Journal of Cybersecurity Education, Research and Practice

Volume 2017 | Number 1 Article 2

June 2017

Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation

Guillermo A. Francia III
Jacksonville State University, gfrancia@jsu.edu

Greg Randall
Snead State Community College, greg.randall@snead.edu

Jay Snellen
Jacksonville State University, jsnellen@jsu.edu

Recommended Citation

Francia, Guillermo A. III; Randall, Greg; and Snellen, Jay (2017) "Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2017 : No. 1 , Article 2.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/2

Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation

Abstract

Industrial Control Systems (ICS), which are pervasive in our nation's critical infrastructures, are becoming increasingly at risk and vulnerable to internal and external threats. It is imperative that the future workforce be educated and trained on the security of such systems. However, it is equally important that careful and deliberate considerations must be exercised in designing and implementing the educational and training activities that pertain to ICS. To that end, we designed and implemented pedagogical materials and tools to facilitate the teaching and learning processes in the area of ICS security. In this paper, we describe those resources, the professional development workshop to disseminate the curriculum materials, and the evaluation results pertaining to those artifacts and activities.

Keywords

Industrial Control Systems, Security, Professional Development Workshop, Critical Infrastructure, Vulnerability Assessment of Industrial Control Systems

Cover Page Footnote

This work is supported in part by a Center for Academic Excellence (CAE) Cyber Security Research Program grant (Grant Award Number H98230-15-1-0270) from the National Security Agency (NSA) and a National Science Foundation (NSF) grant (Award No. 1515636). Opinions expressed are those of the authors and not necessarily of the granting agencies.

INTRODUCTION

Industrial Control Systems (ICS), which are pervasive in our nation's critical infrastructures, are becoming increasingly at risk and vulnerable to internal and external threats. The connectivity of these systems to traditional and enterprise Information Technology (IT) infrastructure without regard to their inherent vulnerabilities presents unimaginable threats. These threats could possibly usher successful cyberattacks leading to dire consequences of tremendous losses of human lives and properties as well. It is imperative that the future workforce be educated and trained on the security of such systems. However, it is equally important that careful and deliberate considerations must be exercised in designing and implementing the educational and training activities that pertain to ICS.

The rest of the paper is organized into four parts. First, we present background materials and the motivation behind this work. Second, we provide details on the design and implementation of ICS security curriculum resources and a professional development workshop for college instructors to disseminate the pedagogical materials. Third, we examine the evaluation data that were collected to gauge the efficacy of the curriculum modules, tools, and the summer workshop. Finally, we provide concluding remarks and present possible research avenues that can be pursued as extensions to this work.

BACKGROUND AND MOTIVATION

With an ever-increasing part of our nation's critical infrastructures (CIs) in the hands of public and private employees via computer systems, the need for a cybersecurity educated future workforce in cybersecurity has never been so great. Our critical infrastructures, such as power grid, transportation, drinking water, wastewater treatment, and defense systems, find themselves increasingly vulnerable to internal and external threats that can cause serious damage to our economy and well being. Since the operation of these infrastructures is heavily dependent on control systems, it is imperative that the future workforce be educated and trained on the security of such systems. However, it is equally important that careful and deliberate considerations must be exercised in designing and implementing the educational and training activities that pertain to ICS security. To this end, we embark on a collaborative capacity-building project with the following objectives:

- Develop control system security curriculum modules;
- Offer 2-day faculty development workshops on control systems security;

- Provide cost-effective resources (hardware/software) to enable teachers to develop content, pedagogical knowledge, and skills on cyber and control system security to meet the needs of diverse student populations;
- Evaluate teaching and learning effectiveness on the control system security curriculum;
- Devise tools to facilitate the sharing of teaching expertise and curriculum modules for widespread adoption across national setting; and
- Design and implement a virtual and distributed control system testbed for cybersecurity competitions and experimentations.

In this paper, we provide a description of each of the ICS security curriculum modules that we designed and developed. In addition, we also discuss the experiences gained in a 2-day ICS security-training workshop for college instructors.

