Embedded and Control Systems Security Projects

Guillermo A. Francia, III, Jay Snellen III
Center for Information Security and Assurance,
Mathematical, Computing, and Information Sciences
Jacksonville State University
700 Pelham Rd. North
Jacksonville, AL 36265
United States of America
{gfrancia, jsnellen@jsu.edu}

ABSTRACT: **:** *Robust and resilient cyber defense mechanisms and better educated future workforce are vital components for the protection of our nation's critical infrastructures. As such, the need for an enhanced information assurance and security curriculum with emphasis on embedded and control systems can no longer be ignored. Recognizing this training gap, we designed and implemented a collection of laboratory projects for an embedded and control systems security curriculum that emphasizes a balance between theory and application. Each project, whose main purpose is to stimulate learning and motivate critical thinking among undergraduate students, is designed with careful attention to details. In this paper, we provide the learning objectives, knowledge prerequisites, activities involved, expected outcomes, and a list of suggested references for additional reading assignments for each one of those projects.*

Keywords: Critical Infrastructures, Control Systems, Embedded Systems, SCADA, Security, Vulnerability

Received: 1 July 2014, Revised 4 August 2014, Accepted 8 August 2014

1.Introduction

In 2011, the Department of Homeland Security (DHS) released a document entitled "*Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*" (DHS, 2011). This document clearly underscores the importance of cyberspace in our way of life. With an ever-increasing part of our nation's critical infrastructures (CIs) being connected to the Internet, the need for a more sophisticated cyber defense mechanism and better educated future workforce has never been so great. Our critical infrastructures, such as power grid, transportation, drinking water, manufacturing plants, waste water 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 — and, increasingly, devices in the consumer appliance and automotive markets—is heavily dependent on embedded and control systems, it is imperative that current and 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 these educational and training activities.

In what follows, we present hands-on laboratory projects that are envisioned to stimulate learning and motivate critical thinking among undergraduate students in embedded and control systems security.

2. Background

The need for Information Assurance and Security education is well established. The ACM/IEEE's Computer Science Curriculum guidelines (CS2013), finalized in December 2013, include the Information Assurance and Security Knowledge Area (ACM/IEEE, 2013). In addition, a joint program by the U.S. National Security Agency (NSA) and the Department of Homeland Security (DHS) to promote information assurance education and research prescribes knowledge units that are specifically geared towards the protection of control systems (NSA/DHS, 2014).

Previous works on curriculum development in the areas of critical infrastructure and control systems security include Auerswald, et al. (2008) and Francia (2011).

Beyond these areas, however, an education in information assurance and security is also becoming increasingly important to practitioners in the areas of consumer electronics and automotive systems. With the proliferation of networked embedded computers in household appliances and other consumer devices, and the rising complexity of automotive computers, the vulnerabilities and threats that have long been an issue to critical infrastructure and control systems are increasingly becoming an issue to the "*Internet of Things*" (Roman, Najera, & Lopez, 2011; Atzori, Iera, & Morabito, 2010). This places a new premium on information assurance and secure coding practices, making a rigorous curriculum in information security of increasing importance to all students of computer and information sciences. To this end, we require students to investigate the feasibility and security of the AllJoyn Service Frameworks in an Internet of Things (IoT) application environment. The AllJoyn Service Frameworks (AllJoyn, 2014) include open source software development kits (SDKs) which allow rapid development of peer-to-peer applications in IoT devices.

3. Control Systems Security Curriculum

Experiential learning on information security using hands-on laboratory activities has been extensively studied (e.g. Rosenberg & Hoffman, 2006; Abler, et al., 2006). In one notable work by Konak, et al. (2014), the authors argue that hands-on activities that are based on the Kolb's Experiential Learning Cycle (Kolb, 1984) framework is more effective in enhancing student learning.

