Identifying and Verifying Vulnerabilities through PLC Network Protocol and Memory Structure Analysis

Joo-Chan Lee[1], Hyun-Pyo Choi[1], Jang-Hoon Kim[1], Jun-Won Kim[1], Da-Un Jung[1], Ji-Ho Shin[1] and Jung-Taek Seo[1, *]

Abstract: Cyberattacks on the Industrial Control System (ICS) have recently been increasing, made more intelligent by advancing technologies. As such, cybersecurity for such systems is attracting attention. As a core element of control devices, the Programmable Logic Controller (PLC) in an ICS carries out on-site control over the ICS. A cyberattack on the PLC will cause damages on the overall ICS, with Stuxnet and Duqu as the most representative cases. Thus, cybersecurity for PLCs is considered essential, and many researchers carry out a variety of analyses on the vulnerabilities of PLCs as part of preemptive efforts against attacks. In this study, a vulnerability analysis was conducted on the XGB PLC. Security vulnerabilities were identified by analyzing the network protocols and memory structure of PLCs and were utilized to launch replay attack, memory modulation attack, and FTP/Web service account theft for the verification of the results. Based on the results, the attacks were proven to be able to cause the PLC to malfunction and disable it, and the identified vulnerabilities were defined.

Keywords: Industrial control system, programmable logic controller, cybersecurity, network protocol, vulnerability.

1 Introduction

An Industrial Control System (ICS) is used for operating and maintaining geographically distributed major infrastructure, such as power, gas, and water. The ICS was initially operated in a closed environment, separately from any external networks, but technical advancement enabled its integration with various network technologies for efficient operation and maintenance. Although such advancement allowed organized operation and improved convenience, it also gave rise to many security vulnerabilities of the system [Dabidson, Andel, Yampolskiy et al. (2018)]. Cyberattacks exploiting such vulnerabilities of ICSs are increasing nowadays. As such, cybersecurity for such systems is essential as cyberattacks on ICSs can incur massive economic cost and cause human injuries as well. Most ICS have elements such as Human Machine Interface (HMI), Programmable Logic Controller (PLC), and Remote Terminal Unit (RTU) [Farhangi

[1] Department of Information Security Engineering, Soonchunhyang University, Asan, 31538, Korea.
[*] Corresponding Author: Jung-Taek Seo. Email: seojt@sch.ac.kr.
Received: 29 April 2020; Accepted: 25 May 2020.

(2010)]. Among them, the PLC is applied to almost all ICSs as it monitors and controls the field devices constituting the system, such as switches, valves, and sensors. Especially, the PLC is a vital cog in controlling field devices and is consequently targeted by cyberattacks. One of the features of attacks on ICSs is that the attackers identify the manufacturer of the ICS used by the target organization or company and pre-analyze the software vulnerability and proprietary network protocols of the device to launch cyberattacks. Today, more and more vulnerabilities of PLCs are discovered; a quick search on the ICS-CERT Repository shows more than 80 PLCs from 589 recommendations in all [Wardak, Zhioua and Almulhem (2016a)]. In addition, many scenario-based studies on PLC-related vulnerabilities and threats have come from global hacking and cybersecurity conferences. The PLC is believed to be generally safe if separated from any external networks, but the separation strategy (Air-gap) will not completely guarantee safety against attacks utilizing various malicious codes. For example, Stuxnet, which was developed for the purpose of destroying the centrifugal separator in the nuclear facilities in Iran, clearly showed the potential of an attack on an ICS; an attack was actually launched, with about 1,000 centrifugal separators destroyed [Falliere, Murchu and Chien (2010)]. Moreover, a lot of malicious code attacks have been launched, such as the BlackEnergy malicious code attack on Ukraine's power distribution system—which caused large-scale blackout [Khan, Maynard, McLaughlin et al. (2016)]—and other malicious code-based attacks exploiting vulnerabilities like Chien et al. [Chien, Murchu and Falliere (2011); Rrushi, Farhangi, Howey et al. (2015)]. Thus, there is an urgent need to analyze actively the vulnerabilities of PLCs to prevent possible cyberattacks preemptively.

This study dealt with the vulnerabilities of XGB PLC, which utilizes the XGT and GLOFA protocols exclusively developed by the manufacturer. The structures of the memory and network protocol of the PLC were analyzed, and a replay attack was launched by exploiting the vulnerabilities identified from the analysis. A memory modulation attack was also launched based on the analyzed memory structure, and it was confirmed to have caused a fatal error on the PLC. The rest of this paper is organized as follows: Section 2 presents the background of the study; Section 3 deals with other studies on the vulnerabilities of PLCs; Section 4 discusses the experimental setup to identify security vulnerabilities by analyzing the structures of the memory and network protocol; Section 5 defines the vulnerabilities identified after verifying the potential of attacks that exploit them; Section 6 presents the conclusion.

2 Background

2.1 Industrial control system architecture

This section deals with the overall structure to aid in understanding the ICS. Fig. 1 shows the architecture of ICS, which has 5 levels in all. Level 0 is made up of field devices such as motor, sensor, and valve, and it runs the actual physical processes. Level 1 collects the status information of the field devices through the control device and controls the physical processes. Level 2 receives the status data from the control devices and displays it on the HMI for overall operation and monitoring, and the engineer controls and manages the control devices on the network at the Engineering Workstation (EWS).

