NPS-CS-16-004

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

NETWORK FORENSICS LESSONS FOR

INDUSTRIAL CONTROL SYSTEMS

by

Thuy D. Nguyen

December 2016

Approved for public release; distribution is unlimited

Prepared for: National Science Foundation

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
08-12-2016	Technical Report	

4. TITLE AND SUBTITLE

NETWORK FORENSICS LESSONS FOR INDUSTRIAL CONTROL SYSTEMS

5a. CONTRACT NUMBER

5b. GRANT NUMBER
DUE-1140938

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Thuy D. Nguyen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

NPS-CS-16-004

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

The views expressed in this material are those of the author and do not reflect the official policy or position of the Department of Defense, the National Science Foundation, or the U.S. Government.

14. ABSTRACT

Network security monitoring is an important element in incident response and forensics investigation. Most forensic investigators are trained to recognize abusive network behavior in conventional information systems, but they may not have the technical skills to detect anomalous traffic patterns in industrial control systems that manage critical infrastructure services. We have developed and laboratory-tested hands-on teaching material to introduce students to forensics investigation of intrusions on an industrial network. Rather than using prototypes of ICS components, our approach utilizes commercial industrial products to provide students a more realistic simulation of an ICS network. The lessons cover four different types of attacks and the corresponding post-incident network data analysis. This report describes the initial development of these network forensics lessons.

15. SUBJECT TERMS

Industrial control system, network forensics, Ethernet/Industrial Protocol (EtherNet/IP), Common Industrial Protocol (CIP), cybersecurity education

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Thuy Nguyen
Unclassified	Unclassified	Unclassified	UU	45	**19b. TELEPHONE NUMBER** *(include area code)* 831-656-3989

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Steven R. Lerman
Provost

The report entitled "*Network Forensics Lessons for Industrial Control Systems*" was prepared for and funded by the National Science Foundation.

Further distribution of all or part of this report is authorized.

This report was prepared by:

_____
Thuy D. Nguyen
Faculty Associate – Research
Department of Computer Science

Reviewed by:

_____
Peter J. Denning, Chairman
Department of Computer Science

Released by:

_____
Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network security monitoring is an important element in incident response and forensics investigation. Most forensic investigators are trained to recognize abusive network behavior in conventional information systems, but they may not have the technical skills to detect anomalous traffic patterns in industrial control systems that manage critical infrastructure services. We have developed and laboratory-tested hands-on teaching material to introduce students to forensics investigation of intrusions on an industrial network. Rather than using prototypes of ICS components, our approach utilizes commercial industrial products to provide students a more realistic simulation of an ICS network. The lessons cover four different types of attacks and the corresponding post-incident network data analysis. This report describes the initial development of these network forensics lessons.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. MOTIVATION 1
B. CONTRIBUTION 3
II. RELATED WORK 5
III. BACKGROUND 7
A. REFERENCE FUNCTIONAL MODEL 7
B. COMMON INDUSTRIAL PROTOCOL 8
C. ETHERNET/INDUSTRIAL PROTOCOL 9
IV. APPROACH 11
A. THREAT MODEL 11
B. EXPERIMENTAL LABORATORY 12
C. DATA COLLECTION 14
V. LESSON DEVELOPMENT 17
A. ATTACK SCENARIOS 17
1. Reconnaissance Attack 17
2. Data Exfiltration Attack 18
3. Malicious Insider Attack 18
4. Denial-of-Service Attack 19
B. LESSON DESCRIPTION 20
1. Lesson 1: Reconnaissance 21
2. Lesson 2: Data Exfiltration 22
3. Lesson 3: Controller Manipulation 22
4. Lesson 4: Resource Exhaustion 23
VI. CONCLUSION 25
LIST OF REFERENCES 27
INITIAL DISTRIBUTION LIST 31

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. ICS vulnerabilities reported to ICS-CERT. Source: [6]. 2
Figure 2. ISA99 Reference Model. Source: [35] 7
Figure 3. A CIP node with multiple object instances. Source: [9]. 8
Figure 4. EtherNet/IP packet format. Source: [10]. 9
Figure 5. ICS experimental laboratory. 12
Figure 6. Lesson development laboratory. 13
Figure 7. Resource exhaustion using RequestSession command. 20

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Attack scenarios 11
Table 2. Summary of data corpus. 14
Table 3. Summary of packet trace files in dataset D. 15

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In recent years, industrial control systems (ICS) have increasingly become targets of cyber-attacks. These cyber-physical systems are no longer isolated, as they are alarmingly connected to vulnerable external networks to provide real-time assessment of operating conditions. Our research investigates vulnerabilities in widely-used industrial network protocols and develops hands-on course material to introduce students to forensics investigation of intrusions on industrial networks.

A. MOTIVATION

A recent publicly reported ICS attack was a large-scale power outage in Ukraine in December 2015. The U.S. Department of Homeland Security reported that the attack crippled three regional power distribution companies through a series of highly synchronized operations that required extensive, long-term reconnaissance of the target operating environment [1]. Other reports indicated that variants of the BlackEnergy and KillDisk (aka Disakil Trojan) malware were present on the compromised system [2, 3]. In December 2014, ICS-CERT issued an alert stating that control system networks in the United States have been infected by the BlackEnergy malware since 2011. ICS-CERT recently confirmed that a BlackEnergy 3 variant was present on the Ukrainian systems, and that it appears to have been delivered via spear phishing emails with malicious attachments [4].

IRONGATE, an ICS malware that surfaced in June 2016 [5], includes a Stuxnet-style exploit with enhancements, i.e., sandbox evasion, and hiding its activity by actively recording and replaying process data. At the time of its discovery, IRONGATE seemed to be prototype malware, but its existence confirms the threat of stealthy malware lurking in repositories and potentially operational ICS networks. It was introduced in 2014 but not detected until late 2015 by researchers who were looking for a different exploit—antivirus software used in the hosting malware repository did not recognize it.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports that, for fiscal year 2015, there was an increase in reported vulnerabilities relating to cryptographic issues, poor code quality,

credentials management, and access controls (including permissions and privileges management). The report also shows a significant decrease in the improper input validation category, and no change in vulnerabilities concerning resource control [6]. Figure 1 illustrates this trend analysis.