PRIOR AND SIMILAR WORKS

There have been similar efforts to address the need for enhancing control systems security. Prior and notable related works that this project builds upon are found in Francia and Snellen (2014), Thornton, Francia, and Brookshire (2012), and Francia and Francia (2014). In 2003, the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NTSB) was established (US Department of Energy, 2003). The primary goal of the so-called “national resource” is to provide a facility for research and training to address critical security vulnerabilities. The Cyber Security Education Consortium (CSEC) has created centers of excellence in automation and control systems to provide training on automation and control systems security (CSEC, 2014). The courses that were created for this security curriculum are excellent training tools to upgrade the security skills of operators. However, widespread adoption is restricted by the high cost and the lack of hardware resources to support the courses in an academic setting. The SANS Institute offers a course on Industrial Control Systems and SCADA Security (SANS, 2014) which targets those personnel who are directly involved with the operation of industrial controls. The exorbitant registration cost for the course makes it impractical for classroom adoption. Our project offers freely available course modules using affordable resources that can deliver hands-on and realistic control systems security training and education.

ICS SECURITY CURRICULUM RESOURCES

Given the constraint of a 2-day long faculty development workshop, we decided to cover the four basic areas of control systems application and security –

Programmable Logic Controller (PLC) programming, control system networks and protocols, control system vulnerability assessment and penetration testing, and defensive techniques and incident response for control systems. Furthermore, for each module, we provided hands-on laboratory projects that introduced the Problem Based Learning (Hung, Jonassen, & Liu, 2008) approach to learning and enabled the participants to practice the technique before applying it in their classrooms. These laboratory exercises were conducted using a control system toolkit, shown in Figure 1, which was designed guided by the fundamental concepts of simplicity, modularity, and portability. Every participant gets to take a toolkit back to his/her home institution. Technology support and a follow-up meeting are provided and scheduled during the school year. The coaching and follow-up process ensures that the instructors are likely to keep the strategy, skill, or concept and make it part of the classroom repertoire (Joyce & Showers, 2002). The initial curriculum modules, which will be enhanced and expanded in subsequent years, are shown in Table 1. A subset of the accompanying laboratory projects is enumerated in Table 2.