Level 3 carries out the specific scheduling of tasks and assures the reliability and optimization of overall on-site operation based on the data collected on the data historian. Lastly, Level 4 performs tasks such as operation management and maintenance as the area providing operation information to the control system.

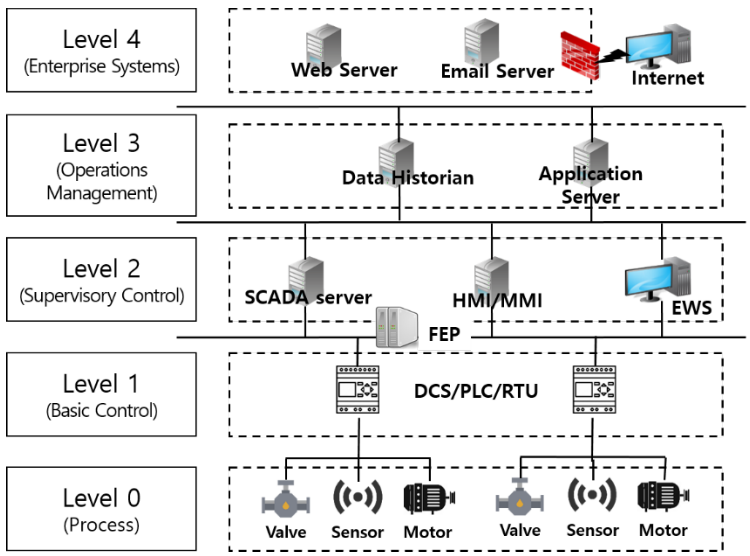


Figure 1: ICS architecture

2.2 PLC overview

As a programming-based universal control device activating machinery in manufacturing and industrial sites according to the predetermined order and conditions, the PLC is used in various fields of ICS; its application is expanding alongside the demand for automation and high efficiency. Basically, the PLC is made up of the CPU, memory, Input/Output (I/O) ports, and power supply unit. The CPU controls all operations of the PLC and reads the content from the memory to launch the programmed function. The memory is categorized into ROM and RAM. The ROM stores the software programmed upon manufacturing the PLC, mostly the system software needed to operate the PLC. The RAM is where the logic program by the user is stored and run including the frequently changed data from components such as timer and counter. The I/O ports are used for direct connection to the external field devices and delivery to the output port of the signals inputted to the calculation unit of the CPU and calculation results to operate the connected devices. The PLC has a programming interface that lets the user control the I/O devices and define the behavioral structure of the system. Generally, programming the PLC requires the PLC management software from the manufacturer; such software is installed on the EWS, which is tasked with developing and managing the overall system logic of the ICS. There are various programming languages for controlling the PLC. As the relevant international standard, IEC 61131-3 suggests the ladder diagram and function block diagram, which are graphic languages and structured text, instruction list, and sequential function chart in text format language [IEC (2013)]. Universally used network protocols of ICSs are Modbus, DNP3, Profinet, etc.; for PLC, however, each manufacturer of the device independently developed their proprietary network protocol to conduct communication.

3 Related works

Since the PLC plays a key role in controlling the field devices in ICSs, it is a major target of cyberattacks on ICSs. Thus, PLC security is directly linked to the overall security of the ICS, and many researchers are working on identifying the vulnerabilities of PLCs for the preemptive prevention of such cyberattacks.

Sandaruwan et al. [Sandaruwan, Ranaweera and Oleshchuck (2013)] presented the PLC vulnerabilities that may affect major infrastructure through various attack routes and cited replay attacks, man-in-the-middle attack, and authentication bypass attacks as effective attacks on PLCs. They also proposed security measures to protect PLCs, such as authentication, timestamp, and intrusion detection system.

Wardak et al. [Wardak, Zhioua and Almulhem (2016b)] used the analysis on the authentication mechanism of PLCs to specify attacks on PLCs such as simple replay attack, password theft, and unauthorized password update attack.

Cheng et al. [Cheng, Li and Ma (2017)] researched the vulnerabilities of the s7commplus protocol used for the Siemens PLC. They analyzed the s7commplus protocol utilized for communication between Tia Portal, workstation, and PLC device, reverse-engineered the authentication algorithm for communication to analyze the communication encryption of the protocol, and utilized the result in verifying the potential of replay attacks on the s7commplus protocol.

Spenneberg et al. [Spenneberg, Bruggemann and Schwartke (2016)] experimented with the Siemens PLC to prove the spread of a worm among PLCs. They analyzed the anti-replay byte of the protocol to launch the attack and assumed that the PLC is already infected with the worm from the attack on the supply chain, not from an external attack. They also noted that the control system does a poor job of detecting malicious codes on the PLC and described the three protective functions of the S7-1200 PLC, including the functions that can be protected from the worm.

Ylmaz et al. [Ylmaz, Ciylan, Gönen et al. (2018)] launched Denial of Service (DoS) attacks on the PLC to study the ripple effect from the attack. They analyzed the network protocol of the PLC and used the Hping utility based on the result to launch the DoS attack. The result showed delayed network traffic, which in turn led to the slowdown in the operation of the PLC and disabled control over the PLC control software.

Voyiatzis et al. [Voyiatzis, Katsigiannis and Koubias (2015)] designed and deployed the Modbus/TCP Fuzzer to analyze the vulnerabilities of the Modbus network protocol, which is widely used for ICS. They proposed an appropriate measure to address the vulnerabilities in the current or future Modus/TCP environment through the fuzzing tool.