Theorists and researchers have often stated the conviction that helping students construct their own meaningful knowledge and skills is the primary focus of education (Jonassen, 1991). The challenges for educators are not simply to adopt innovative teaching techniques, but to direct students toward authentic forms of achievement and connect learning to real-world problems. Hence, the following laboratory activities and assessment plans are designed based on the theoretical and pedagogical frameworks of delivering effective instructions. Laboratory activities will be evaluated through surveys addressing learner's perspective towards the efficacy of the hands-on activities and their level of satisfaction. The results from the collected data will provide us with evidence to determine the success of each laboratory project and the curriculum as a whole.

Our design of a new course on embedded and control systems security is guided by the Knowledge Units (KUs) that are specified in the Centers of Academic Excellence for Information Assurance/Cyber Defense Focus Area on Industrial Control Systems—SCADA Security (NSA/DHS, 2014). These KUs are:

- Cybersecurity Planning and Management
- Embedded Systems
- Hardware/Firmware Security
- Industrial Control Systems
- Intrusion Detection
- Operating Systems Hardening
- Secure Programming Practices
- Security Risk Analysis
- Systems Engineering
- Vulnerability Analysis

Since most of the KUs are already covered in existing security courses, the development of the new course puts special emphasis on embedded systems, hardware/firmware security, industrial controls, and secure programming.

4. Laboratory Projects

4.1 Project 1: HMI Design and Security (Estimated Completion Time: 6 hours)

4.1.1 Learning Objectives

- To be able to design, implement, and test a Human Machine Interface (HMI) for a control system.
- To familiarize with security issues pertaining to HMI.
- To be able to gain a hands-on understanding of the functionalities of one of the most common control system protocols: Modbus/TCP.

4.1.2 Prerequisites

Knowledge of Modbus/TCP protocol, HMI programming using InduSoft Web Studio, Visual Studio and C#.

4.1.3 Laboratory Activities

- Design an HMI for a water pumping station that is controlled by Programmable Logic Controllers (PLC); design specification is provided.
- Implement and test the design using Modbus /TCP.
- Perform a vulnerability analysis on the implementation.

4.1.4 Report and Assessment

Write a report that:

- Documents your design and implementation,
- Describes the vulnerability assessment of the system, and
- Provides remedial measures to correct the security weaknesses of the system.

4.1.5 References/Additional Readings

(Pollet, 2002; Francia, Bekhouche, Marbut, & Neuman, 2012).

4.2 Project 2: Control Systems Forensics (Estimated Completion Time: 6 hours)

4.2.1 Learning Objectives

- To be able to collect, preserve, and analyze digital forensic evidence associated with control systems.
- To be able to gain a hands-on understanding of deep packet inspection of control system network packets.
- To familiarize with open-source digital forensic tools for collection preservation, and analysis.

4.2.2 Prerequisites

Knowledge of control system protocol (MODBUS/TCP, CIP, Profibus, etc.) packet structure, Wireshark, SIFT, Kali, and DEFT.

4.2.3 Laboratory Activities

- Capture packets in the SCADA laboratory using Wireshark.
- Preserve the digital forensic data.
- Perform an analysis of the captured packets using the open-source tools.

4.2.4 Report and Assessment

Write a report that:

- documents the processes of digital forensic collection and preservation, and 0preservation, and
- describes your findings during the analysis process.

4.2.5 References/Additional Readings

(Antonello, R., et al., 2012; Byres, 2012; Fabro & Cornelius, 2008; Francia & Francia, 2013).

4.3 Project 3: Programmable Logic Controller (PLC) Secure Programming (Estimated Completion Time: 10 hours)

4.3.1 Learning Objectives

- To be able to design, implement, and test a control system.
- To familiarize with ladder logic programming.
- To be able to develop a secure application that will be used to operate a SCADA system prototype.
- To be able to gain a hands-on understanding of the functionalities of a PLC and the importance of secure development.

4.3.2 Prerequisites

Knowledge of ladder logic programming, secure development, and Modbus/TCP protocol.