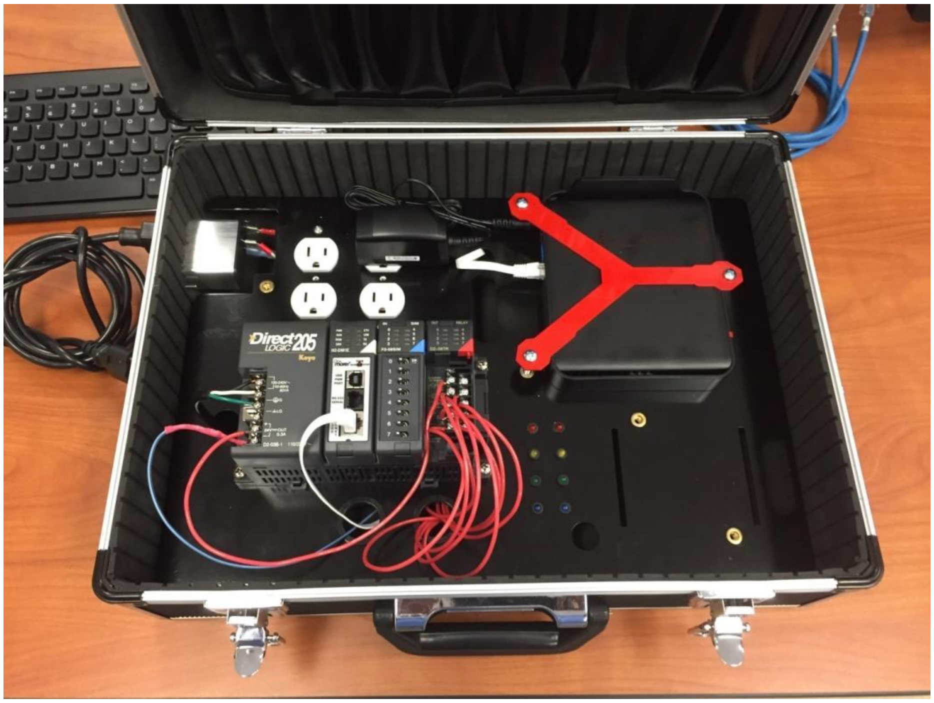

Figure 1. The Industrial Control Systems Toolkit

Module Name: Control System Networks and Protocols **Duration:** 1/2 day **Learning Objectives:** To understand control system networking concepts and communication protocols. **Prerequisite:** Basic knowledge of computer networks. **Topic Outline:** • Control systems and networks (SCADA, DCS, ICS) • Human Machine Interfaces (HMI) • Communication Protocols: ModBus, Profibus, OPC, DNP3, EtherNet/IP, • Deep Packet Inspection of Control packets **Associated Problem-based Laboratory Exercises:** • Control system packet capture and analysis • Deep packet inspection	**Module Name:** PLC Programming, Toolkit Customization, and HMI Security **Duration:** 1/2 day **Learning Objectives:** To understand the basic functions and programming of PLCs; To be able to design and implement a control system HMI; To understand HMI security. **Prerequisite:** Basic knowledge of control devices and associated protocols. **Topic Outline:** • PLC programming using Ladder Logic • Secure programming of control systems • HMI design and implementation • HMI vulnerability analysis and penetration testing **Associated Problem-based Laboratory Exercises:** • PLC programming • Creating a control system Human Machine Interface (HMI) • Customizing the toolkit
Module Name: Defensive Techniques and Incident Response for Control Systems **Duration:** 1/2 day **Learning Objectives:** To understand attack methodologies, defensive	**Module Name:** Control System Vulnerability Assessment and Penetration Testing **Duration:** 1/2 day **Learning Objectives:** To understand control system vulnerability assessment; To be able to perform penetration testing

techniques and incident response for control systems. **Prerequisite:** Basic knowledge of computer networks, control system protocols, and security principles. **Topic Outline:** • Understanding basic firewall rule configuration (Authentication, Authorization, and Accounting) • Intrusion Detection and Prevention Systems on control systems • Indicators of compromise on control systems • Event investigation and data analysis • Incident response policy and plans on control systems • Evidence handling and administration **Associated Problem-based Laboratory Exercises:** • Configure an IDS for a control system environment • Configure and test a firewall configuration for the toolkit • Design a modular firewall policy; Critique a given firewall policy • Perform a behavioral analysis of a compromised control system	of control systems; To be able to recommend remedial actions for control system hardening. **Prerequisite:** Basic knowledge of control system and network protocols. **Topic Outline:** • Attack surfaces of control systems • Vulnerability assessment and tools • Penetration testing and tools **Associated Problem-based Laboratory Exercises:** • Control system reconnaissance and mapping • Vulnerability assessment of control systems • Penetration testing of control system networks

Table 1. The Control System Security Curriculum Modules

Lab 1: ICS Network Packet Capture and Analysis with Wireshark **Duration:** 25 minutes **Learning Objectives:** To understand ICS communication protocols and ICS network packet capture and analysis. **Lab Tasks:** Capture live ICS packets Analyze two types of ICS packets: Modbus and DNP3. Write a report on the results of the analysis.	**Lab 2:** PLC Programming and ICS Communication Setup **Duration**: 30 minutes **Learning Objectives:** To understand ICS communication setup. To learn ladder logic programming using a simulator and a Direct Logic PLC. **Lab Tasks:** Setup a wireless router for ICS communication. Write a ladder logic program to implement a given control specification. Test the ladder logic program using a simulator. Download and test the program on a PLC.
Lab 3: ICS Firewall Configuration **Duration**: 45 minutes **Learning Objectives:** To understand the basics of firewall configuration. To design a modular firewall policy. To configure an intrusion detection system for an ICS environment. **Lab Tasks:** Configure remote shell access using PuTTY. Reconfigure router to enable remote shell access and event logging. Implement and test firewall configuration using IPTables. Download sample firmware to PLC and open HMI for testing.	**Lab 4:** ICS Reconnaissance and Enumeration **Duration:** 45 minutes **Learning Objectives:** To understand ICS reconnaissance, network mapping, and device enumeration using Zenmap. To be able to identify ICS devices on the network. **Lab Tasks:** Use Zenmap to perform an ICS network reconnaissance. Analyze the results and write a report on network mapping and the configuration information of all devices that were discovered. Perform an ICS device discovery on the Internet using Shodan.
Lab 5: ICS Penetration Testing and Exploit **Duration**: 45 minutes **Learning Objectives:** To understand the basics of penetration testing and system exploitation. To learn how to	**Lab 6:** ICS Vulnerability Assessment **Duration:** 30 minutes **Learning Objectives:** To understand basic ICS vulnerability assessment. To be able to perform a vulnerability assessment on an ICS using an open source tool: OpenVAS.

apply the Kali Linux tool on the ICS environment. **Lab Tasks:** Launch Metasploit. Specify Modbusclient as the exploit. Read PLC coil values. Modify the coil values. Run the HMI program to verify that coil values are changed.	**Lab Tasks:** Configure OpenVAS on Kali Linux. Perform an ICS network reconnaissance. Start the OpenVAS services and save the prognostic report. Analyze and write a report on the discovered vulnerabilities.