They also analyzed the vulnerabilities of the PLC and conducted attack tests while proposing preventive measures for the attack test on ICSs and PLCs. Malchow et al. [Malchow, Marzin, Klick et al. (2015)] deployed the PLC Guard prototype, which is the security solution for preventing the falsification of network packets in the communication between the PLC and EWS. On the other hand, Akinori et al. [Akinori, Kenji, Seiichi et al. (2017)] modeled the behaviors of the field devices connected to the PLC and converted the model into ladder diagrams to come up with a whitelist and research preventive measures for cyberattacks targeting the PLC. Yau et al. [Yau and Chow (2015)] proposed the method of defining detection rules for the control logic of PLCs to detect logic-changing attacks and of subsequently utilizing the Control Program Logic Change Detector (CPLCD) developed in the study to detect the control logic arbitrarily changed by the attack. You et al. [You, Oh, Kim et al. (2018)] developed an information security maturity model that can measure and manage the data security functionality of critical infrastructure, verified its applicability through simulations, and identified the core security processes and their goals in determining the security maturity of the infrastructure. Other ongoing studies include the research to develop the technology for detecting abnormality in the data of ICSs based on machine learning in other to cope with the advancement of cyberattacks [Akpina and Ozcelik (2019); Lutz, Vogt, Berkhout et al. (2020); Gomez, Maimo, Celdran et al. (2019)].

These previous studies mostly identified vulnerabilities by analyzing the network protocol, which was also used to launch attacks. Thus, attacks exploiting the vulnerabilities of the network protocol are considered superior in terms of the methodology of attack on the PLC. In this study, the vulnerabilities of the XGB PLC were analyzed, and the potential of attacks was verified through experiments. This study is expected to contribute to the preparation of measures against attacks on PLCs.

4 Design of experimental setup and analysis of PLC structure

4.1 Design of experimental setup

Communication between the EWS and PLC was set up as in Fig. 1 to analyze the vulnerabilities of the PLC. The PLC used for the analysis was XGB from LS, which supports Ethernet, RS-232/RS-485 serial interface, and USB2.0 (mini-b) communication. XG5000—which programs, monitors, and controls the PLC—was also used to control the PLC. The network packet analysis tool Wireshark was utilized to analyze the protocol and capture the data packet delivered from XG5000 to the PLC. The potential of attacks was verified by utilizing the vulnerabilities identified from the analysis, and Pwntools was used to generate the packets for attack and transmit them. The PLC used for the experiment and the PC on which XG5000 was installed were each assigned an IP of 192.168.0.46 and 192.168.0.165, respectively. Tab. 1 shows the experimental setup, and Fig. 2 presents the network structure.

Table 1: Experimental setup

Device	Description
Hub	Iptime sw 1600
PLC	XGB series cpu ver 1.8
PC (EWS)	Windows 10 64 bit
	Ryzen 7 2700x, DDR4 16 G
	XG5000
	Wireshark
	Pwntools

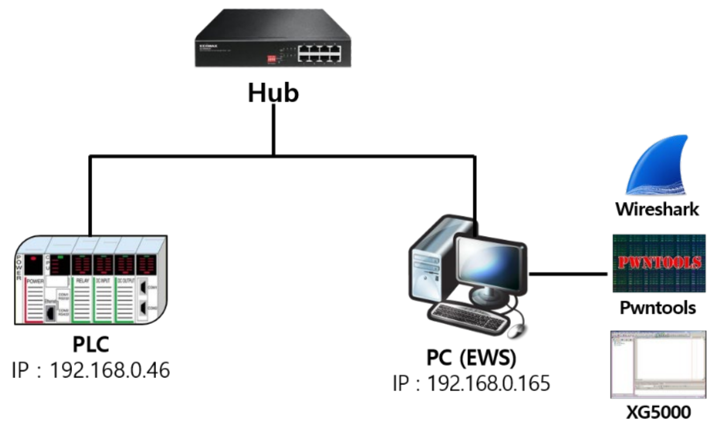


Figure 2: Diagram of network structure

4.2 Analyzing the memory and network protocol of PLC

4.2.1 Memory structure

The PLC has volatile and nonvolatile memories, and each stores the system software required for operation and the logic programmed by the user for controlling the PLC. The PLC used for analysis in this study provides the interface that allows viewing the memory areas from XG5000 by defining each memory area with alphabet. Tab. 2 shows the representative memory areas.

Table 2: Representative memory areas

Memory area	Function	Description
P	I/O contact	Memory of status of I/O contact
M	Internal contact	Memory of bit data
F	Special contact	Flag memory needed for system operation
T	Timer contact	Memory for output of timer bit
C	Counter contact	Memory for output of counter bit
D	Data register	Memory of internal data
R	File register	Memory for storing files

In particular, the memory interface of XG5000 allows the user to edit the memory areas; nonetheless, the area with sensitive data affecting the operation of the PLC is greyed out so that the user cannot access it directly with the interface. Attempting to edit the values of the greyed-out memory area results in an error as shown in Fig. 3.