4.3.3 Laboratory Activities

- Design a SCADA system application that will operate a waste water pumping station that is controlled by two PLC devices; design specification is provided
- Implement and test the design using ladder logic programs.
- Perform a vulnerability analysis on the implementation.

4.3.4 Report and Assessment

Write a report that:

- documents your design and implementation,
- describes the vulnerability assessment of the system, and
- provides remedial measures to correct the security weaknesses of the system.

4.3.5 References/Additional Readings

(Bartelt, 2011; PLC Manual, 2014; Stoufer, Falco, & Scarfone, 2008; Todd, 2007).

4.4 Project 4: Secure Microcontroller Programming (Estimated Completion Time: 6 hours)

4.4.1 Learning Objectives

- To explore secure programming techniques within the context of microcontroller-based embedded systems.
- To understand the importance of resource management and memory safety within embedded systems, and the vulnerabilities that can arise due to insecure programming practices.
- To gain hands-on experience with code hardening and regression testing.

4.4.2 Prerequisites

Knowledge of 8051 Microcontroller Architecture; C programming using SDCC.

4.4.3 Laboratory Activities

- Acquire privileged information by identifying and exploiting security flaws within a microcontroller-based data acquisition system.
- Perform a vulnerability analysis of the microcontroller firmware, identify the causes of the discovered flaws, and develop and implement revisions to correct them.

- Performing regression testing of the revised firmware, to ensure that the discovered vulnerabilities have been eliminated without affecting the functionality of the system.

4.4.4 Report and Assessment

Write a report that:

- describes the discovery process which revealed the security flaws,
- describes the firmware analysis process, the causes of the discovered flaws, and the implemented solutions, and
- describes the regression testing process, and the methods of confirming that the vulnerabilities have been eliminated.

4.4.5 References/Additional Readings

(Huang, 2009; Graff & van Wyk, 2003; Stroustrup, 2009).

4.5 Project 5: Security for Embedded Systems and Web Services (Estimated Completion Time: 10 Hours)

4.5.1 Learning Objectives

- To explore the use of Web services for the integration of distributed, heterogeneous embedded systems.
- To understand the applications of Web services in industrial control systems.
- To understand the issues of synchronization, timing, and security which can arise from the use of Web services with embedded systems.

4.5.2 Prerequisites

Knowledge of Android programming and Java servlets.

4.5.3 Laboratory Activities

- Design a set of Web services to expose server-side business data, and an Android client application which uses this data to construct a simple Human Machine Interface (HMI).
- Capture packets in the laboratory using Wireshark, and analyze the captured packets to gauge the security of the application.
- Modify the Web services and client application for encrypted communications using SSL, without affecting functionality.
- Capture and analyze network packets using Wireshark again, comparing the security of the application before and after the integration of SSL.

4.5.4 Report and Assessment

Write a report that:

- documents the design and implementation,
- describes the initial security assessment of the system, and
- describes the security assessment of the system after the integration of SSL encryption.

4.5.5 References/Additional Readings

(Six, 2012; Hoog, et al., 2011; Bertino, et al., 2010).

4.6 Project 6: Secure Peer-to-Peer Communications for Embedded Systems (Estimated Completion Time: 10 Hours)

4.6.1 Learning Objectives

- To explore the challenges of developing and integrating competitive implementations of a common specification.
- To investigate the feasibility and security of the open source AllJoyn Service Framework in an IoT application environment.
- To compare and contrast a variety of security models.

4.6.2 Prerequisites

Knowledge of Android systems, AllJoyn Framework, and network programming.

4.6.3 Laboratory Activities

- Based on a provided specification, two teams will independently implement a simple peer-to-peer messaging and control system for Android-based mobile devices.
- Both teams will participate in integration testing of the two competing implementations, working together to resolve any incompatibilities that are found. Both implementations must interoperate according to the specification.
- Investigate various security models, either message-based or session-based, and decide on the best model for securing the control or embedded system.
- Both teams will add the security component to their respective implementations, and will perform a new round of integration testing.