Table 2. ICS Security Laboratory Projects

DETAILS OF THE LABORATORY PROJECTS

The development of the hands-on exercises that were used in the ICS laboratory projects are based upon the five attack phases noted by EC Council's Ethical Hacking and Countermeasures Certified Ethical Hacker (C|EH) guide (International Council of E-Commerce Consultants, 2010). The laboratory scenario provided to the participants consisted of six sequenced laboratory exercises that details each phase of the attack, which includes reconnaissance, scanning, and gaining access, maintaining access, and covering tracks. During the course of the two-day project, participants used the Kali Linux penetration testing distribution to perform network scanning and exploitation of the Industrial Control Systems Toolkit. Participants used a simulated WAN environment to perform scanning and enumeration. Figure 2 depicts the physical layout of the network environment used in the exercises.

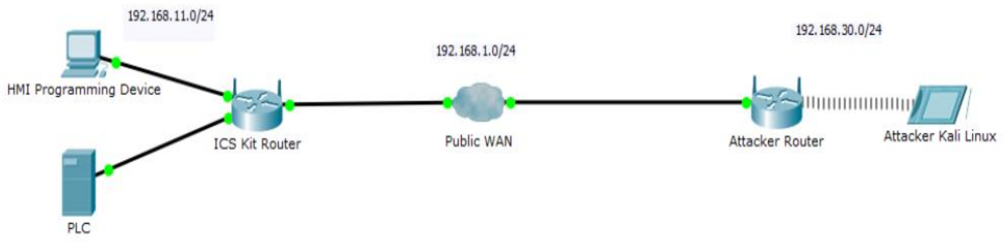

Figure 2. Simulated WAN Environment

For the first day of the project, participants completed scanning, enumeration, and gaining access using Wireshark and Wifite attack tools located in the Kali Linux distribution. Once access to the network was successful, participants were able to perform deep packet analysis of the systems within the network. The goal of the day two exercise was to locate and exploit the PLC in the ICS toolkit. Packets captured from the ICS router were analyzed using Wireshark by filtering the transmissions on port 502, which is the standard port identification for Modbus communication. ICS traffic capture provided enough information for the participant to conduct an exploitation of the ICS programmable logic controller. The last exercise in the scenario used the Modbus Client exploit module from Armitage found in the Kali Linux distribution (Offensive Security, 2016). Armitage allowed the participants to create a reverse TCP connection to the PLC using port 502. With a successful connection to the PLC, the participants were able to send control data to the PLC, which resulted in complete control of inputs and outputs on the system.

The laboratory exercise on Defensive Security involves analyzing and expanding the default firewall rule set for the router included with the ICS lab kit, with an emphasis on securing the Modbus protocol. In order to modify the firewall rules using a command-line interface, it will first be necessary to configure the router to allow remote shell access. This can be done from any workstation, which has a Web browser and a secure shell (SSH) client installed such as PuTTY, a free SSH and telnet client for Windows. In order to test the firewall configuration, the PLC is first configured to communicate with the HMI through the local network. A simple HMI program has been provided with this exercise, along with the corresponding ladder logic firmware. After the PLC has been configured and tested, the router in the ICS lab kit is configured to accept remote SSH connections, and message logging is enabled. Once this has been accomplished, the firewall is configured at the command line using IPTABLES. After completing the desired configuration, it is made permanent and readily available by creating a firewall configuration script. Specifically, each participant is required to perform the following:

- Configure the router firmware for remote shell access and event logging
- View and analyze the default firewall configuration
- Open a Modbus connection to the PLC within the LAN
- Add and test a firewall rule to allow Modbus connections from the WAN
- Add and test a rule to block Modbus connections from a specific WAN host
- Add and test a rule to block all Modbus traffic from the WAN
- Add and test a rule to enable auditing of successful and unsuccessful Modbus connection attempts from the WAN

The equipment setting for this laboratory exercise is depicted in Figure 3.