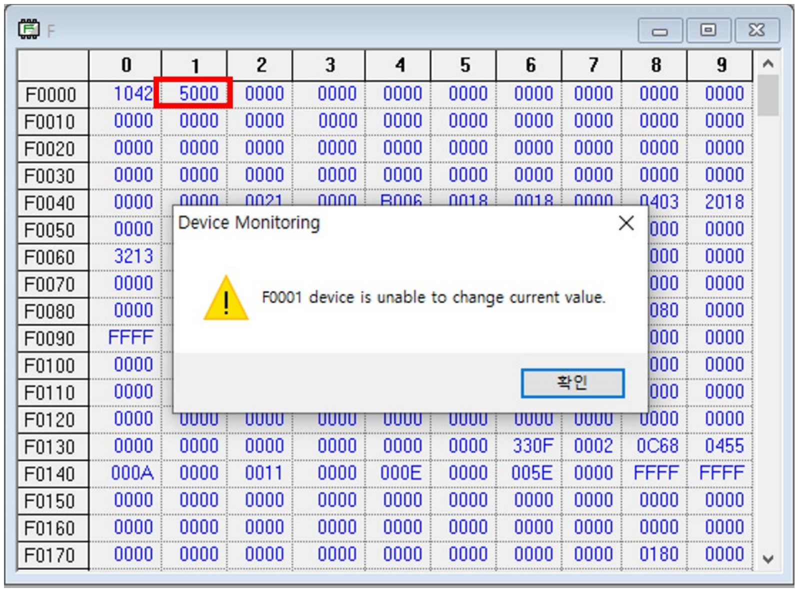


Figure 3: Error due to memory value change

4.2.2 Network protocol structure

The PLC analyzed in this study supports Ethernet and serial communication and uses the proprietary protocol developed by the manufacturer for the former. The experiment targeted the Ethernet protocol. In particular, the Ethernet protocol of the XGB PLC comes in two types: the XGT protocol for communication between the HMI and PLC, and; the GLOFA protocol for communication between XG5000 and PLC. The names XGT and GLOFA are the character strings in the header ID of the corresponding protocols and were used to name each protocol. Cyberattacks on the ICS mostly target the EWS, which runs the overall programming and management of control devices on the ICS. Obtaining the control rights of the EWS means having overall control of the ICS. Thus, in this study, the GLOFA protocol was analyzed to attack communication between the EWS and PLC, and the packets used for analysis are those from sending the Run/Stop commands from XG5000 to the PLC. The GLOFA protocol uses port no. 2002 for communication, whereas XG5000 undergoes the TCP 3-way handshake process for connection to the PLC. After the process was completed, the GLOFA protocol shown in Fig. 4 was used to deliver the basic information of PLC and establish the initial connection.

```
0000  00 0b 29 71 07 ed 0c 9d  92 76 6f 0d 08 00 45 00    ··)q···· ·vo···E·
0010  00 48 73 e0 40 00 80 06  04 ac c0 a8 00 a5 c0 a8    ·Hs·@··· ········
0020  00 2e f1 9c 07 d2 c0 f6  ef 2c 00 00 2f e6 50 18    ·.······ ·,··/·P·
0030  fa f0 2c c0 00 00 4c 47  49 53 2d 47 4c 4f 46 41 ①  ··,···LG IS-GLOFA
0040  00 00 00 22 00 00 0c 00  00 f3 0a 00 c0 a8 00 2e ②  ···"···· ·······.
0050  00 00 00 00 ff 00                                   ······
```

Figure 4: Initial connection establishment in the GLOFA protocol

① in Fig. 4 is the protocol header consisting of the protocol ID, information, and length of the application data of the connected PLC. ② is the application data area, showing the behavior information of the PLC as per commands. The frame structure of the GLOFA protocol is presented in Tab. 3.

Table 3: Frame structure of the GLOFA protocol

Header	Command	Data address	Data	Application checksum
20 bytes	1 byte	1 byte	n bytes	2 bytes

After establishing communication between XG5000 and PLC, the packets in Fig. 5 are transmitted when sending the "PLC Run" command. An analysis of the packets in Fig. 5 found that the character string M is the mode, and that R means the "Run" command. In addition, the character string R is replaced with S when the "Stop" command is sent from the PLC; only the corresponding character strings and checksum values are changed, with the other values on the network packets unaffected.

```
0000  00 0b 29 71 07 ed 0c 9d  92 76 6e 92 08 00 45 00   ··)q···· ·vn···E·
0010  00 44 4a 99 40 00 80 06  2e 48 c0 a8 00 54 c0 a8   ·DJ·@··· .H···T··
0020  00 2e e5 ee 07 d2 c4 36  64 0a 09 2f c8 a4 50 18   ·.·····6 d··/··P·
0030  f7 34 57 b7 00 00 4c 47  49 53 2d 47 4c 4f 46 41   ·4W···LG IS-GLOFA
0040  00 00 00 22 00 00 08 00  00 ef 0e 00 04 00 4d 52   ···"···· ······MR
0050  39 46                                              9F
```

Figure 5: Packet of the PLC Run command

Based on the analysis of the protocol, neither security-related elements such as anti-replay byte, session verification, or timestamp in the communication with the PLC nor authentication or encryption with proper security was in place. Such lack of security elements is believed to give rise to vulnerabilities to replay attacks and intermediary attacks using packet sniffing. Thus, in this study, the vulnerabilities in the communication process of the GLOFA protocol were utilized to confirm the possibility of replay attacks and memory modulation attacks.

4.2.3 FTP/Web service

The PLC used for the analysis in this study supports FTP/Web services and enables access to the Secure Digital (SD) card on the PLC through FTP/Web connection. Upon connecting to the service, the data log files on the SD card can be copied to the PC or other devices of the user (the FTP/Web services available from the PLC support downloading only). Such access necessitates setting up the account on XG5000, and the account information was found to be stored in the project file of the PLC.

5 Defining vulnerabilities from attacks and results

5.1 Experimental method

An analysis of the PLC's GLOFA protocol exposed its vulnerabilities as verified through an experiment of the potential of attacks exploiting them. Experiments were performed using three methods: replay attack, memory modulation attack, and account theft attack. The detailed methodology is described below.

5.1.1 Replay attack

The protocol of the PLC network was found not to be applied with security elements such as encryption and session verification. Thus, replay attacks exploiting the vulnerabilities were set as the experiment goal. First, for the replay attacks on the PLC, the Run/Stop command packets were captured between XG5000 and the PLC with Wireshark. Based on the analysis in 4.2.2, the Pwntools library was utilized to generate the packets for the attack, and the replay attack was launched on the PLC from the PC.

5.1.2 Memory modulation

Memory modulation targeted the F area to which the memory protection described in 4.2.1 was applied. For the experiment, the data in the normal memory area was first obtained; the command packets were then created to write data modulated with Pwntools. Afterward, the memory modulation attack was launched using the replay attack method. In verifying the success of the attack, the memory interface function of XG5000 was utilized to see if the modulated data was inserted into the actual memory area.

5.1.3 FTP/Web service account theft

The PLC was confirmed to store the information of the account for the FTP/Web services in the project file. Thus, a service account theft attack was launched by analyzing the project file download packets, and the user ID and password were set up for the experiment as in Fig. 6.

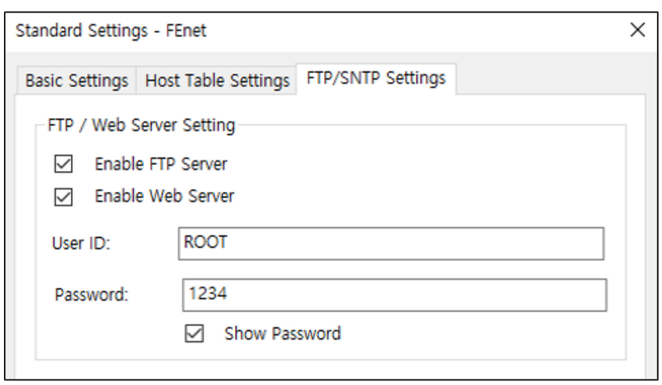


Figure 6: Setup of the FTP/Web service account

5.2 Results of attacks and definition of vulnerabilities

5.2.1 Results of replay attack

The packets for the replay attack are those for sending the Run command to the PLC and will be received as in the red part of Fig. 7 from the PLC if normal communication is established between XG5000 and the PLC.

```
0000  0c 9d 92 76 6e 92 00 0b  29 71 07 ed 08 00 45 00   ···vn··· )q····E·
0010  00 48 f9 aa 00 00 80 06  bf 32 c0 a8 00 2e c0 a8   ·H······ ·2···.··
0020  00 54 07 d2 e5 ee 09 2f  c8 a4 c4 36 64 26 60 18   ·T·····/ ···6d&`·
0030  05 dc 87 67 00 00 02 04  05 b4 4c 47 49 53 2d 47   ···g···· ··LGIS-G
0040  4c 4f 46 41 06 02 b0 11  00 00 08 00 3f d5 0f 00   LOFA···· ····?···
0050  04 00 06 4d 34 44                                  ···M4D
```

Figure 7: Response packet to the PLC Run command

As described in 5.1.1, a replay attack was launched with the Run command. Fig. 8 shows the packets received by the PLC after sending the attack packets.

```
 OSX 〉 glucose 〉    81% (5:48)  …/Sources
└    python replay.py
[+] Opening connection to 192.168.0.46 on port 2002: Done
'\x06\x02\xb0\x11\x00\x00\x08\x00?\xd5\x0f\x00\x04\x00\x06M4D'
[*] Closed connection to 192.168.0.46 port 2002
```

Figure 8: Response packet to the replay attack of the PLC Run command

As shown in Fig. 8, the same response has been given as the resent packets are recognized as normal communication by the PLC, which recognized the corresponding packet data as normal data without applying any restrictions. This means that the attacker —after analyzing the normal control commands through network sniffing—can send malicious control commands to the PLC by modulating the control command packets and may cause physical damages to the field devices by downloading malicious logic and causing a malfunction of the PLC.

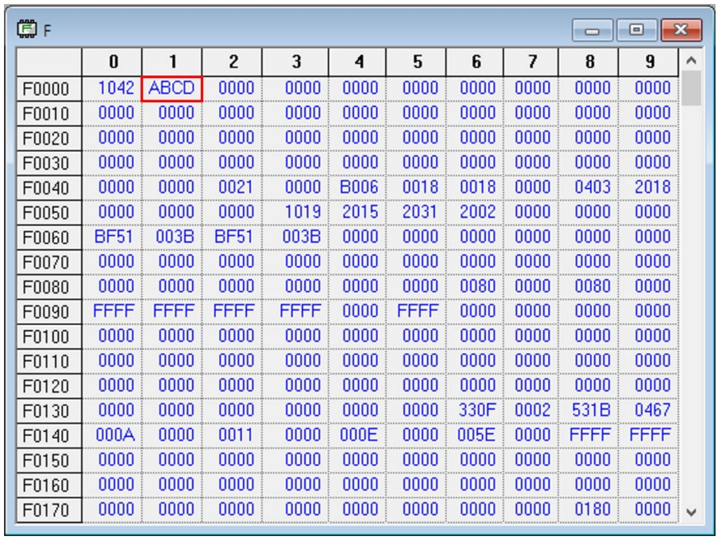
5.2.2 Results of the memory modulation attack

With the attack methods from 5.1.2, an attack involving inserting the character strings of 0xABCD as in Fig. 9 in the memory areas described in 4.2.1 was launched.

```
from plc import CLASS_XX

plc = CLASS_XX()
plc.connect()

print plc.W("n", 2, 2, "\xCD\xAB")

plc.disconnect()
```

Figure 9: Memory modulation attack using pwntools

As a result of the network packet-based memory modulation attack on the area inaccessible to the user with XG5000, the F0001 area with value of 0×5000 as shown in Fig. 3 was found to have been changed to 0xABCD as in Fig. 10.



F

	0	1	2	3	4	5	6	7	8	9
F0000	1042	ABCD	0000	0000	0000	0000	0000	0000	0000	0000
F0010	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0020	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0030	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0040	0000	0000	0021	0000	B006	0018	0018	0000	0403	2018
F0050	0000	0000	0000	1019	2015	2031	2002	0000	0000	0000
F0060	BF51	003B	BF51	003B	0000	0000	0000	0000	0000	0000
F0070	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0080	0000	0000	0000	0000	0000	0000	0080	0000	0080	0000
F0090	FFFF	FFFF	FFFF	FFFF	0000	FFFF	0000	0000	0000	0000
F0100	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0110	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0120	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0130	0000	0000	0000	0000	0000	0000	330F	0002	531B	0467
F0140	000A	0000	0011	0000	000E	0000	005E	0000	FFFF	FFFF
F0150	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0160	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
F0170	0000	0000	0000	0000	0000	0000	0000	0000	0180	0000

Figure 10: Modulated memory value through the attack

To verify the ripple effects of additional attacks, a memory modulation attack was launched on the system flag memory area (F area), which has a key role in the PLC. The attack was launched by overwriting random values in the whole area of the F memory, and Fig. 11 presents the results.

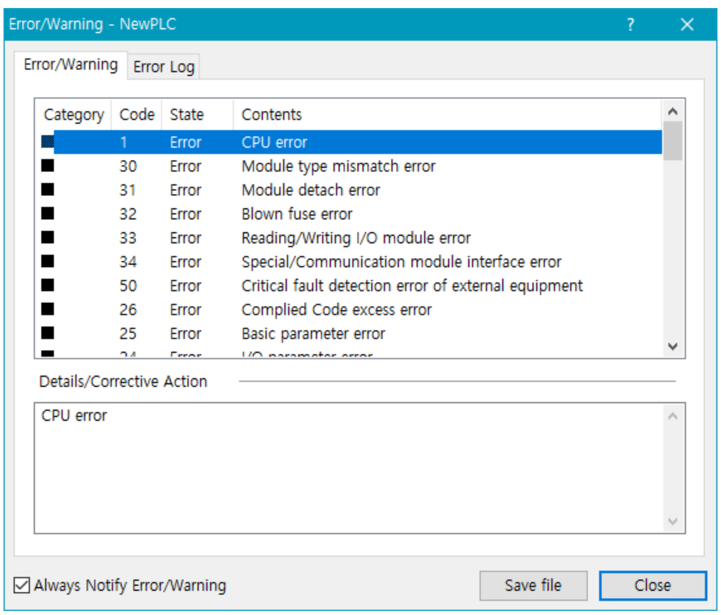
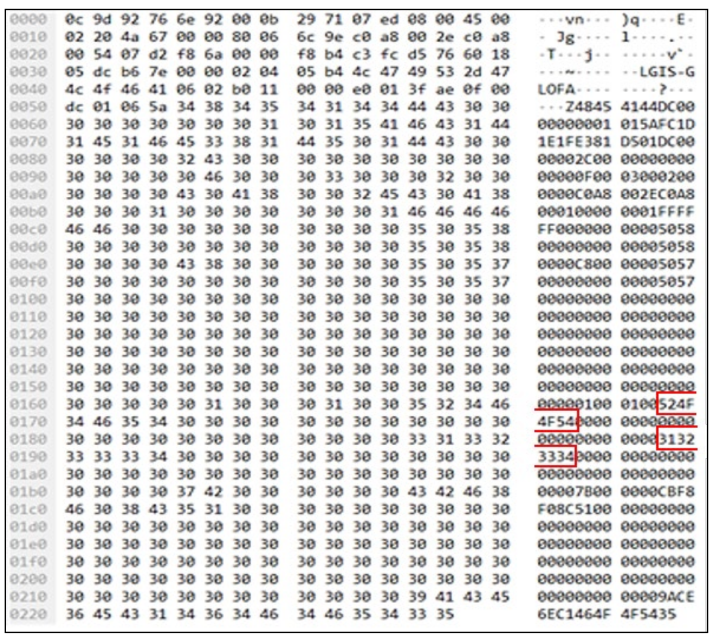


Figure 11: PLC disable due to memory modulation attack

Based on the results, the PLC encounters numerous errors as shown in Fig. 11 by having its memory modulated and becomes incapacitated, in which case no operation is possible at all. Recovery from the errors of the PLC necessitates resetting it, but the network was inaccessible as the Ethernet port was disabled by the attack; only physical communication utilizing the USB port was possible in order to reset the PLC and restore its operation successfully. If these kinds of attack as described herein are launched on national infrastructure or major industrial sites, illegal commands can be sent, and the memory can be modulated to incapacitate the PLC; thus causing huge economic and physical damages and even injury or death in the most severe cases.