4.6.4 Report and Assessment

Write a report that:

- Documents the design and implementation,
- Documents the integration testing process, including any compatibility issues, and
- Compares and contrasts the security models that were evaluated, and describes the security implementation and testing processes.

4.6.5 References/Additional Readings

(Dwivedi, Clark, & Thiel, 2010; Boudriga, 2010).

5. Conclusion and Future Work

This paper outlined a number of laboratory projects that are used to enhanced an embedded and control systems security curriculum. Although these hands-on exercises and experimentations are in no way exhaustive, they can be can be utilized as building blocks with which advanced and more sophisticated security laboratory activities can be built.

These laboratory projects are part of an on-going curriculum development in the area of embedded and control systems security. A major challenge is the introduction of more advanced laboratory activities that mimic realistic security incursions and defense scenarios. Future work will include:

- Simulation of random attacks on embedded and control systems;
- Activities that will scrutinize the security of IoT devices; and
- Introduction of hands-on exercises on automobile control security.

References

[1] Abler, R. T., Contis, D., Grizzard, J.B. and Owen, H. L. (2006). Georgia Tech Information Security Center Hands-on Network Security Laboratory. IEEE Trans. on Educ. 49, 1 (September 2006), 82-87. DOI=10.1109/TE.2005.858403 http://dx.doi.org/10.1109/TE.2005.858403.

[2] AllJoyn (2014). About AllJoyn.Retrieved July 28, 2014 from https://www.alljoyn.org/about

[3] Antonello, R., et al. (2012). Deep Packet Inspection Tool and Techniques in Commodity Platforms: Challenges and Trends. *Journal of Network and Computer Applications*, November , 35(6):1863-1878. Elsevier, Ltd.

[4] Association for Computing Machinery (ACM)/IEEE Computer Society Joint Task Force, Curriculum Guidelines for Undergraduate Degree Programs in Computer Science, Website: http://www.acm.org/education/CS2013-final-report.pdf. December 20, 2013.

[5] Atzori, L., Iera, A., Morabito, G.. (2010).The Internet of Things: A Survey,Computer Networks, 54 (15), October. p. 2787-2805.

[6] Auerswald, P., Branscomb, L.M., Shirk, S., Kleeman, M., Porte, T. M., Ellis, R.N. (2008). Critical Infrastructure and Control Systems Security Curriculum," Department of Homeland Security, version 1.0, Washington, DC, March.

[7] Bartelt, Terry (2011). Industrial Automated Systems Instrumentation and Motion Control, Delmar-Cengage Learning Publishing.

[8] Bertino, Elisa, et al. (2010). Security for Web Services and Service-Oriented Architectures, Springer.

[9] Boudriga, Noureddine (2010). Security of Mobile Communications, CRC Press.

[10] Byres, Eric (2012). Understanding Deep Packet Inspection for SCADA Security. White paper—Tofino Security. December 12, 2012. Retrieved January 10, 2013 from http://www.tofinosecurity.com.

[11] Department of Homeland Security (2011). Blueprint for a Secure Cyber Future The Cybersecurity Strategy for the Homeland Security Enterprise,Website: http://www.dhs.gov/blueprint-secure-cyber-future. Last access: July 16, 2014.

[12] Dwivedi, Himanshu, Clark, Chris, Thiel, David (2010). Mobile Application Security, McGraw-Hill..

[13] Fabro, M., Cornelius, E. (2008).Recommended Practice: Creating Cyber Forensics Plans for Control Systems,August 2008. Retrieved July 16, 2014 from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf.

[14] Francia, G.A., III. (2011).Critical Infrastructure Curriculum Modules, *In*:Proceedings of the 2011 Information Security Curriculum Development (INFOSECCD) Conference. Kennesaw, GA. October.

[15] Francia, G.A. III , Bekhouche, N., Marbut, T., Neuman, C.(2012).Portable SCADA Security Toolkits. *International Journal of Information and Network Security*.1(4), p. 265-274. October.

[16] Francia, G.A. III, Francia, X.P. (2013).Dissecting Industrial Control Systems Protocol for Deep Packet Inspection, *In*: Proceedings of the 17th Annual Colloquium for Information Systems Security Education (CISSE), Mobile, AL, June 10-13.

[17] Graff, Mark. G.., van Wyk, Kenneth, R. (2003). Secure Coding: Principles and Practices, O'Reilly Media.

[18] Hoog, Andrew, et al. (2011). Android Forensics: Investigation, Analysis, and Mobile Security for Google Android, Syngress.

[19] Huang, Han-Way (2009). Embedded System Design with the 80C51, Cengage Learning.

[20] Jonassen, D. H. (1991). Objectivism versus constructivism: do we need a new philosophical paradigm? *Educational Technology Research and Development*, 39 (3), 5-14.

[21] Kolb, D.A. (1984). Experiential Learning: Experience as the Source of Learning and Development. Prentice-Hall, New Jersey.

[22] Konak, A., Clark, T.K., Nasereddin, M. (2014). Using Kolb's Experiential Learning Cycle to Improve Student Learning in Virtual Computer Laboratories. Comput. Educ. 72 (March 2014), 11-22. DOI=10.1016/j.compedu.2013.10.013 http://dx.doi.org/10.1016/j.compedu.2013.10.013

[23] National Security Agency/Department of Homeland Security (NSA/DHS, 2014), Centers of Academic Excellence for Information Assurance/Cyber Defense Focus Areas.

[24] PLC Manual (2014). PLC Manual Basic Guide to PLCs, Website: http://www.plcmanual.com/. Last access: July 15.

[25] Pollet, J.(2002). Developing a Solid SCADA Security Strategy, 2nd ISA/IEEE Sensors for Industry Conference, p.148-156, Nov. 19-21.

[26] Roman, R., Najera, P., Lopez, J.(2011). Securing the Internet of Things, *Computer*, 44 (9) September. p. 51-58.

[27] Rosenberg, T., Hoffman, L. J. (2006). Taking Networks on the Road: Portable Solutions for Security Educators. IEEE Security and Privacy 4, 1 (January 2006), 57-60. DOI=10.1109/MSP.2006.25 http://dx.doi.org/10.1109/MSP.2006.25.

[28] Six, Jeff (2012). Application Security for the Android Platform, O'Reilly Media.

[29] Stouffer, K., J. Falco, K. Scarfone (2008). Guide to Industrial Control Systems (ICS) Security, NIST, Gaithersburg, MD, Special Publication 800-82, September.

[30] Stroustrup, Bjarne (2009). Programming: Principles and Practice Using C++, Pearson Education.

[31]Todd, W. (2007). Ladder logic: Strengths and Weaknesses, *Control Engineering*, 54 (3), p. 17-18, March.

Author Biographies

Dr. Guillermo A. Francia, III received his Ph.D. in Computer Science from New Mexico Tech. Before joining Jacksonville State University (JSU), he was the chairman of the Computer Science department at Kansas Wesleyan University. Dr. Francia is a recipient of numerous grants and awards. His projects have been funded by the National Science Foundation, Eisenhower Foundation, Department of Education, Department of Defense, the State Department, and Microsoft Corporation. He served as a Fulbright scholar to Malta in 2007. Currently, Dr. Francia is a Professor of Computer Science and the Director of the Center for Information Security and Assurance at JSU.

Jay Snellen, III received his Master's degree in Computer Systems and Software Design from Jacksonville State University in 2009. For three years, he has served as an adjunct instructor at Jacksonville State University, where his teaching interests at the undergraduate level include information systems, computer programming, embedded systems, and information assurance. He previously worked for fifteen years in the Information Technology industry in both the public and private sector, where his responsibilities included computer network and security policy design and administration.