INDUSTRIAL CONTROL SYSTEM SECURITY

FORENSIC ANALYSIS OF INDUSTRIAL NETWORK DATA

PLC-FORENSICS

Lab Description: Analysis of packet captures from a network monitor in an industrial control system (ICS) is an important step towards understanding what has transpired on the control network. Captured network data between a supervisory computer (e.g., a Human-Machine Interface (HMI) system or a Historian system) and a field device such as a programmable logic controller (PLC) can provide a record of commands to field devices, malware payloads, and exfiltration of field data during a breach. In addition to Ethernet-based industrial protocols such as Common Industrial Protocol (CIP) [1] and Ethernet/Industrial Protocol (EtherNet/IP) [2], most PLCs support common TCP/IP application protocols such as HTTP, FTP, SNMP, etc. for system configuration and management purposes. These protocols can be exploited by a rogue machine on the network.

The learning objective of this lab 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.

Lab Environment: The lab environment is provided by the Labtainer framework, which can be installed and run as described in the Labtainer Student Guide, available at: https://my.nps.edu/web/cisr/labtainers. The lab is started by typing

    $ labtainer plc-forensics

at your Labtainer workspace directory. That will display a link to this lab manual, and will create a virtual terminal.

Lab Configuration

The resulting virtual terminal labeled "investigator" is connected to a computer that you will use to access a simulated copy of the vulnerable PLC in a manner similar to that followed by the attacker. But first, you will need to analyze a set of PCAP files to determine what the attacker did.

This lab uses the Wireshark network protocol analyzer tool to examine packet traces in the lab exercises below. The PCAP files are in the home directory of the investigator computer, and they can be viewed in Wireshark, e.g.,

```
wireshark Task1-trace.pcap &
```

ICS Test Environment

The simulated ICS environment used to generate the PCAPs for this lab consists of a Windows HMI system, an industrial network switch, a Linux system used to launch attacks on the PLC, and a modular PLC rack. This ICS environment is illustrated in Figure 1. The network monitor, industrial switch, remote terminal unit (RTU), and physical devices shown in the diagram are informational only.
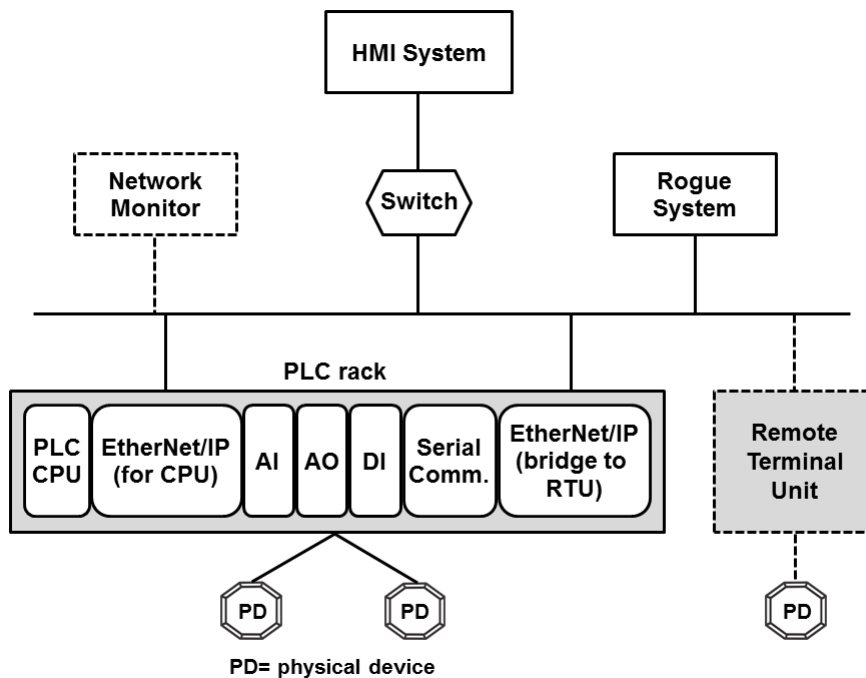
Figure 1. ICS environment used to generate PCAP files

The IP addresses that are relevant to the lab exercises are shown in Table 1.

Table 1. IP address allocation.

Component	IP address
HMI system	10.1.30.1
Rogue system	10.1.40.1
PLC rack (EtherNet/IP for CPU)	10.1.100.2

The PLC rack is a Rockwell Automation/Allen-Bradley (RA/AB) 1756 ControlLogix system [3] 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.