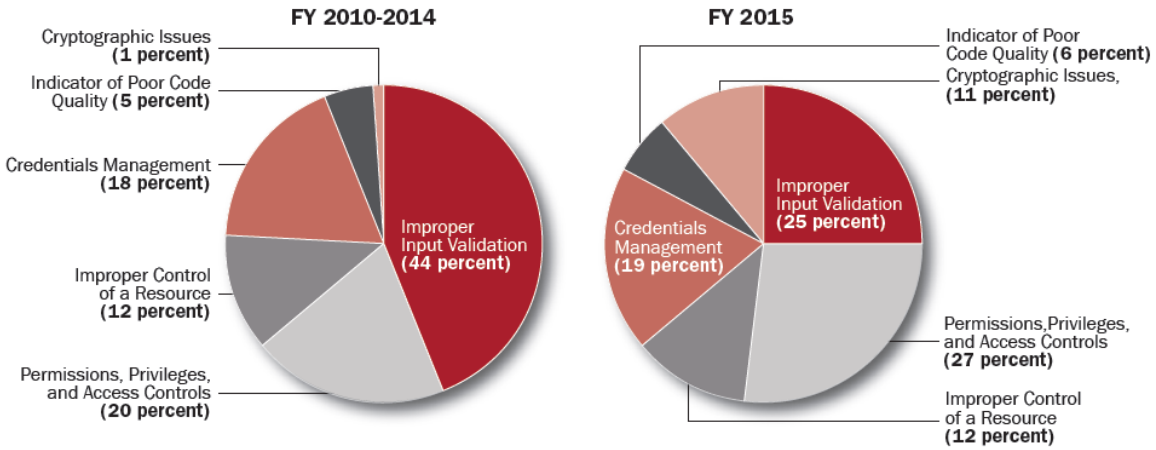

Figure 1. ICS vulnerabilities reported to ICS-CERT. Source: [6].

Modern industrial network protocols have evolved from serial-based fieldbus protocols to Ethernet-based protocols that operate at the application layer of the TCP/IP networking model [7, 8]. The Common Industrial Protocol (CIP) [9] and Ethernet/Industrial Protocol (EtherNet/IP) [10] are two well-known Ethernet-based industrial network protocols. They are managed by the Open DeviceNet Vendors Association (ODVA) and are used by a large number of industrial automation vendors. The Rockwell Automation/Allen-Bradley (RA/AB) ControlLogix programmable logic controllers (PLCs) implement these protocols, and a number of EtherNet/IP and CIP vulnerabilities in the ControlLogix PLCs have been identified since 2012 [11, 12].

Network security monitoring is an important element in incident response and forensics investigation for both Information Technology (IT) and Operational Technology (OT) systems. Passive monitoring does not disrupt time-critical control processes and thus is well suited for use in an OT environment. Similar to analyzing conventional network traffic data in IT systems, interpreting the flow of industrial network traffic requires knowing the difference between the expected and observed

behavior of the OT systems. Most forensic investigators are trained to recognize abusive network behavior in IT systems. However, industrial network protocols such as EtherNet/IP and CIP differ significantly from the traditional network protocols, and these investigators may not have the technical skills to detect anomalous industrial traffic patterns.

B. CONTRIBUTION

The protocols used in each ICS application domain are driven by application-specific need such as connectivity, reliability, safety, and more recently security. As PLCs communicate with field devices and human operators (via human-machine interface (HMI) systems), their network traffic contains information that can provide important clues about the characteristics of an attack.

This report describes the initial development of four hands-on lessons on forensics analysis of industrial network traffic. These lessons can be used as a standalone ICS module in a traditional network forensics course, or be assimilated to create more advanced lessons in an ICS forensics course. Our work focuses on the EtherNet/IP protocols and ControlLogix PLC since, according to a user survey conducted by the ARC Advisory Group [13], Rockwell Automation has a large market share in North America. Our contribution also includes the establishment of an EtherNet/IP network data corpus that we plan to make available to other researchers.

The remainder of this report is organized as follows. Chapter II reviews prior work and Chapter III provides basic information on industrial network protocols. Chapter IV discusses our experimental laboratory and data collection process, while Chapter V details the attack scenarios and the associated forensics lessons. We conclude in Chapter VI.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RELATED WORK

In many Computer Science curricula, computer communications and network security are core courses that teach students the concepts and technology of the Internet protocol suite, and how to secure those protocols. Several works confirm the need for a security curriculum with an emphasis on control systems security [14, 15, 16]. Other prior efforts on ICS security education include the design and development of teaching laboratories [17, 18, 19] and teaching modules [20, 21, 22].

The SEED project has developed a suite of hands-on laboratory exercises that can be used in computer and information security courses [23]. These labs are grouped into six categories: software security, network security, web security, system security, mobile device security, and cryptography. To date, there is no SEED lab that focuses ICS security [24]. Our research aims to fill this gap.

There are different application domains in the ICS landscape, e.g., process automation, power generation and distribution, and supervisory control and data acquisition (SCADA). A generalized view of a SCADA system consists of a supervisory center in which human operators uses human-machine interface (HMI) software to control automated tasks performed by the field devices, and a control network in which intelligent controllers (e.g., PLCs and Remote Terminal Units (RTU)) manipulate the mechanical functions of the field devices as directed by the operators. McGrew and Vaughn describe several software vulnerabilities associated with a commercial HMI product such as password recovery, insecure network authentication, and user authentication bypass [25]. On the control side, Grandgenett *et al*. discuss several attacks that exploit EtherNet/IP and CIP vulnerabilities in a ControlLogix PLC [26, 27]. They describe two EtherNet/IP denial-of-service attacks, one TCP connection hoarding attack, and two CIP attacks that allow an attacker to bypass the PLC authentication mechanism and to remotely send privileged commands to the PLC.

Barbosa proposes an anomaly detection mechanism for SCADA systems that is based on the periodic request-response patterns in industrial network traffic [28]. Their research utilizes network packet traces collected at various water treatment and energy

(gas and electricity) facilities to formulate the differences between industrial network protocols (e.g., Modbus) and traditional network protocols.

The CRISALIS project has developed the FERRET forensics investigation platform for the acquisition and analysis of forensic data of industrial control systems [29]. This platform consists of collection agents deployed on selected supervisory hosts, a processing backend component, and a web-based analysis frontend component. While FERRET was used to investigate security incidents in an actual wind power installation, it lacks the ability to collect and analyze industrial network traffic.

Folkerth discusses the need for including field devices in a forensics program and presents techniques for detecting and analyzing ICS compromises using captured network data [30]. This work shows that analyzing packet trace files can help identify reconnaissance activities and targeted PLC exploitations. Folkerth's approach is most closely related to ours.

NETRESEC maintains a repository of publicly available ICS packet trace files that were captured during various ICS attack challenges [31]. The PLCs used in DigitalBond S4x15 capture-the-flag competitions were Schneider Electric Modicon, Allen Bradley MicroLogix, Advantech ADAM, and Wago PLC [32]. The PLCs used in the ICS Geek Lounge lab at the 2015 4SICS ICS summit were DirectLogic 205, Siemens S7-1200, and xLogic x-Messenger [33]. In contrast, we use ControlLogix PLCs to generate our data corpus of network traffic.