5.2.3 Result of FTP/Web service account theft attack

Establishing connection to the PLC using XG5000 enables downloading the active project files in the PLC. Fig. 12 shows some of the packets with values from downloading the uploaded project file as read from the 0×86 memory. The red parts—0×524F4F54 and 0×31323334—and the hex-encoded values of the user ID and password set up in Fig. 6 were found to be information of the account accessing the FTP/Web services of the actual PLC through decoding. The experiments verified that the account information was stored in the memory area with no encryption; this also means that the attacker can steal the account information easily by analyzing in advance the memory area of the PLC. Accessing the services with this attack lets the attacker obtain the operation logs of the PLC; an uploaded project file will provide specific information for attacks such as the structure and control logic of the PLC.



```
0000  0c 9d 92 76 6e 92 00 0b  29 71 07 ed 08 00 45 00   ···vn··· )q····E·
0010  02 20 4a 67 00 00 80 06  6c 9e c0 a8 00 2e c0 a8   · Jg···· l····.··
0020  00 54 07 d2 f8 6a 00 00  f8 b4 c3 fc d5 76 60 18   ·T···j·· ·····v`·
0030  05 dc b6 7e 00 00 02 04  05 b4 4c 47 49 53 2d 47   ···~···· ··LGIS-G
0040  4c 4f 46 41 06 02 b0 11  00 00 e0 01 3f ae 0f 00   LOFA···· ····?···
0050  dc 01 06 5a 34 38 34 35  34 31 34 34 44 43 30 30   ···Z4845 4144DC00
0060  30 30 30 30 30 30 30 31  30 31 35 41 46 43 31 44   00000001 015AFC1D
0070  31 45 31 46 45 33 38 31  44 35 30 31 44 43 30 30   1E1FE381 D501DC00
0080  30 30 30 30 32 43 30 30  30 30 30 30 30 30 30 30   00002C00 00000000
0090  30 30 30 30 30 46 30 30  30 33 30 30 30 32 30 30   00000F00 03000200
00a0  30 30 30 30 43 30 41 38  30 30 32 45 43 30 41 38   0000C0A8 002EC0A8
00b0  30 30 30 31 30 30 30 30  30 30 30 31 46 46 46 46   00010000 0001FFFF
00c0  46 46 30 30 30 30 30 30  30 30 30 30 35 30 35 38   FF000000 00005058
00d0  30 30 30 30 30 30 30 30  30 30 30 30 35 30 35 38   00000000 00005058
00e0  30 30 30 30 43 38 30 30  30 30 30 30 35 30 35 37   0000C800 00005057
00f0  30 30 30 30 30 30 30 30  30 30 30 30 35 30 35 37   00000000 00005057
0100  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0110  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0120  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0130  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0140  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0150  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0160  30 30 30 30 30 31 30 30  30 31 30 30 35 32 34 46   00000100 0100524F
0170  34 46 35 34 30 30 30 30  30 30 30 30 30 30 30 30   4F540000 00000000
0180  30 30 30 30 30 30 30 30  30 30 30 30 33 31 33 32   00000000 00003132
0190  33 33 33 34 30 30 30 30  30 30 30 30 30 30 30 30   33340000 00000000
01a0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
01b0  30 30 30 30 37 42 30 30  30 30 30 30 43 42 46 38   00007B00 0000CBF8
01c0  46 30 38 43 35 31 30 30  30 30 30 30 30 30 30 30   F08C5100 00000000
01d0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
01e0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
01f0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0200  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   00000000 00000000
0210  30 30 30 30 30 30 30 30  30 30 30 30 39 41 43 45   00000000 00009ACE
0220  36 45 43 31 34 36 34 46  34 46 35 34 33 35         6EC1464F 4F5435
```

Figure 12: FTP/Web service account information

5.2.4 Defining vulnerabilities according to the experiment results

A vulnerability analysis on an XGB PLC was conducted in this study. The security vulnerabilities were identified by analyzing network protocols and memory structure and utilized to launch replay attack, memory modulation attack, and FTP/Web service account theft. The results of attacks were put forward and verified based on the experiment results. Tab. 4 shows the vulnerabilities verified by experiments conducted in this study.

Table 4: Definition of vulnerabilities on the PLC

Vulnerability	Definition
Absence of authentication	No authentication is performed during PLC communication. This enables attackers to access the PLC system without explicit authorization.
Bypass of memory protection	PLC memory protection could be compromised since the memory can be modulated by generating and transmitting an attack packet.
Replay attack	Neither authentication nor encryption is done during network communication between the devices connected to the PLC. This gives rise to a vulnerability since unauthorized access and attacks can occur using the copied packet.
Memory modulation	Generating and sending a memory modulation attack packet give rise to a vulnerability in the illegal manipulation of PLC memory through the analysis of the protocol, since no authentication is performed during PLC communication.
Privilege escalation	Since no authentication is performed during PLC communication, copying and retransmitting control packets give rise to a vulnerability, i.e., the privilege of an attacker may be escalated to that of a normal user.
Account theft	Since the account information by which FTP/Web services could be accessed is stored in plain text format, attackers can steal the account information by analyzing the memory area.

6 Conclusion

At present, many ICSs utilize Ethernet-based communication protocols for obtaining data and controlling processes conveniently and efficiently. Nonetheless, such trend gave rise to new security threats to ICSs, which are made up of closed networks. Given the growing number of attacks exploiting the vulnerabilities of Ethernet-based communications protocols, many studies are ongoing to apply cybersecurity to PLCs. In this study, the vulnerabilities of PLCs deployed in ICSs were analyzed to determine the viability of attacks. First, this study dealt with the general features of PLCs, and then identified the security vulnerabilities by analyzing the network protocols and memory structure used by PLCs while carrying out replay attacks, memory modulation attacks, and FTP/Web service account theft attacks based on the results of the identification. Moreover, the viability of attacks exploiting such vulnerabilities was confirmed, and the vulnerabilities requiring improvement were defined based on the experiment results. Identifying said vulnerabilities and verifying the attacks both contribute considerably to the preparation of measures for the on-site operators. Future studies will focus on the analysis and research on issues of the operational environment of the PLCs by analyzing the vulnerabilities and launching attacks. A study on the protection measures for the previously suggested vulnerabilities will be carried out as well.

Funding Statement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT: Ministry of Science and ICT) (Nos. NRF-2016M2A8A4952280 and NRF-2020R1A2C1012187).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Akpinar, K. O.; Ozcelik, I. (2019): Analysis of machine learning methods in EtherCAT-based anomaly detection. *IEEE Access*, vol. 7, pp. 184365-184374.

Cheng, L.; Li, D.; Ma, L. (2017): The spear to break the security wall of S7commplus. *Proceedings of Black Hat USA*, pp. 1-12.

Chien, E.; Murchu, L. O.; Falliere, N. (2011): W32.Duqu: the precursor to the next Stuxnet. *Symantec Security Response*, pp. 1-71.

Dabidson, C. C.; Andel, T. R.; Yampolskiy, M.; McDonald, J. T.; Glisson, W. B. (2018): On SCADA PLC and fieldbus cyber-security. *Proceedings of 13th International Conference on Cyber Warfare and Security*, pp. 140-148.

Falliere, N.; Murchu, L. O.; Chien, E. (2010): W32.Stuxnet Dossier. *Symantec Security Response*, pp. 1-64.

Farhangi, H. (2010): The path of the smart grid. *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18-28.

Gomez, A. L. P.; Maimo, L. F.; Celdran, A. H.; Clemente, F. G.; Sarmiento, C. C. et al. (2019): On the generation of anomaly detection datasets in industrial control system. *IEEE Access*, vol. 7, pp. 177460-177473.

IEC (2013): International standard IEC 61131-3 (edition3.0) programmable logic controllers, part 3: programming languages. *International Electrotechnical Commission*, pp. 1-220.

Khan, R.; Maynard, P.; McLaughlin, K.; Laverty, D.; Sezer, S. (2016): Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. *Proceedings of 4th International Symposium for ICS & SCADA Cyber Security Research*, pp. 53-63.

Lutz, M. A.; Vogt, S.; Berkhout, V.; Faulstich, S.; Dienst, S. et al. (2020): Evaluation of anomaly detection of an autoencoder based on maintenance information and SCADA-data. *Journal of Energies*, vol. 13, pp. 1-18.

Malchow, J.; Marzin, D.; Klick, J.; Kovacs, R.; Roth, V. (2015): PLC guard: a practical defense against attacks on cyber physical systems. *Proceedings of IEEE Conference on Communications and Network Security*, pp. 326-334.

Mochizuki, A.; Sawada, K.; Shin, S.; Hosokawa, S. (2018): On experimental verification of model based white list for PLC anomaly detection. *Proceedings of 11th Asian Control Conference*, pp. 1766-1771.

Rrushi, J.; Farhangi, H.; Howey, C.; Carmichael, K.; Dabell, J. (2015): A quantitative evaluation of the target selection of Havex ICS malware plugin. *Proceedings of Industrial Control System Security Workshop*, pp. 1-5.

Sandaruwan, G. P. H.; Ranaweera, P. S.; Oleshchuk, V. A. (2013): PLC security and critical infrastructure protection. *Proceedings of IEEE 8th International Conference on Industrial and Information Systems*, pp. 81-85.

Spenneberg, R.; Bruggemann, M.; Schwartke, H. (2016): PLC-blast: a worm living solely in the PLC. *Proceedings of Black Hat Asia*, pp. 1-16.

Voyiatzis, A. G.; Katsigiannis, K.; Koubias, S. (2015): A Modbus/TCP fuzzer for testing internetworked industrial systems. *Proceedings of IEEE 20th Conference on Emerging Technologies & Factory Automation*, pp. 1-6.

Wardak, H.; Zhioua, S.; Almulhem, A. (2016): PLC access control: a security analysis. *Proceedings of World Congress on Industrial Control Systems Security*, pp. 56-61.

Yau, K.; Chow, K. P. (2015): PLC forensics based on control program logic change detection. *Journal of Digital Forensics, Security and Law*, vol. 10, no. 4, pp. 59-68.

Ylmaz, E. N.; Ciylan, B.; Gönen, S.; Sindiren, E.; Karacayılmaz, G. (2018): Cyber security in industrial control systems: analysis of DoS attacks against PLCs and the insider effect. *Proceedings of 6th International Istanbul Smart Grids and Cities Congress and Fair*, pp. 81-85.

You, Y. J.; Oh, J. Y.; Kim, S. H.; Lee, K. H. (2018): Advanced approach to information security management system utilizing maturity models in critical infrastructure. *KSII Transactions on Internet and Information Systems*, vol. 12, no. 10, pp. 4995-5012.