Note for Students

This lab assumes the following:

1. The student has taken TCP/IP networking course(s);
2. The student has working knowledge of HTTP and FTP application protocols, and HTML syntax;
3. The student is familiar with basic ICS terminology and concepts;
4. The student has hands-on experience with Wireshark. Minimally, the student must know how to: filter a particular packet type, obtain protocol-specific statistics, follow a TCP stream, customize display columns, and set up TCP preferences such as turning off TCP streams reassembly feature;
5. The student can independently look up vendor information available on the Internet.

Note for Instructors

We suggest that this lab be conducted in a supervised lab environment, and that the following materials be covered at the beginning of the lab session:

1. Labtainer installation, including installation of Virtual Box and a Linux VM (if a Linux system is not already available). Refer to the Labtainer Student User Guide.
2. Review of HTTP and FTP protocol, and HTML format. Only need to cover the basic structure of HTTP authentication and GET method, basic FTP commands, and basic structure of a webpage and HTML elements.
3. Review of ICS fundamentals.

Summary of Lab Tasks

This lab consists of three tasks. Tasks 1 and 2 cover reconnaissance activities. Task 3 addresses data exfiltration.

The following list provides some useful hints for Wireshark:

1. When working with a particular protocol, set the display filter to only show traffic for that protocol, e.g., set the display filter to only show HTTP traffic when working with web requests.
2. When working with HTTP, enable the HTTP header and body reassembly options. These options are usually enabled by default.
3. Disable the TCP streams reassembly option if packet data span multiple TCP segments. This option is usually enabled by default. See https://wiki.wireshark.org/TCP_Reassembly for more information about the TCP reassembly option.
4. Use the Follow TCP Stream feature to see application-specific data that span multiple packets, e.g., a web page or an FTP operation.

Lab Files that are Needed: The PCAP files needed by this lab are on the investigator computer.

LAB EXERCISE 1: RECONNAISSANCE ACTIVITY

Reconnaissance is the first phase of an attack progression. This 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. The ControlLogix EtherNet/IP modules include an integrated web server that 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 (Figure 4), some of which require login with appropriate access permissions.
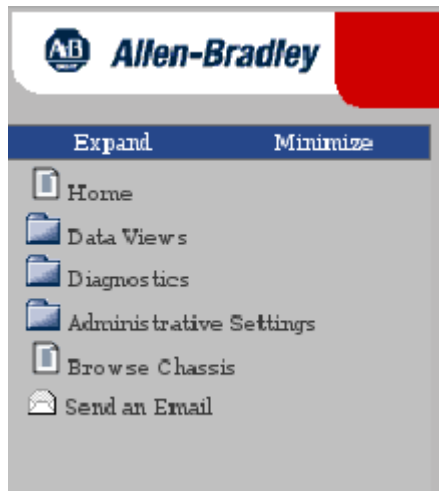

Figure 2. Operations supported by the web server.

The objective of this task is to determine how much information about the PLC rack a rogue machine on the network can discover from browsing the web server. Your task is to use Wireshark to inspect the Task1-trace.pcap file and work through work through the questions below.

Question 1.1: Which browser (user-agent) was used to collect controller data?

Question 1.2: What is the name of the web server?

Question 1.3: How many HTTP requests are contained in the PCAP file?

Question 1.4: Which top-level operation shown in Figure 4 was performed?

Question 1.5: What subsequent actions were performed to get information about the PLC rack after the top-level operation was selected? Describe your method for producing your answer to this question and provide Wireshark output you use for your answer.

Question 1.6: What information about the PLC rack and each module in the rack was obtained from the first chassisWho.asp query? Provide all data that are relevant to the chassis and each module.

Question 1.7: Show how the information obtained from the first chassisWho.asp query corresponds to the PLC rack configuration shown in Figure 1. You can use the following table for your answer:

Question 1.8: For each module, how many subsequent queries were made to obtain additional information about the module? Describe the method you use to find these queries and identify the packet used to send each query.

Question 1.9: What kinds of information were returned from the queries identified in Question 1.7? Describe your method for producing your answer and list the returned information for the following modules: controller, EtherNet/IP module for the controller, and serial communication module.

Question 1.10: Examine the returned data for other modules. What similarities and differences between the data returned for those modules and the data for the three modules covered in Question 1.8 do you observe? You don't need to list specific values.