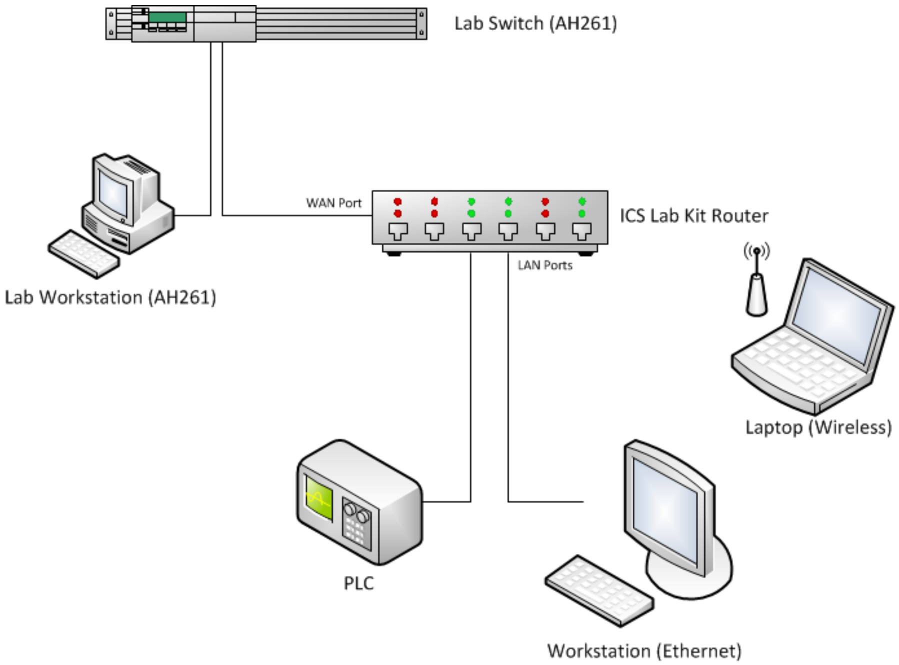

Figure 3. The Defensive Security Equipment Setting

PROJECT EVALUATION

The evaluation plan includes a mixed methods approach utilizing both qualitative methods prescribed by Patton (2002) and quantitative methods prescribed by Creswell (2005) to guide the formative and summative evaluation procedures. Formative evaluation procedures assure continual improvement of the project, and summative evaluation procedures assess project objectives and implementation.

PRE-WORKSHOP SURVEY

Prior to the workshop, participants (n = 10) completed a short survey to gauge their level of understanding of the various control systems security topics to be covered in the workshop. The survey used a standard four-point Likert scale and asked participants to rate their familiarity with each of the workshop's major topics. Choices were "Very Familiar" (4 points), "Somewhat Familiar" (3 points), "Not Very Familiar" (2 points) and "Not at all familiar" (1 point). The pre-workshop survey results showed that the specific topics were well chosen. A majority of participants selected "Not Very Familiar" or "Not at all familiar" on each of the seven workshop topics. Participants reported being least familiar with Human-

Machine Interface (HMI) programming (mean score 1.73), Deep Packet Inspection (mean score 1.55), and Industrial Control System (ICS) Security (mean score 1.18).

The pre-workshop survey also asked which of the workshop topics were included in their curricula. Only Firewall Configuration was chosen by a majority of participants responding to the question (n = 10, 60%). Industrial Control Systems / PLCs, Ladder Logic Programming, and Defense in Depth are included in 40% of participant curricula. Industrial Control System (ICS) Security was not included in the curriculum taught by any of the participants.

POST-WORKSHOP SURVEY

Immediately following the workshop, participants took a post-workshop survey. The post-workshop survey focused on the primary areas outlined in the project's evaluation plan—the quality of the toolkit, the quality of the laboratory activities, the quality of the workshop sessions, and how prepared the participants felt to teach the topics covered in the workshop. Like the pre-workshop survey, a majority of the survey was a four-point Likert scale, with more positive choices rated with the choices being "Strongly Agree," "Agree," "Disagree," and "Strongly Disagree." Laboratory activities, the toolkit, and the curriculum modules were rated from "Very Effective" to "Very Ineffective."

Respondents (n = 10) overwhelmingly agreed they were better prepared to teach the topics covered in the workshop, with the exception of one participant who did not feel better prepared to teach Penetration Testing. Comments indicated that Penetration Testing and PLC programming were viewed as having been covered most effectively.

All of the laboratory activities were rated very positively, with average scores ranging from 3.5 to 3.89. Comments indicated that the modules were well received and would be good experiences for students, but that the PLC and HMI modules could be improved.

