Demonstrable System of Operational Technologies Cybersecurity with Industrial Control Protocols

Leyan Pan, Zezhou Zhang, Matthew Dobbs, Nat Prakongpan, John Clarke, Richard Moore
X-Force Command Center at IBM Security, USA

Abstract— **Due to the development of Big Data, Internet of Things, and Artificial intelligence, instead of being air-gapped, modern industries start merging Information Technology and their existing Operational Technologies for business continuity and efficiency. However, various fatal vulnerabilities are being exposed to the outside world, and because of a lack of security measurements, cyberattacks can cause severe problems, such as Denial of Service (DoS), information exposure, and other harmful actions to damage the industrial equipment. This paper provides an overview and commonly used system topologies of Industrial Control System (ICS), and discovered vulnerabilities from basic low-level infrastructure to industrial control protocols including EtherNet/IP and Modbus. Besides, some countermeasures and methods for those attacks and risks are provided in this paper to mitigate the threats of the Internet. A demonstrable system is developed in the IBM by using Rockwell Automation/Allen-Bradley MicroLogix 1100 PLC to indicate how vulnerable this popular industrial controller is and how effortless to perform attacks by exploiting it.**

Keywords—Distributed Control System (DCS), Industrial Control System (ICS), Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA) system, Human Machine Interface (HMI)

I. Introduction

With the trend of working from home, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against critical infrastructure by exploiting internet-accessible operation technology (OT) assets, according to the alert (AA20-205A) from National Cyber Awareness System[1] announced on July.23, 2020. Hardening the network, making incident response Plan, and implementing a continuous and vigilant system monitoring program are recommended to strengthen the OT processes and mitigate risks from potential cyber threat activities. Integrated with Information Technology (IT), the previously isolated control systems and obsolete automation equipment are connected to the enterprise-wide network with other utility providers. However, the network security weakness is usually not put on the first place by industrial technicians. In addition, the Modern industrial network protocols have evolved from serial-based field-bus protocols to TCP/IP-based protocols that are transported over standard Ethernet links[2]. To demonstrate the significance of cyber threats in the current ICS environment, the IBM X-Force Cybersecurity team developed an industrial water control system with EtherNet/Industrial Protocols. If a remote attacker once attacks a computer or simply get access into the enterprise intranet, this attacker can sneak into the central control system through various methods, such as Man-in-the-Middle (MitM) attack to sniff authentication packets in air or send invalid packets to trigger the PLC into a fault status. Eventually, it can cause damage to the water system by messing with the memory data files and make the process not easily recoverable. Attackers can remain persistently and stealthily. In the communication layer, the Common Industrial Protocol (CIP) and EtherNet/Industrial Protocol (EtherNet/IP) are well-known protocols used by a large amount of industrial automation vendors. In the demonstrable system, Rockwell Automation MicroLogix 1100 with the latest firmware version 16.000 are being used for controlling the solenoid valve and water pump. RsLogix Micro Starter Lite and Pycomm module are the software for programming the PLC and implementing the EtherNet/IP communication.

II. Background

A. Purdue Model

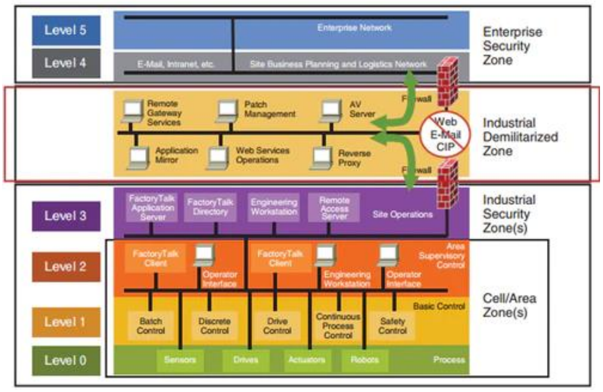


Fig. 1. The Purdue Model of Computer Integrated Manufacturing[3]

The ICS Purdue Model has provided industrial communication security through its separation of layers and definition of how machines and processes should function and interact[3]. Despite the influence of ISA-95 standard that defines the interface between enterprise and control systems, this hierarchical structure is not strictly followed in the industry due to the use of smart sensors, or the web server embedded in the PLC, etc., For instance, the data collected from the sensor at level 0 can be sent to cloud for predictive computing and maintenance, but sending data directly from level 0 to 5 violates the segmentation of the Purdue Model[3]. To achieve the data flow between IT and OT and meet the flexibility need of the IoT environment, a new hybrid approach and topology should be presented in the future. Before that, the traditional Purdue Model should continue to be followed to ensure the network is not comprised and maintain the safe operation of industrial equipment.

B. Stuxnet

In 2010, Stuxnet is discovered as a computer worm that was originally aimed at Iran’s nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities[4]. After the virus finds a PLC computer, the malware installed can update its code over the internet and start sending malicious commands to the controller which is connected with the PC. At the same time, false feedbacks are sent back to the main controller to make the operator unaware of the problem until the real physical destruction happens. After that, PLC producers such as Hitachi, Mitsubishi, and Siemens started working with antivirus producers to determine solutions for the inefficiencies in PLC systems. In other words, the discovery of Stuxnet malware opened up a way of redesigning secured PLC architectures[5]. The demonstrable system design partially follows the methodology of Stuxnet. Anyone monitoring the control system may have little clue about what is happening when watching the HMI display. Also, the affected devices are industrial standard, which means the attack can be applied to most fields.

C. *Water Heat Exchange System*

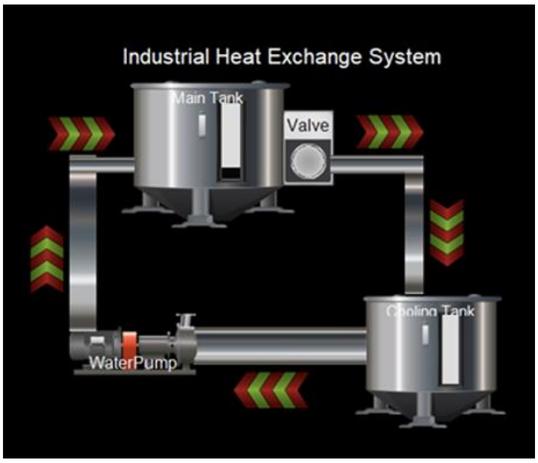


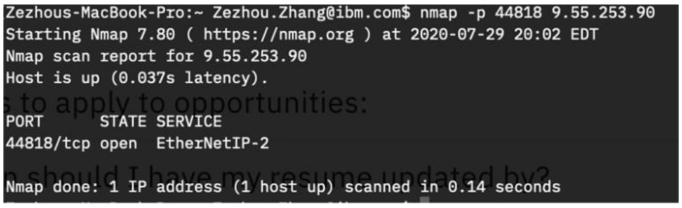
Fig. 2. Industrial Heat Exchange System in HMI

In the demonstrable design, a temperature sensor is used to measure the device in the field. When the temperature exceeds a certain threshold, it will trigger the water pump to pump cold water into the main tank to cool down the device. At the same time, the solenoid valve is open to drain the water out. The principle of water cooling for heat dissipation is not complicated. When the liquid contacts the cooling block, it takes away the heat generated by the hardware. Then the liquid with heat enters the cooling tank to cool down. Finally, it is pushed by the pump to push the cryogenic liquid to the cooling block again to complete the water circulation.

D. *PLC Memory*

Ladder logic functions allow PLCs to perform calculations, make decisions, and other complex tasks. They rely on the memory data stored inside the PLC that is divided into two files: data files and program files. Data files store information needed to carry out the user programs and are accessed through the ladder logic programs. The memory of the CPU stores the program files while also holding the status of the input/output and data values. Maliciously changing data files can have fatal impacts on the OT process that is running on that PLC. In a real-world scenario, wrong temperature values in a water control system may trigger the alarm or the pump. According to the MicroLogix 1100 reference Manual, modifying the data values stored in memory can be done on the web page that runs on PLC's web server. The other methods used in the demonstration are EtherNet/IP protocols and RsLogix programming software.