Last, Morris and Gao describe four datasets of industrial network traffic that were created from various attacks against two simulated SCADA systems [34]. This work closely relates to our research except that it focuses on the MODBUS protocol while our work concentrates on the EtherNet/IP protocol.

III. BACKGROUND

This chapter provides basic information on the industrial network protocols and functional model for an industrial automation and control system (IACS) used in our research.

A. REFERENCE FUNCTIONAL MODEL

For this work, we adopt the functional hierarchy model of ANSI/ISA-99.00.01-2007, which was jointly developed by the American National Standards Institute and the ISA99 Committee for Industrial Automation and Control Systems Security of the International Society of Automation [35]. The ISA99 model partitions the architecture of an IACS into five layers as shown in Figure 2.

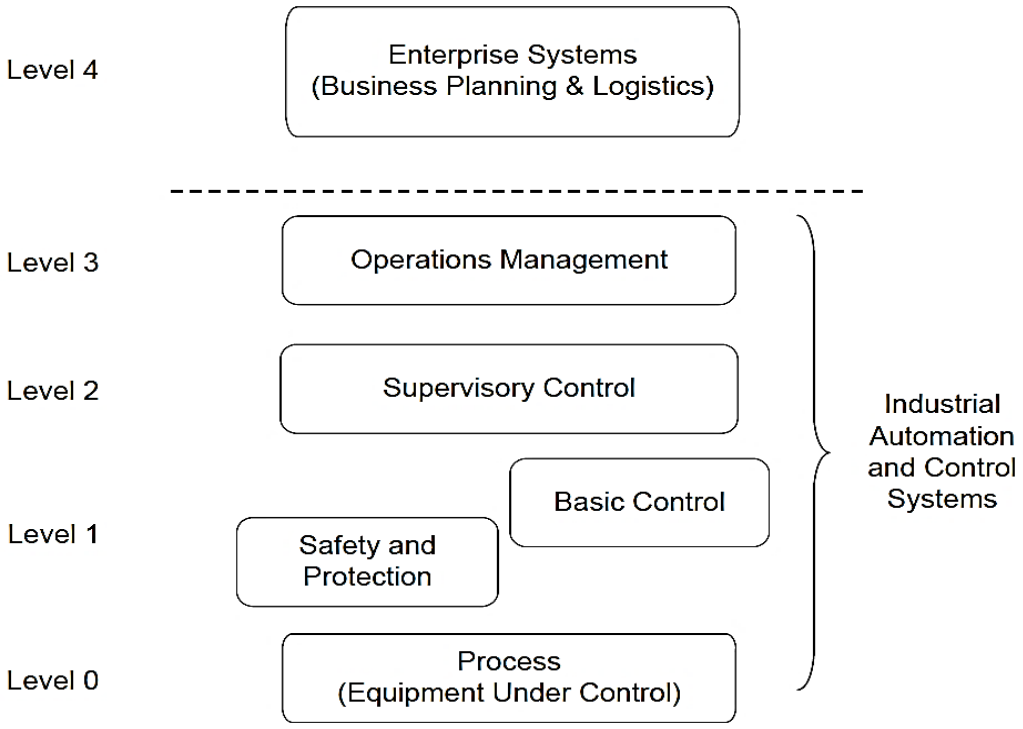

Figure 2. ISA99 Reference Model. Source: [35]

The enterprise systems in the Level 4 layer consist of corporate systems and applications that manage the organization's industrial environment. The operations

management systems in the Level 3 layer are responsible for managing the work-flow of an IACS. Monitoring and controlling the physical process are the primary functions of the supervisory control systems in the Level 2 layer. This layer is where supervisory systems such as the HMI and process historian systems exist. The systems in the Level 1 layer perform continuous sensing and manipulation of the physical devices. They include safety controllers and processing controllers such as PLCs and RTUs. The systems in the Layer 0 layer are the field devices such as sensors, actuators, and physical equipment.

Our work focuses on the Level 1 layer and the communications channels between the Level 1 and Level 2 layers; the components used in these areas are complex and historically designed for real-time functionality, not security.

B. COMMON INDUSTRIAL PROTOCOL

The Common Industrial Protocol (CIP) models each node in the network as a set of objects (Figure 3). The following definitions are taken from the CIP specification [9]. An object provides "an abstraction of a component within a product." A class is a set of objects that "are identical in form and behavior, but may contain different attribute values." An object instance is "the actual representation of a particular object within a class." An instance of a class shares "the same set of attributes, but has its own particular set of attribute values." An attribute describes "an externally visible characteristic or feature" of an object.

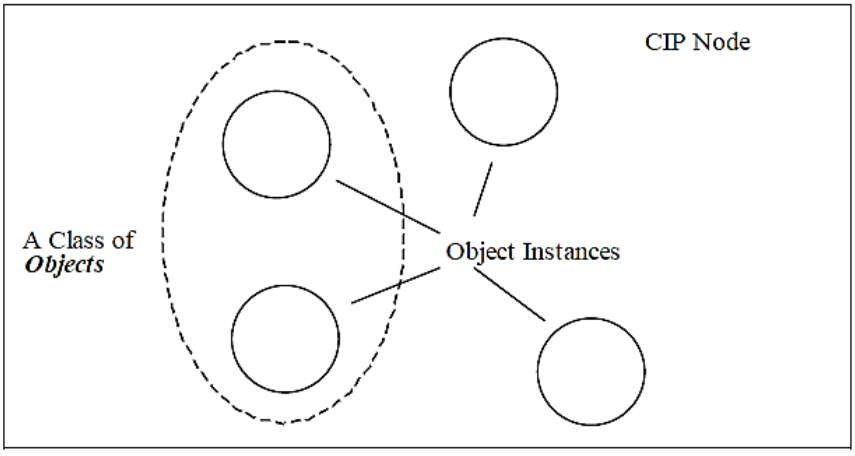

Figure 3. A CIP node with multiple object instances. Source: [9].

Each object or class supports a set of common services (defined in Appendix A of [9]), and in certain products, a number of vendor-specific services. For example, the Identity object "provides identification of and general information about the device," and the Status attribute (attribute ID=5) of the Identity Object provides the "current status of the entire device" [9].

C. ETHERNET/INDUSTRIAL PROTOCOL

The Ethernet/Industrial Protocol (EtherNet/IP), also known as "CIP over Ethernet", uses standard Ethernet and TCP/IP protocols to transport CIP messages [ENIP]. EtherNet/IP supports two types of communications: UDP-based implicit messaging for time-critical operations and TCP-based explicit messaging for operations that are not time-sensitive. An implicit message can be multicast or unicast, and requires a CIP connection to be established between the two devices; an explicit message does not require a CIP connection. EtherNet/IP uses the same port number (44818 or 0xAF12) for both UDP and TCP connections.

The EtherNet/IP encapsulation message inside a TCP/UDP packet consists of a 24-byte header and a command-specific data portion (Figure 4) [10].

Structure	Field Name	Data Type	Field Value
Encapsulation header	Command	UINT	Encapsulation command
	Length	UINT	Length, in bytes, of the data portion of the message, i.e., the number of bytes following the header
	Session handle	UDINT	Session identification (application dependent)
	Status	UDINT	Status code
	Sender Context	ARRAY of octet	Information pertinent only to the sender of an encapsulation command. Length of 8.
	Options	UDINT	Options flags
Command specific data	Encapsulated data	ARRAY of 0 to 65511 octet	The encapsulation data portion of the message is required only for certain commands

Figure 4. EtherNet/IP packet format. Source: [10].

There are both pre-defined commands and vendor-specific commands, and the same packet format is used for both requests and replies.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. APPROACH

In this chapter, we describe the threat model we used to formulate the attack scenarios, our ICS experimental laboratory, and our data collection process.

A. THREAT MODEL

A 2016 congressional report by the Government Accountability Office states that the most serious and most often attacks come from nation states, and the most serious threat source is the malicious insider [36]. The report is based on information collected from eighteen government agencies having high-impact systems, including the Nuclear Regulatory Commission. While the report is not ICS-specific, the summaries contained therein provide insight into cyber threats encountered by operational systems.

Any given weakness in a constituent element of a control system (redundancy mechanisms, monitoring and logging services, etc.) can adversely impact its security posture. NIST SP 800-82 discusses a number of common attacks such as reprograming PLC firmware, sending false status to the operator, modifying the functionality of safety mechanisms, manipulating configuration settings, and denying control actions [37].

For this work, we formulate the attack scenarios described in Table 1.

Table 1. Attack scenarios

Type	Attack Scenarios
Reconnaissance	Probing functionalities implemented in the target PLC
Data exfiltration	Exploiting vulnerable services to obtain high-value data
Malicious insider	Performing unauthorized operations that affect the target PLC's execution state
Denial-of-service	Exploiting a protocol-specific vulnerability in the target PLC's EtherNet/IP implementation

These attack scenarios assume the existence of a rogue machine on the control network and a malicious insider with unfettered access to the target PLC.

B. EXPERIMENTAL LABORATORY

A high-level view of our experimental control system is depicted in Figure 5.

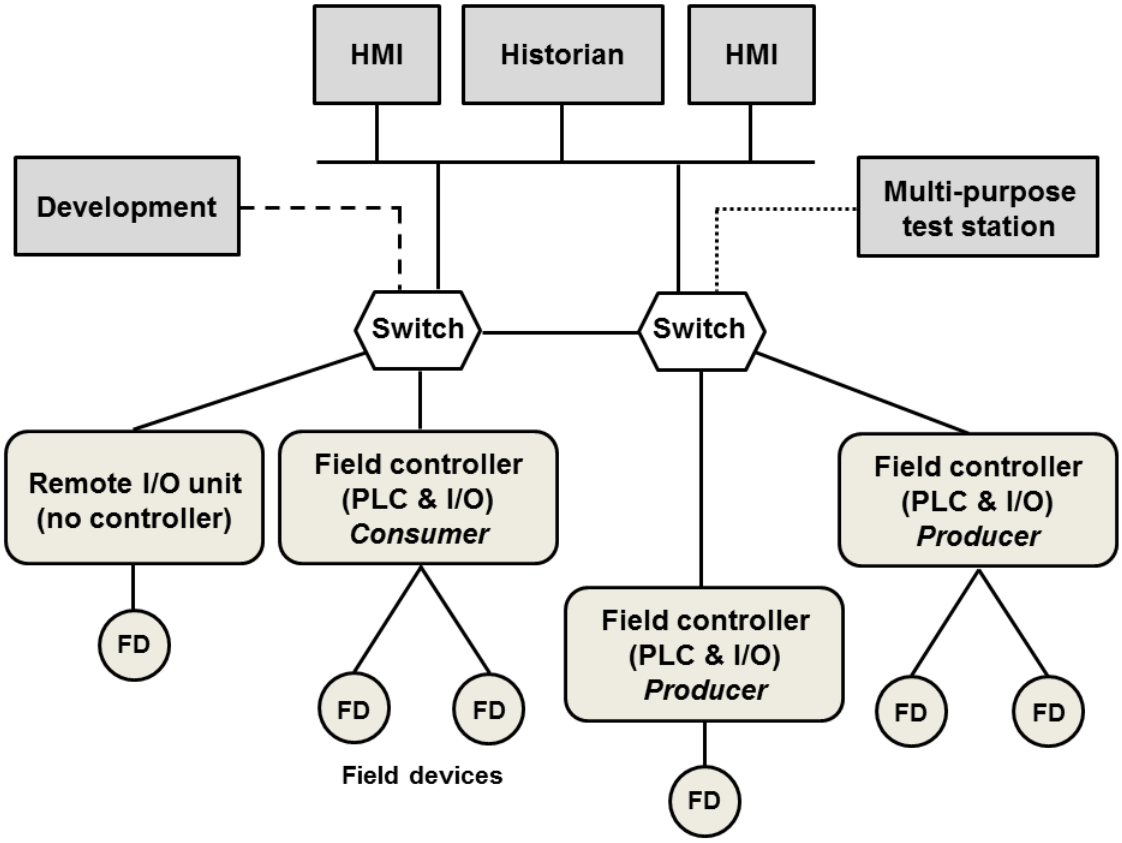

Figure 5. ICS experimental laboratory.

The supervisory segment consists of two HMI systems, a Historian system, a multi-purpose Linux test workstation, and a development system. The workstation can be configured to assume different functional roles such as a maintenance system or a rogue machine. In the control segment, there are three modular PLC racks and one remote I/O unit; each connects to one or more field devices. The PLCs implement the producer-consumer communications model to share data among themselves. Two industrial network switches facilitate communications between the supervisory and control networks; these switches support both standard Ethernet and EtherNet/IP. Standard Ethernet is used by the supervisory systems to communicate with each other while

EtherNet/IP is used by the supervisory systems communicate with the PLCs, and by the PLCs to communicate with each other.

In this work, only a subset of the equipment is used to develop the forensics lessons. This lab environment consists of a Windows HMI system, a Hirschmann industrial switch, the test workstation configured as a rogue system to launch attacks on the PLC, and a PLC rack, and a network monitor (Figure 6).

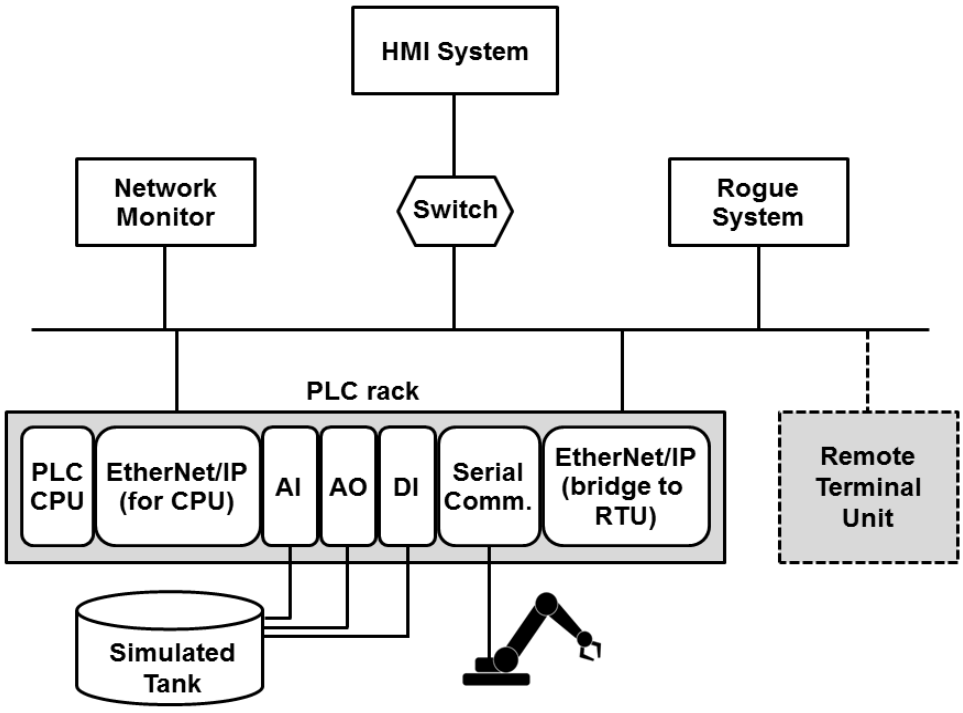

Figure 6. Lesson development laboratory.

The PLC rack is an RA/AB 1756 ControlLogix system [38] that consists of a controller (CPU) module and multiple I/O modules—an EtherNet/IP communication module used to communicate with the HMI system, an analog input (AI) module, an analog output (AO) module, a digital input (DI) module, a serial communication module, and a second EtherNet/IP module used to communicate with the RTU. These I/O modules communicate with the controller module via a proprietary backplane. For the forensics lessons, the controller runs a ladder logic application that controls two field devices: a simulated fluid tank system (commonly found on ships) and a robotic arm—a stand-in for any serial-connected, motorized apparatus, e.g., a rudder system.

The HMI system runs the RA Studio 5000 Logix Designer software [39], which is used to develop and run ladder logic applications on the controller. The HMI system regularly asks the controller for I/O statuses and the controller's current operating mode.

C. DATA COLLECTION

In this work, we use the network packet analyzer Wireshark[1] to capture and analyze network traffic between the HMI systems and the PLCs, and between the PLCs themselves. Wireshark supports a larger number of protocol display filters, including one filter for EtherNet/IP and several filters for different CIP objects.

We construct a data corpus that contains four datasets of network trace files captured by Wireshark (Table 2). The organization of the datasets is based on specific operations from the observed PLC(s).

Table 2. Summary of data corpus.

ID	Description
Dataset A	Single PLC with local I/O operations
Dataset B	Single PLC with remote I/O operations
Dataset C	Multiple PLCs with producer-consumer operations
Dataset D	Single PLC with malicious operations

Dataset A contains EtherNet/IP packets used to control the simulated fluid tank system and the robotic arm, including the use of a simulated HMI override mechanism that allows a local operator to control the equipment in case of an emergency. The data captured in Dataset B represent the communications between a master PLC and a slave remote I/O unit to control a remote field device—a simulated steering system. Three PLCs are used to generate the producer-consumer traffic for Dataset C; one PLC functions as the producer and the other PLCs act as consumers (see Figure 5). In this data exchange model, the producer PLC broadcasts a shared tag (variable) and multiple

[1] Wireshark website: https://www.wireshark.org/
[2] SCADA StrangeLove SCADAPASS, https://github.com/scadastrangelove/SCADAPASS

consumer PLCs can simultaneously receive the same tag without additional programming logic.

Dataset D consists of six packet trace files that are used to develop the forensics lessons. The lessons and packet statistics associated with the capture file used in each lesson are shown in Table 3.

Table 3. Summary of packet trace files in dataset D.

ID	Forensics Lesson	Total Packets	EtherNet/IP Packets
Capture I	Reconnaissance—PLC information	14232	390 (2.7%)
Capture II	Reconnaissance—TCP/IP services	1829	312 (17.1%)
Capture III	Data exfiltration	1177	294 (25.0%)
Capture IV	Malicious insider—normal activity	90	50 (55.6%)
Capture V	Malicious insider—abnormal activity	848	490 (57.8%)
Capture VI	Denial-of-service	202006	42660 (21.1%)

The next chapter describes the attack scenarios and network forensics lessons in more details.

THIS PAGE INTENTIONALLY LEFT BLANK

V. LESSON DEVELOPMENT

This chapter describes the attack scenarios and the hands-on lessons that we develop to address various aspects of ICS incident assessment.

A. ATTACK SCENARIOS

The attack scenarios range from well-known vulnerabilities such as password recovery to malicious insider incidents and denial-of-service attacks (see Table 1). The malicious insider attack is against the ControlLogix CPU module whereas the other three attacks are against the ControlLogix Ethernet/IP module.

1. Reconnaissance Attack

Reconnaissance activity is often difficult to detect if it was done using the same tools and processes prescribed for regular system maintenance, e.g., reviewing component configuration and status via a web browsing interface. In this scenario, the attack is against the integrated web server; it allows remote systems to monitor and manipulate controller data. When contacted, the web server returns a home page that includes a list of available operations, some of which require user login with appropriate access permissions. However, the web server's password authentication mechanism is susceptible to a man-in-the-middle attack [12], and it is common knowledge that ICS operators tend to use vendor default or easy-to-remember passwords for ease of maintenance. The ControlLogix EtherNet/IP module's default password is included in SCADAPASS—a list of default passwords of ICS products maintained by the SCADA StrangeLove research group[2].

Unprotected operations that do not require login can be exploited to obtain information about the web server, and the configuration of the PLC rack, including the model number and firmware version of each module in the rack, and the running status of each PLC module. This information allows an attacker to construct malware targeting the specific web server and PLC modules.

[2] SCADA StrangeLove SCADAPASS, https://github.com/scadastrangelove/SCADAPASS

In this scenario, we assume that the attacker successfully guesses a password and can access protected web pages to discover other vulnerable embedded services. While the vendor recommends keeping these services disabled when not in use, they are customarily left to run once they are enabled.

2. Data Exfiltration Attack

In addition to web access, the ControlLogix EtherNet/IP module provides other TCP/IP services, including file transfer (via the File Transfer Protocol (FTP)), email (via the Simple Mail Transfer Protocol), and network management (via the Simple Network Management Protocol). This attack scenario focuses on the FTP server since, while inherently insecure, FTP is generally used in ICS. Similar to other FTP servers, the ControlLogix FTP server also transmits the password in plain text.

The FTP server allows access to the file system on the EtherNet/IP module whose directory structure is divided into two categories: normal-access and special-access. Module configuration files and data view files[3] are special-access files; they can only be accessed when the module is in backup/restore mode. Normal-access files can always be accessed, and include Electronic Data Sheet (EDS) files, predefined web pages, custom web pages, and user-defined files.

An EDS file is a text file provided by the device vendor that contains device-specific configuration data [9]. An EDS file for a ControlLogix module contains the module's firmware version, device characteristics, and TCP/IP capability (e.g., the total number of TCP/IP connections the module can sustain without performance impact, TCP/IP inactivity timeout, and CIP inactivity timeout). For a ControlLogix module, multiple EDS files can be found in the file system if the module went through multiple firmware updates. An attacker can use FTP to retrieve the EDS files and use the information contained in those files to craft a targeted malware.

3. Malicious Insider Attack

The ControlLogix CPU module has a mechanical mode switch on the front of the module that sets the operating mode of the controller. The location of this switch affords an adversary a quick and non-intrusive mechanism to alter the operating behavior of the

[3] A data view file contains information about a set of tags (variable in PLC memory).

controller, which can greatly affect the industrial control process. The CPU module can be in one of five operating modes [40]. In the Run mode, the controller continuously monitors and controls the I/O modules, and process control applications cannot be modified. In the Program mode, the controller stops executing application code and does not control the I/O modules. While in this mode, applications can be modified or loaded from the controller's user memory. The Remote Run mode is identical to the Run mode except that applications can be modified remotely. Similarly, the Remote Program mode is identical to the Program mode except its operations can be invoked remotely. In the Remote Test mode, the controller continues executing the loaded application code, stops controlling the I/O modules, and provides limited editing capability.

In this attack scenario, an insider gains physical access to the PLC rack and uses the mode switch to manipulate the controller's operating mode.

4. Denial-of-Service Attack

This attack utilizes the RegisterSession command to cause a resource exhaustion condition on the ControlLogix Ethernet/IP module. The RegisterSession command must be executed to establish an EtherNet/IP session prior to any CIP communications between two devices. The session handle returned in a RegisterSession reply is used in all subsequent EtherNet/IP messages until the session is terminated, either via the UnRegisterSession command or when the TCP connection is closed. The session handle is a 32-bit unique value generated by the target device, and its assignment is application-dependent. The session handles captured in the Capture VI (see Table 3) indicate that the ControlLogix EtherNet/IP module increments the session handle value by one hundred hexadecimal.

Using a Python program that repeatedly sends the RegisterSession command without terminating any existing sessions, we observe that the EthereNet/IP module eventually stops responding to the RequestSession command after 17000 (approx.) requests. The CIP messages between the HMI system and the PLC also cease afterward. The line graphs in Figure 7 illustrate the observed behavior.

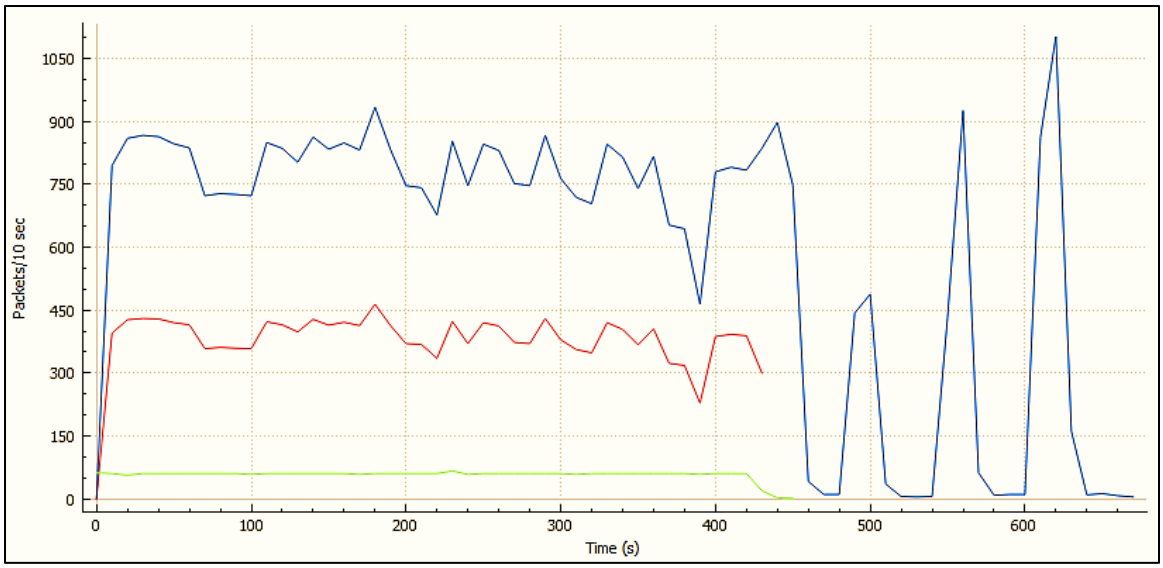

Figure 7. Resource exhaustion using RequestSession command.

The blue graph shows all TCP/IP traffic captured in the packet trace. The red graph depicts successful RequestSession commands, i.e., the EtherNet/IP module returned non-zero session handles. The green graph indicates CIP traffic between the HMI system and the PLC. This attack leverages the EtherNet/IP exploit described by Grandgenett *et al.* [26].