The Control System Security Toolkit was rated very positively, with 90% calling it "Very Effective" and 10% calling it "Somewhat Effective." Comments about the toolkit indicated that the toolkit would be very valuable at providing a hands-on experience for students.

The four main curriculum modules were also rated extremely positive, with PLC, Penetration Testing, and ICS mentioned by name as being most effective. Respondents also indicated the workshop was a valuable professional networking experience. When asked for how the workshop could be improved, responses indicated that the amount of material was high for time allotted.

EVALUATION SUMMARY

Overall, the pre- and post-workshop surveys indicate that the topics for the workshop were well chosen and well delivered, and the toolkit was rated as excellent. The results highlight that Industrial Control System Security is a topic that is not well-covered in computer science curricula and the workshop, as intended, highlighted the importance of that and other aspects of cybersecurity and provided instructors with tools (the toolkit and the laboratory activities) to integrate control system security into their courses.

CONCLUSION AND FUTURE PLANS

In this paper, we argued for the critical need for an educated workforce that is trained in industrial control systems security. We also reported the ICS curriculum modules and the laboratory exercises that were disseminated to a group of college instructors in a professional development workshop during the summer. The evaluation results that were gathered prior and after the workshop highlight the following notable pedagogical facts and outcomes:

- ICS security is not a part of the information security curriculum in college;
- The curriculum modules and the related laboratory projects were overwhelmingly well received;
- The pedagogical materials on ICS security will be integrated by the participants into their respective security curriculum; and
- The ICS toolkit was rated very positively and will greatly benefit and enhance the participants' existing infrastructure.

Future plans, connected with these activities and toolkit, are the following:

- The enhancement of the toolkit to include a Raspberry Pi for Internet of Things (IoT) security; and
- The development of additional curriculum modules in the areas of deep packet inspection of other ICS network packets that are not previously covered, secure programming in ICS program development, and threat intelligence/kill chain model for ICS security.

ACKNOWLEDGEMENTS

This work is supported in part by a Center for Academic Excellence (CAE) Cyber Security Research Program grant (Grant Award Number H98230-15-1-0270) from the National Security Agency (NSA) and a National Science Foundation (NSF) grant (Award No. 1515636). Opinions expressed are those of the authors and not necessarily of the granting agencies.

REFERENCES

ATE Centers. (2004). *CSEC Advances Cybersecurity & Homeland Defense.* Retrieved August 8, 2016, from Cyber Security Education Consortium (CSEC): http://www.atecenters.org/st/csec/

Creswell, J. (2005). *Education Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research* (2nd ed.). Upper Saddle River, NJ: Merrill.

Francia, G. A., & Francia, X. P. (2014). Critical Infrastructure Protection and Security Benchmarks. In M. Khrosrow-Pour, *Encyclopedia of Information Science and Technology* (pp. 4267-4278). Hersey, PA: IGI Global.

Francia, G. A., & Snellen, J. (2014). Embedded and Control Systems Security Projects. *Information Security Education Journal*, *1*(2), 77-84. http://www.dline.info/isej/fulltext/v1n2/3.pdf

Hung, W., Jonassen, D. H., & Liu, R. (2008). Problem Based Learning. In J. M. Spector, J. G. van Merrienboer, M. D. Merrill, & M. Driscoll, *Handbook of Research on Educational Communications and Technology* (3rd ed., pp. 485-506). Mahwah, NJ: Erlbaum.

International Council of E-Commerce Consultants. (2010). *Ethical Hacking and Countermeasures.* Clifton Park, NY: CENGAGE Learning.

Joyce, B., & Showers, B. (2002). *Student Achievement Through Staff Development.* Alexandria, VA: Association for Supervision and Curriculum Development.

Offensive Security. (2016). *Penetration Testing and Ethical Hacking Linux Distribution.* Retrieved September 9, 2016, from Kali Linux: https://www.kali.org

Patton, M. (2002). *Qualitative Evaluation and Research Methods* (4th ed.). Newbury Park, CA: Sage.

Thornton, D., Francia, G. A., & Brookshire, T. (2012). Cyberattacks on SCADA Systems. *2012 Colloquim for Information Systems Security Education (CISSE).* Mobile, AL.

US Department of Energy. (2003). *National SCADA Test Bed.* Retrieved August 8, 2016, from Office of Electricity Delivery & Energy Reliability: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed