The Security Challenges with The Widespread Use of IT Infrastructure in ICS

Kuan-Ming Su
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan

Jung-Shian Li[*]
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan
E-mail: kmsu@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw[*]

Abstract

The communication established by Ethernet is becoming more and more common in the industrial control systems (ICS), and it brings not only pros but also cons like vulnerabilities from information technology. We generalized a procedure of attacking an Ethernet-enabled ICS and implemented it to the real industrial system we obtained. The procedure gets the information and access of the devices in the ICS, like identifying the manufacturer of programmable logic controllers (PLCs) and overwriting the configuration of PLCs.

Keywords: Industrial Control Systems (ICS), Programmable Logic Controller (PLC), Information Technology (IT), Network Security, Ethernet

1. Introduction

In the modern industrial control system (ICS), information technology (IT) is getting more and more widespread in the operation technology (OT) field because of Industry 4.0 [1], and serial communication is becoming incompetent to meet the demands. Therefore, in terms of communication of IT in ICS, Ethernet is coming to the most popular one. Ethernet is commonly used in ICS with IT. Comparing to serial connection, Ethernet has much more flexibility and scalability. For example, to access and manage multiple devices, all you need to do is connecting your engineering workstation (EWS) to the network where devices are. Also, Ethernet allows hundreds of devices to communicate with each other. In addition, there have been many industrial protocols supporting Ethernet and Internet Protocol.

Although Ethernet meets the demands of IT and OT, it also brings vulnerabilities to ICS. Considering the cost of building information security, most ICS defense mechanisms only have an external firewall, isolation from the office network, or complete independence from other networks. Moreover, for the purpose of operation stability, many running operation systems are not updated to the latest version including the security patches. Therefore, those devices are very vulnerable to malware. Let us take TSMC for example. TSMC is the most advanced integrated circuit manufacturer in the world, and they have the top of cyber security standards to protect the intellectual property and factory operation. However, an accident occurred in 2018. Because of the operational errors during the software installation on the new equipment, after the new equipment hooked up to the internal network, the ransomware infected other computer systems and fab tools and caused about $170 million US dollars losses [2].

In order to show how fragile information security inside the ICS network is, we generalized a procedure to attack ICS networks, and we carried it out on a real ICS which was used before. Eventually, we compromised the PLC in the ICS network with MODBUS TCP packets. We successfully read and wrote the registers in the PLC and stopped the running PLC.

2. Background

There are devices controlled in ICS, and there must be some methods for the controller to communicate with each other to make those devices work together. We can divide it into the physical connection part and the communication protocol part. For the physical connection in ICS, there are several standards like RS-232, RS-422, RS-485, and Ethernet. Among those standards, Ethernet is the focus of this discussion due to the trend of IT. For the communication protocols in ICS, there are various protocols based on different standards. Many relatively modern protocol versions are based on Ethernet. Some of them are based on Internet Protocol, such as MODBUS TCP and Ethernet/IP, and some of them are not, such as EtherCAT and PROFINET. For the following discussion, we will focus on MODBUS TCP.

2.1. *Industrial Ethernet*

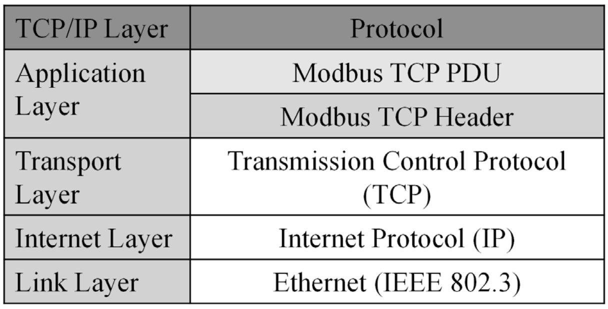
Fig. 1. M12 connector [3]

In addition to Ethernet interfaces on the ICS devices like PLC and HMI, Ethernet switches and cables are also needed to build the network, and there are some differences between common and industrial Ethernet products. Depending on the different environments, the industrial cables may have high-quality foil and braid to protect data transmission from EMI [4], use cable jackets with different materials like FEP and TPE for durability [5], or have M12 and M8 connectors (see Fig. 1) instead of common 8P8C (often miscalled RJ45) in order to be waterproof. Besides the difference of the connectors, the industrial Ethernet switches have other features comparing to common switches. Let us take Cisco industrial Ethernet 4000 series switches (IE-4000) [6] for example. IE-4000 can work in extreme environments and temperature range (-40 to 70 Celsius), has a durable design, support power over Ethernet up to 240W, and so on.

To sum up, the main difference between industrial and common Ethernet products is the durability in different environments and the features in use and management. There is no change to the data transmission standards.

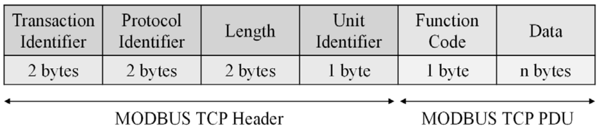
2.2. *MODBUS Messaging on TCP/IP*

MODBUS is a popular communication protocol in industrial environments because it is opened and does not need a license fee. The protocol data unit (PDU) of



TCP/IP Layer	Protocol
Application Layer	Modbus TCP PDU
	Modbus TCP Header
Transport Layer	Transmission Control Protocol (TCP)
Internet Layer	Internet Protocol (IP)
Link Layer	Ethernet (IEEE 802.3)

Fig. 2. MODBUS on TCP/IP



Transaction Identifier	Protocol Identifier	Length	Unit Identifier	Function Code	Data
2 bytes	2 bytes	2 bytes	1 byte	1 byte	n bytes

Fig. 3. MODBUS TCP Data Frame

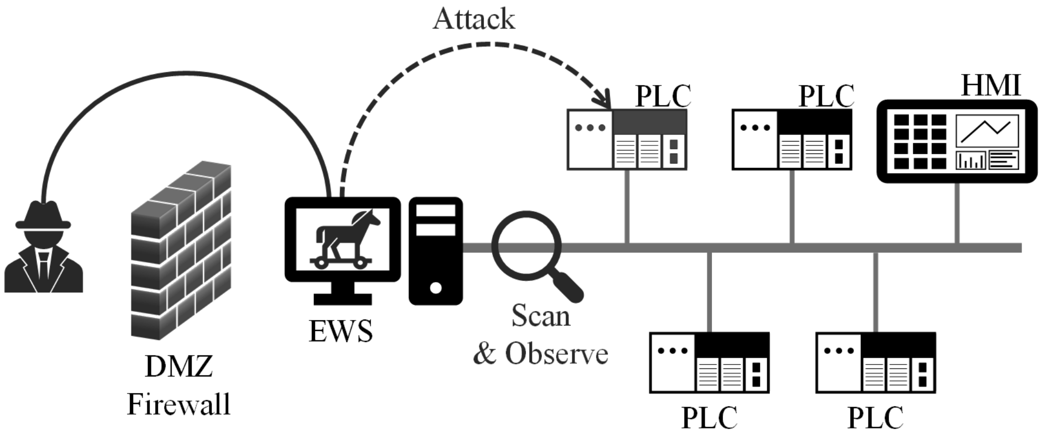


Fig. 4. The Scenario and Procedure of Attack in an Ethernet-enabled ICS Network

MODBUS is simple. It only consists of function code and data. Depending on the function codes and request or response, the following data structure is different. For example, function code 03 is reading multiple holding registers, the request data structure is composed of 2 bytes starting address and 2 bytes quantity of registers, and the response data structure is composed of 1 byte following data size and the value of registers [7].

MODBUS Messaging on TCP/IP, or MODBUS TCP for short, as the name suggests, is MODBUS implemented on the TCP/IP (see Fig. 1), and the port number of it is 502. The data frame of MODBUS TCP is in Fig. 2. Transaction identifier is for pairing the request and response. Protocol identifier is used for internal system multiplexing, and value 0 stands for MODBUS protocol. The length field is the byte count of the rest part including unit identifier, function code, and data field. Unit identifier is used for the internal system routing purpose. Function code and data field are MODBUS PDU [8].

3. Attacking an Ethernet-enabled ICS Network

3.1. *Scenario*

Since ICS with IT brings vulnerabilities, the attacker could use those vulnerabilities to inject a backdoor into the computers in the ICS, bypass the information security protection measures, and perform malicious operations. For example, an attacker could implant a Trojan horse into the EWS in the ICS via social engineering, then bypass the firewall and invade into the ICS network to do whatever he wants. Therefore, assuming that the attacker is able to access the ICS network with some method like backdoor, we generalized a procedure to get the information of the ICS and attack it.

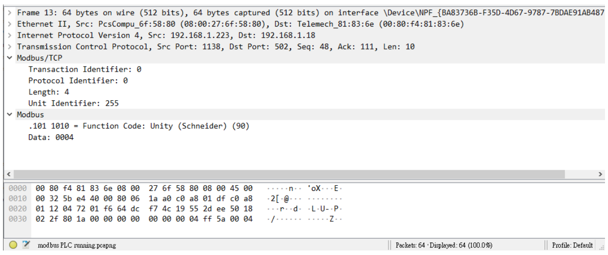
3.2. *Procedure*

The first thing to do is scanning the internal network. In most internal ICS networks, due to the weakness of IT security in ICS, there is no protection method like IDS and IPS. Therefore, by scanning the network, the attacker can observe the information in the ICS network such as enabled services, subnets' range, the number of devices, manufacturer of devices, and so on. After obtaining the information of the ICS network, according to the information, the attacker can formulate detailed attack methods such as man-in-the-middle attack with ARP spoofing to compromise the information security and operation safety in the ICS.