B. LESSON DESCRIPTION

Analysis of packet captures from a network monitor in an ICS is an important step towards understanding what has transpired on the control network. Captured network data between an HMI and a PLC can provide a record of commands to field devices, malware payloads, and exfiltration of field data during a breach. The objective of the lessons is to introduce students to common vulnerabilities in an industrial network and a commercial EtherNet/IP implementation, and to demonstrate the importance of industrial network data analysis in forensics investigations.

The lessons require students to have working knowledge of common TCP/IP application protocols such as HTTP and FTP, familiarity with basic ICS terminology and concepts, and have hands-on experience with packet analysis using Wireshark. The instructor is expected to deliver the following units at the beginning of the lessons:

- A review of HTTP and FTP protocols, and HTML document format. The review only needs to cover the basic structure of HTTP authentication and the GET method, basic FTP commands, and basic structure of a webpage and HTML elements.
- A review of ICS fundamentals.
- An explanation of the EtherNet/IP session management.
- An explanation of the CIP Identity object and two common services—Get Attribute List (GAL) and Multiple Service Packet (MSP).

The lessons are in the form of hands-on exercises, in which students use Wireshark to analyze one or more packet capture (PCAP) files in dataset D and answer a series of questions in a written report to demonstrate their comprehension of the assigned tasks. The students must provide evidence from the PCAP files that supports their answers. A naïve way to ensure that each student performs his or her own work is to change the timestamp values in the original PCAP files to make a unique PCAP file for each student. This parameterization can easily be done via a script that uses Wireshark's `editcap` utility[4] to make the time adjustment.

There are four lessons; each corresponds to an attack scenario described earlier. The following sections describe the objectives and learning outcomes, which are assessed through written reports.

1. Lesson 1: Reconnaissance

This lesson demonstrates how a rogue machine on the network can discover information about the PLC configuration and its embedded services from browsing the web server running on the ControlLogix EtherNet/IP module. This lesson consists of two exercises. In the first exercise, students examine the Capture I packet trace to reconstruct the browsing activities used by the attacker to learn about the different modules installed in a PLC rack. Vendor documentation (available on the Internet) indicates that the ControlLogix EtherNetIP modules support several TCP/IP application services. In the second exercise, students inspect the Capture II packet trace to determine how the attacker uncovers which services are enabled.

[4] editcap manual page: https://www.wireshark.org/docs/man-pages/editcap.html

Upon successfully completing this lesson, the students will be able to:

- Describe the actions performed by the attacker;
- Describe the types of information returned from the web queries;
- Identify the available TCP/IP services.

2. Lesson 2: Data Exfiltration

After finding out which application services are enabled on a controller, the next step for the attacker is to exploit those services to obtain high-value control data. The objective of this lesson is to show how such data can be extracted if a vulnerable service such as FTP is left running on the PLC. This lesson uses the Capture III packet trace.

At the end of this lesson, the students will be able to:

- Identify the type of embedded FTP server used in the ControlLogix EtherNet/IP module based on useful information such as the name, the version number, and the operating system on which the software is designed to run;
- Describe the commands issued to and data returned from the FTP server;
- Describe the contents of the retrieved data which include EDS files of the EtherNet/IP module;
- Discuss a hypothetical attack scenario based on their understanding of the EDS data.

3. Lesson 3: Controller Manipulation

This lesson addresses the malicious insider threat described in Section 5.A.3 above. The main task is to analyze CIP messages in two packet traces (Capture IV and Capture V) to determine the actions taken by the insider.

This lesson requires a basic understanding of how the Identity object is used in the Get Attribute List (GAL) and Multiple Service Packet (MSP) services. The GAL service returns the value(s) of the requested object attribute(s) or class attribute(s); the MSP service allows a CIP client (e.g., the HMI system) to request a CIP server (e.g., the controller) to perform a number of services in a single CIP message. In this lesson, the HMI system uses the MSP service with multiple embedded GAL requests to obtain device and I/O information from different modules in the PLC rack. One of those GAL

requests returns the current status of the CPU module via the Status attribute of the Identity object.

After completing this lesson, the students will be able to:

- Interpret EtherNet//IP packets to determine the number of active EtherNet/IP sessions between the HMI system and the PLC;
- Describe the CIP traffic between the HMI system and the PLC;
- Describe how the CPU module uses the CIP Identity object to report its operating mode at a given time;
- Compare and contrast normal traffic and abnormal traffic to detect unauthorized operating mode changes.

4. Lesson 4: Resource Exhaustion

The narrative for this lesson is as follows: The HMI system reports that EtherNet/IP communications with the PLC has been lost, but there is no error indication on the controller module or the EtherNet/IP module, i.e., the status LEDs on the front panel of those modules still indicate that the modules are running normally. The HMI system can still "ping" the EtherNet/IP module, however subsequent requests to establish EtherNet/IP sessions continue to fail. This problem persists until the PLC system is reset.

Whereas Lesson 3 focuses on the CIP services, this lesson concentrates on the RegisterSession EtherNet/IP command (see Section 5.A.4). The objective is to show how a deficiency in a protocol implementation could be used to silently bring down a PLC.

The students will be able to:

- Describe the mechanism (i.e., repeatedly asking for new EtherNet/IP sessions without terminating existing sessions) and resource (i.e., the pool of session handles) used by the attacker to cause the observed denial-of-service condition.
- Build a time line of events leading to the observed malfunction.
- Describe the algorithm used by the ControlLogix EtherNet/IP implementation to allocate session handles.

In summary, the skills that the students gain from the four lessons are essential for meeting the goal of exposing students to network forensics in industrial control systems, including technical proficiency in assessing and reconstructing security incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This report describes the initial results of our effort to develop hands-on lessons that expose students to network forensics in an industrial network. The lessons demonstrate that by critically analyzing the network traffic between the supervisory systems and the control systems, a forensics investigator can identify malicious activities injected into a control network, ranging from seemingly innocuous reconnaissance operations to the massive consumption of a critical resource that can silence a PLC.

The lessons have been laboratory-tested and will be used in a new computer science course that considers threats and vulnerabilities in operational technologies employed in critical infrastructure. The lessons and our EtherNet/IP network data corpus will be publicly disseminated after they are "field-tested" by students.

As our investigation on vulnerabilities in industrial protocol implementations continues, we plan to develop additional lessons to facilitate transfer of our findings into classroom activities.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Department of Homeland Security, "Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), February 25, 2016.

[2] SANS Institute and Electricity Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," March 2016.

[3] Symantec Corporation, "Destructive Disakil malware linked to Ukraine power outages also used against media organizations," Symantec Security Response blog. http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations

[4] Department of Homeland Security, "Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), March 02, 2016 (Original release date: December 10, 2014).