LAB EXERCISE 2: RECONNAISSANCE ACTIVITY

RA documentation (available on the Internet) indicates that the ControlLogix EtherNetIP modules support several TCP/IP application services. The objective of this task is to determine what information about these services a rogue machine can retrieve from the web server. Your task is to use Wireshark to inspect the Task2-trace.pcap file and work through the questions below.

Question 2.1: Starting at which packet did the rogue machine discover that certain web pages are protected? Describe your method for producing your answer.

Question 2.2: Describe the actions performed by the rogue machine after this discovery? Describe your method for producing your answer and show the result of each action.

Question 2.3: What information did the rogue machine discover? Describe your method for producing your answer and show the returned information.

LAB EXERCISE 3: DATA EXFILTRATION

After finding out which application services are running on a controller, the next step for the attacker is to exploit those services to obtain high-value control data. The objective of this task is to determine what information a rogue machine can retrieve from an integrated application server in a ControlLogix system. Your task is to use Wireshark to inspect the Task3-trace.pcap file and work through the questions below.

Question 3.1: Excluding the two CIP services, how many application services discovered in Task 2 were exploited and what were they? Show evidence from the PCAP file that supports your answer.

Question 3.2: Provide the name, version number, and information about the operating system of an exploited server. Show evidence from the PCAP file that supports your answer.

Question 3.3: Did the exploited service(s) require user authentication? If yes, was the user credential protected during transit? Show evidence from the PCAP file that supports your answer.

Question 3.4: What information did the rogue machine find out about the directory structure of the exploited server(s)? Show evidence from the PCAP file that supports your answer.

Question 3.5: Provide a high level description of the actions performed by the rogue machine to obtain data from the exploited server(s). Show evidence from the PCAP file that supports your answer.

Question 3.6: Describe the information contained in the retrieved data? Show evidence from the PCAP file that supports your answer. See Chapter 7 of the CIP specification [1] for more information on the retrieved data. Note that EtherNet/IP vendor ID for RA/AB is 1, and thus vendor-specific information will have a "1_" prefix.

Question 3.7: Discuss a hypothetical attack scenario based on your understanding of the retrieved data.

Action 3.1: Using information derived from the PCAP, use the "investigator" terminal to access the service as it was accessed by the attacker and retrieve the information that the attacker retrieved.

Action 3.1: Experiment with the credentials you utilized in Action 3.1 to use wget to retrieve the protected web page identified in Lab Exercise 2. The syntax of wget for protected resources is:

```
wget --user <user> --password <password> <URL>
```

WHAT TO SUBMIT

When you have completed the lab, run:

    stoplab plc-forensics

from the Labtainer workspace directory and include the resulting zip file in what you submit to the instructor. You also need to submit a detailed lab report to describe what you have done and what you have observed. Please provide details using screen shots. You also need to provide explanations for the observations that are interesting or surprising.

References

[1]   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

[2]   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

[3]   Allen-Bradley, "ControlLogix System," User Manual, Rockwell Automation Publication 1756-UM001O-EN-P, October 2014. http://literature.rockwellautomation.com/idc/groups/literature/documents/u m/1756-um001_-en-p.pdf

[4]   Allen-Bradley, "Logix5000 Controllers Ladder Diagram," Programming Manual, Rockwell Automation Publication 1756- PM008F-EN-P, June 2016. http://literature.rockwellautomation.com/idc/groups/literature/documents/p m/1756-pm008_-en-p.pdf

[5]   Allen-Bradley, "Troubleshoot EtherNet/IP Networks," Application Technique, Rockwell Automation Publication ENET-AT003B-EN-P, June 2014. http://literature.rockwellautomation.com/idc/groups/literature/documents/at /enet-at003_-en-p.pdf

[6]   Allen-Bradley, "ControlLogix System," User Manual, Rockwell Automation Publication 1756-UM001O-EN-P, October 2014. http://literature.rockwellautomation.com/idc/groups/literature/documents/u m/1756-um001_-en-p.pdf

[7]   Allen-Bradley, "Logix5000 Controllers General Instructions Reference Manual," Reference Manual, Rockwell Automation Publication 1756-RM003Q-EN-P, July 2016. http://literature.rockwellautomation.com/idc/groups/literature/documents/r m/1756-rm003_-en-p.pdf

This lab was developed by the Center for Cybersecurity and Cyber Operations at the Naval Postgraduate School in Monterey California.