4. Case Study

The ICS that we are going to demonstrate the procedure on is the same as our previous study [9]. The ICS is composed of tens of PLCs to control the field equipment and one computer as the HMI to gather data and control PLCs. All of them are connected to an Ethernet switch.

First, we used a tool called Nmap to scan the ICS network. In the result, we can see the information of online devices, such as IP address, enabled services, and MAC address, and we can identify that the manufacture of PLC is Telemecanique Electrique which is Schneider Electric from the MAC address. The communication



```
> Frame 13: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{BA83736B-F35D-4D67-9787-7BDAE91AB487
> Ethernet II, Src: PcsCompu_6f:58:80 (08:00:27:6f:58:80), Dst: Telemech_81:83:6e (00:80:f4:81:83:6e)
> Internet Protocol Version 4, Src: 192.168.1.223, Dst: 192.168.1.18
> Transmission Control Protocol, Src Port: 1138, Dst Port: 502, Seq: 48, Ack: 111, Len: 10
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 4
    Unit Identifier: 255
v Modbus
    .101 1010 = Function Code: Unity (Schneider) (90)
    Data: 0004

0000  00 80 f4 81 83 6e 08 00  27 6f 58 80 08 00 45 00   ·····n·· 'oX···E·
0010  00 32 5b e4 40 00 80 06  1a a0 c0 a8 01 df c0 a8   ·2[·@··· ········
0020  01 12 04 72 01 f6 64 dc  f7 4c 19 55 2d ee 50 18   ···r··d· ·L·U-·P·
0030  02 2f 80 1a 00 00 00 00  00 00 00 04 ff 5a 00 04   ·/······ ·····Z··
```

modbus PLC running.pcapng
Packets: 64 · Displayed: 64 (100.0%)
Profile: Default

Fig. 5. The MODBUS TCP packets with function code 90

protocol of Schneider PLC is MODBUS, so we tried to read the holding registers with standard MODBUS function code 03 with the MODBUS TCP testing tool, and it works. Furthermore, the writing holding registers' function code 16 also works.

In our previous study, we used the IDE called TwidoSuite to perform some malicious operation on the PLC. This time, we use a tool called Wireshark to record the MODBUS TCP packets. Unlike the standard MODBUS TCP, the function code of those packets is 90 (see Fig. 5.), which is manufacturer defined. It is not able to just do the replay attack because of the authentication mechanism in the data bytes of MODBUS. However, we found some rules of it. We successfully established the connection and commanded the online PLC to stop.

5. Conclusion

In this paper, we discussed the weakness of IT security in the ICS network, generalized an attacking procedure for the ICS network, and implemented it to the real industrial system to support the argument. It turns out that we can easily obtain the information of the ICS with the procedure in the certain scenario without the knowledge of the ICS. As the widespread use of IT infrastructure in ICS, we must pay more attention to the cyber security in ICS.

Acknowledgements

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 109-2218-E-006-014- and MOST 109-2218-E-006-510-.

References

1. Martin Wollschlaeger, Thilo Sauter, Juergen Jasperneite, The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0, *IEEE Industrial Electronics Magazine*, vol. 11, pp. 17-27, 2017.
2. TSMC, *TSMC Details Impact of Computer Virus Incident*, TSMC, Hsinchu, 2018.
3. eicos*, M12 Plug Connector - M12 Male Straight Connector without Cable,* eicos*,* Online. Available: http://eu.eicos.com/accessories/connectors/m12-male-straight-connector/. Accessed 14 12 2020.
4. Lapp Tannehill, *LAPP ETHERLINE® 2 Pair: CAT5 Flexible - 22 AWG - Green*, Lapp Tannehill, Online. Available: https://www.lapptannehill.com/etherline-2pair-cat5e-flexible-22awg-green. Accessed 15 12 2020.
5. BELDEN, *Category 6 Cable - 7931A*, BELDEN, Online. Available: https://www.belden.com/products/cable/ethernet-cable/industrial-ethernet-cable/7931a. Accessed 15 12 2020.
6. Cisco, *Cisco Industrial Ethernet 4000 Series Switches Data Sheet*, Cisco, 2020.
7. Modbus Organization, *MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3*, Modbus Organization, Hopkinton, 2012.
8. Modbus Organization, *MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE v1.0b*, Modbus Organization, Hopkinton, 2006.
9. Kuan-Ming Su, I-Hsien Liu, Jung-Shian Li, The Risk of Industrial Control System: Programmable Logic Controller Default Configurations, in *International Computer Symposium 2020*, Tainan, 2020.