied as appropriate to questions that span the subject matter. It is expected that the survey be administered both before and after module presentation to gauge the changes in perceptions of the students. Sample questions that are included in the survey are as follows.

1. When operating a critical infrastructure process, which of network security or process reliability is more important? Network security(1), (2), equal(3), (4), process reliability(5).
2. Are cyber-attacks on critical infrastructure on the rise? Decreasing(1), (2), steady(3), increasing with other cyber-attacks(4), outpacing other cyber-attacks(5).

3. How vulnerable do you think our critical infrastructure is? Not vulnerable(1), (2), no more vulnerable than other systems(3), (4), highly vulnerable(5).
4. How effectively do you think IT cyber-security approaches protect ICS networks? Not effectively(1), (2), somewhat effectively(3), (4), completely effectively(5).
5. How isolated are ICS from Internet-based attacks? Not isolated(1), (2), somewhat isolated(3), (4), completely isolated(5).
6. How effectively can ICS networks be attacked if ICS networks are air-gapped from any other network? Not effectively(1), (2), somewhat effectively(3), (4), completely effectively(5).
7. Is the automatic application of operating system security patches for computers used in ICS a good solution or a major problem for ICS reliability? Good solution(1), (2), (3), (4), major problem(5).
8. What is your level of understanding of cyber-security principles, such as encryption, authentication, intrusion detection, attack mitigation, etc.? Almost none(1), (2), some exposure(3), (4), expert understanding(5).
9. What is your level of understanding of ICS hardware/software, critical infrastructure, and the control of physical processes? Almost none(1), (2), some exposure(3), (4), expert understanding(5).
10. How likely are you to pursue a career that involves critical infrastructure cyber-security? Not likely(1), (2), unsure(3), (4), very likely(5).

8. Final discussion

The outline for course modules and laboratory experiments has been presented, including the diagram for a hardware trainer. The key problems to be addressed are the gaps in CIS education of ICS-specific cyber-security, the gaps in engineering education of cyber-security principles, and the siloed approach still prevalent in post-secondary education that discourages, or at least does not sufficiently encourage, the blending of these two student groups such that they learn to work cooperatively on the greater issue of cyber-security of critical infrastructure, in which ICS are the key controlling component. The importance of solving these problems becomes obvious, as society is by definition critically reliant on its critical infrastructure. This critical infrastructure includes power generation and distribution, water treatment and delivery, telecommunications, and several others[6] of which society requires to function. Interdependencies among these infrastructure result in critical codependences[13], e.g., the loss of power delivery results in a loss of water due to lack of electricity to run the water treatment process.

The approach to solving these problems is through education of both CIS and engineering students and professionals to reach a common understanding to facilitate cooperative solutions. Effective solutions require compliance among many regulations, e.g., security guidelines, industrial safety, economics, etc., and across multiple goals, e.g., network security, industrial process liability, etc. The scope of these is too large for a siloed approach to teaching and implementation to accomplish and only results in conflict. By developing the modules such that these two student groups work together towards the common goal of critical infrastructure security, with each student bringing their own perspectives to the approach, the siloed approach is broken and effective cooperation is the result.

The effectiveness of this approach is best measured directly, through an evaluative test based on the subject matter of critical infrastructure cyber-security both before and after presentation of the modules to gauge retention and understanding. Beyond this, a beforehand survey is very informative as preconceived notions of critical infrastructure cyber-security can be detected in both groups of students, as well as an afterward survey to gauge how these notions have changed.

Acknowledgement

This work was fully supported by a gift from the Intel Corporation through their University Program Office.

References

1. David Goldman, "Hacker hits on U.S. power and nuclear targets spiked in 2012," *CNN Money*, WWW, found at http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html, retrieved Jan 2015, Jan 2013.
2. David E. Sanger and Eric Schmitt, "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure," *The New York Times New York Edition*, pp. A8, July 27, 2012.
3. Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y. and Sastry, S., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," *ACM Symposium on Information Computer and Communications Security*, pp. 355-366, 2011.
4. E. Luiijf, "Understanding Cyber Threats and Vulnerabilities," J. Lopez et al. (Eds.): *Critical Information Infrastructure Protection*, LNCS 7130, Springer-Verlag Berlin Heidelberg, pp. 52-67, 2012.
5. The White House, "Improving Critical Infrastructure Cybersecurity," Executive Order, WWW, found at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, retrieved Jan 2015, 2013.
6. Department of Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," WWW, found at http://www.dhs.gov/homeland-security-presidential-directive-7, retrieved on Jan 2015, Dec 2003.
7. C. Foreman, J. Hieb, J. Graham, and R. Ragade, "A Curriculum Model for Industrial Control Systems Cyber-Security with Sample Modules," *IS-CA 27th International Conference On Computers and Their Applications*, Las Vegas, Nevada, pp. 179-183, Mar 2012.
8. Jill Slay and Elena Sitnikova, "Developing SCADA Systems Security Course within a Systems Engineering Program," *Proceedings of the 12th Colloquium for Information Systems Security Education*, pp. 101-108, University of Texas, Dallas, TX, June 2-4, 2008.
9. National SCADA Testbed (NSTC) Fact Sheet, WWW, found at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf, retrieved Jan 2015, 2009.
10. Elena Sitnikova, Ernest Foo, and Rayford B. Vaughn, "The Power of Hands-On Exercises in SCADA Cyber Security Education," *Information Assurance and Security Education and Training*, *IFIP Advances in Information and Communication Technology*, vol. 406, Springer, pp. 83-94, 2013.
11. Robert Radvanovsky and Jacob Brodsky, *Handbook of SCADA/Control Systems Security*, CRC Press, pp. 383, 2013.
12. North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) Standards, WWW, found at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, retrieved Oct 2014.

13. Jerry Gillette, Ronald Fisher, James Peerenboom, Ronald Whitfield, “Analyzing Water/Wastewater Infrastructure Interdependencies,” white paper, Infrastructure Assurance Center Argonne National Laboratory, 2008.