[5] FireEye Inc., "IRONGATE ICS Malware: Nothing to See Here...Mask Malicious Activity on SCADA Systems," FireEye Threat Research blog. https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

[6] Department of Homeland Security (U.S.), "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report," National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, September 2016.

[7] Sauter, J., "The Three Generations of Field-Level Networks--Evolution and Compatibility Issues," IEEE Transactions on Industrial Eletronics, vol. 57, no. 11, pp. 3585–3595, November 2010.

[8] Galloway B. and Hancke, G. "Introduction to Industrial Control Networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 2. pp. 860-880, Second Quarter 2013.

[9] ODVA & ControlNet International Ltd, "The CIP Networks Library Volume 1, Common Industrial Protocol (CIP)," Edition 3.3, November, 2007. http://www.tud.ttu.ee/im/Kristjan.Sillmann/ISP0051%20Rakenduslik%20Andmeside/CIP%20docs/CIP%20Vol1_3.3.pdf

[10] ODVA & ControlNet International Ltd, "The CIP Networks Library Volume 2, EtherNet/IP Adaptation of CIP," Edition 1.4, November 2007. http://www.tud.ttu.ee/im/Kristjan.Sillmann/ISP0051%20Rakenduslik%20Andmeside/CIP%20docs/CIP%20Vol2_1.4.pdf

[11] Santamarta, R., "Attacking ControlLogix,", Digital Bond Project Basecamp, 2012.

[12] Department of Homeland Security, "Advisory (ICSA-13-011-03) Rockwell Automation ControlLogix PLC Vulnerabilities," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), February 17, 2014.

[13] ARC Advisory Group, "ARC User Survey: PLC Supplier Preferences," November 2001.

http://www.arcweb.com/arcreports2001/ARC%20User%20Survey%20PLC%20Supplier%20Preferences.pdf

[14] Department of Homeland Security (U.S.), "Critical Infrastructure and Control Systems Security Curriculum Version 1.0," March 2008.

[15] Foo, E., Branagan, M., Morris, T., "A Proposed Australian Industrial Control System Security Curriculum," Proceedings of the 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 1754–1762. IEEE (2013).

[16] Francia III, G.A., "Critical Infrastructure Security Curriculum Modules," Proceedings of the 2011 Information Security Curriculum Development Conference(InfoSecCD 2011), pp. 54–58, Sept 2011.

[17] Francia III, G.A., Beckhouche, N., Marbut, T., and Neuman, C., "Portable SCADA Security Toolkits," International Journal of Information & Network Security (IJINS), vol.1 no. 4, pp. 265-274, October 2012.

[18] Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., Reddi, R., "A Control System Testbed to Validate Critical Infrastructure Protection Concepts," International Journal of Critical Infrastructure Protection, vol. 4 no. 2, pp. 88–103, August 2011.

[19] Vaughn, R.B., Morris, T., Sitnikova, E., "Development & Expansion of an Industrial Control System Security Laboratory and an International Research Collaboration," Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW '13). ACM , January 2013.

[20] Foreman, J. C., Graham, J. H., Hieb, J. L., Ragade, R. K., "A Curriculum Model for Industrial Control systems Cyber-security with Sample Modules," Technical Report 2012–14, Center for Education and Research, Purdue University (2012).

[21] Francia III, G. A., Snellen III, J., "Embedded and Control Systems Security Projects," Information Security Education Journal, vol.1 no. 2, pp. 77–84, December 2014.

[22] Luallen, M.E., Labruyere, J.-P., "Developing a Critical Infrastructure and Control Systems Cybersecurity Curriculum," Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS), pp. 1782–1791. IEEE, January 2013.

[23] W. Du, K. Jayaraman, and N. B. Gaubatz, "Enhancing security education with hands-on laboratory exercises," Proceedings of the 5th Annual Symposium on Information Assurance (ASIA'10), pp. 56-61, June 2010.

[24] Syracuse University, "Hands-on Labs for Security Education," Project website. http://www.cis.syr.edu/~wedu/seed/index.html

[25] McGrew, R. W., Vaughn, R. B., "Discovering Vulnerabilities in Control System Human-Machine Interface Software," Journal of Systems and Software, vol. 82 no. 4, pp. 583-589, Janurary 2009.

[26] Grandgenett, R., Gandhi, R., and Mahoney, W., "Exploitation of Allen Bradley's Implementation of EtherNet/IP for Denial of Service Against Industrial Control Systems", 9th International Conference on Cyber Warfare and Security, Purdue University, March 2014.

[27] Grandgenett, R., Mahoney, W., and Gandhi, R., "Authentication Bypass and Remote Escalated I/O Command Attacks," Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR '15), April 2015.

[28] Barbosa, R. R. R., "Anomaly Detection in SCADA Systems A Network Based Approach," University of Twente, CTIT Ph.D. thesis series ; no. 14-300, April 2014.

[29] Patzlaff, H., "D7.3 Report on forensic analysis for industrial systems," European Community's Seventh Framework Programme.

[30] Folkerth, L., "Forensic Analysis of Industrial Control Systems," SANS Institute InfoSec Reading Room, September 24, 2015.

[31] NETRESEC AB, "Publicly available PCAP files." http://www.netresec.com/?page=PcapFiles

[32] Digital Bond, "ICS Village," S4x15 ICS Security Conference, January 2015. http://www.digitalbond.com/s4/s4x15-week/s4x15-ics-village/

[33] NETRESEC AB, "Capture files from 4SICS Geek Lounge," 2015. http://www.netresec.com/?page=PCAP4SICS

[34] Morris, T. and Gao, W., "Industrial Control System Traffic Data Sets for Intrusion Detection Research," in Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference Revised Selected Papers, Butts, J. and Shenoi, S., eds., Springer Berlin Heidelberg, pp. 65-78, 2014.

[35] American National Standards Institute/International Society of Automation, "ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models," American National Standards, ISBN: 978-1-934394-37-33, 29 October 2007.

[36] United States Government Accountability Office, "Report to Congressional Requesters, Agencies Need to Improve Controls over Selected High-Impact Systems," GAO-16-501, May 2016.

[37] National Institute of Standards and Technology, "NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security," Revision 2, May 2015.

[38] Allen-Bradley, "ControlLogix System," User Manual, Rockwell Automation Publication 1756-UM001O-EN-P, October 2014.

[39] Allen-Bradley, "Logix5000 Controllers Ladder Diagram," Programming Manual, Rockwell Automation Publication 1756- PM008F-EN-P, June 2016.

[40] Allen-Bradley, "ControlLogix System," User Manual, Rockwell Automation Publication 1756-UM001O-EN-P, October 2014.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943