E. *EtherNet/Industrial Protocols(EtherNet/IP)*



```
Zezhous-MacBook-Pro:~ Zezhou.Zhang@ibm.com$ nmap -p 44818 9.55.253.90
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-29 20:02 EDT
Nmap scan report for 9.55.253.90
Host is up (0.037s latency).
s to apply to opportunities:
PORT      STATE SERVICE
44818/tcp open  EtherNetIP-2

n should I have my resume updated by?
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Fig.3. Nmap Result of PLC IP Address

The IP part of this protocol is the use of the Ethernet infrastructure in conjunction with the industrial protocol, which uses CIP layers and combines with TCP/IP or UDP to create a protocol that can be used to support data exchange and control applications. CIP stands for Common Industrial Protocol that is using a producer-consumer communication model. Each CIP object has attributes, commands, connections, and behaviors[6]. CIP includes an extensive object library to support general-purpose network communications, network services such as file transfer, and typical automation functions such as analog and digital input/output devices, HMI. The EtherNet/IP protocol is an adaption of CIP to allow CIP communications to be transported over standard Ethernet. In addition, the Programmable Controller Communication Commands (PCCC) protocol is the Rockwell protocol that provides legacy support for their older PLCs. MicroLogix 1100 only uses Port 44818 for EtherNet/IP protocol. When used with EtherNet/IP, the PCCC object processes PCCC messages encapsulated in CIP payloads through the use of "Execute_PCCC" CIP service[2]. In the demonstration, a crafted PCCC packet is sent to the port 44818 of MicroLogix 1100 PLC to trigger a Denial-of-Service Fault in the PLC, and only power-cycling the device and resetting can clear the fault.

III. RELATED WORK

A. *DoS Exploit*

ICS-CERT reported the vulnerability in the security advisory ICSA-17-138-03. Also, it identified some critical infrastructure sectors that are potentially vulnerable to this network DoS attack, i.e., Critical Manufacturing, Food and Agriculture, Transportation Systems, and Water and Wastewater Systems[7]. Francisco and his research teams, who discovered and reported this vulnerability when doing the fuzzing test, have given a detailed explanation on how to craft the PCCC packet to trigger the fault status[2]. After replaying his research for this attack, it turns out that this attack can successfully cause the MicroLogix 1100 PLC to enter a DoS condition.

B. *Pycomm*

Pycomm library is a package that includes a collection of modules used to communicate with PLCs. The ab_comm module is specifically made for Allen Bradley PLC with an SLC driver[8]. With the EtherNet/IP protocol, it can write and read from the data files in the PLC memory as long as the PLC is accessible online. This library is distributed under the MIT license. The source code is modified for the use of customized PCCC packets.

C. *Attacks via HTTP traffic*

In ICSA-13-011-03 report, MicroLogix 1100 and 1400 allows man-in-the-middle attackers to conduct replay attacks via HTTP traffic[9]. The built-in web server inside the MicroLogix 1100 is using HTTP digest authentication. which requires a multi-layer of MD5 hashing to encrypt the data. However, the nonce is implemented with the nonce values to prevent replay attacks from the PLC. In the demonstration, there are some characteristics of the MicroLogix 1100 FW 16.000 web server:

- No password Complexity Requirement
- 24-hour Lock time if receive 10 consecutive invalid authentication packets
- unchanged nonce value for authentication packets
- QoP (Quality of Protection) is exposed to indicate hashing mechanism

HTTP digest authentication is designed to be "one way", meaning that it should be difficult to determine the original input when only the output is known. However, If the password itself is too simple, it may be possible to perform a brute-force attack. The detailed exploiting process is explained in section V.

IV. System Implementation

In this section, the physical setup for the control system is illustrated and explained according to this OT architecture.

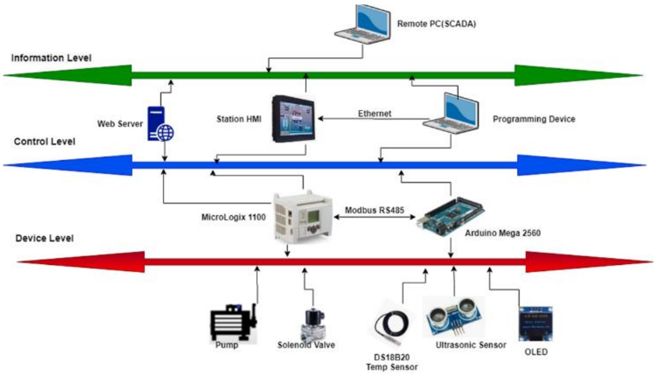


Fig. 4. OT Architecture

The control system setup is illustrated in Fig.5.

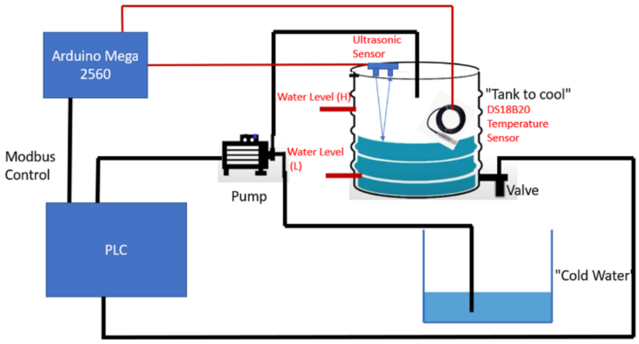


Fig. 5. Water Heat Exchange Control System

A. Device Level

DS18B20 waterproof temperature sensor is used to measure the device temperature on the field, and the ultrasonic sensor will be placed on the top of the water tank to measure the water level. OLED is used to indicate the real-time temperature and water level. These three components will be controlled by Arduino Mega 2560.

On the side of PLC, 12 Volts water pump and 24 Volts solenoid valve are placed to control the heat exchange process.

B. Control Level

Allen Bradley MicroLogix 1100 (1763-16BWA) PLC with firmware version 16.000 and Arduino Mega 2560 are used for controlling devices through ladder logic programming and C language. The PLC also communicates with the Arduino through Modbus RTU RS485 serial communication. The PLC acts as a Modbus Master and sends request to Arduino Slave for sensor data.

C. Information Level

On the information level, AdvancedHMI is an open-source HMI software that runs on Microsoft .Net Framework, which is used to operate and observe the whole control process. All the PLC and Arduino programming will be done on the PC. Also, the built-in web server will be used to display the data values on the web page. The last one is the remote PC that can be used to get access to the intranet through a VPN tunnel and run the python script to hack or fix the PLC. During the hacking process, HMI is also compromised to display the faked “normal” water level values, and for the comparison, the OLED can show the abnormal water level values in the control system after hacking happens.

D. Physical Setup

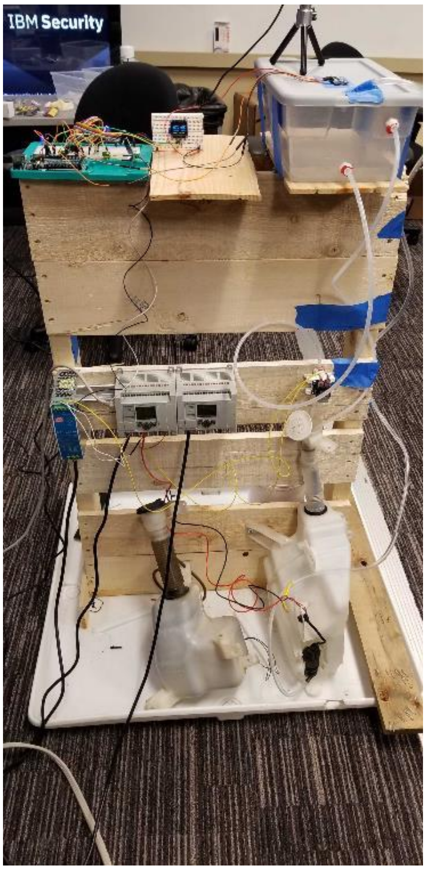


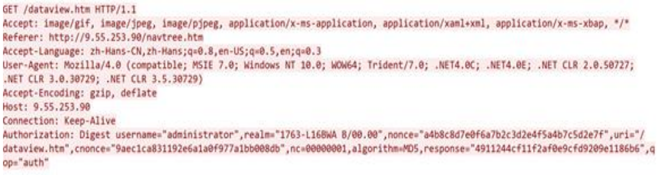
Fig. 6. Physical Setup of the Heat Exchange System

The base is made up of a windshield washer reservoir for the cooling tank and pump. On the top, Arduino and sensors are placed beside the main water tank. Two tubes are coming from the main tank to the cooling tank. The below one is connected through a solenoid valve, while the top one is to prevent overfilling the water tank. In one of the hacking scenarios, the water tank is going to be overfilled once the PLC is compromised. For safety issues, the hacking is considered done successfully if the tube on the top is going to drain the water, meaning the water level has exceeded the upper limit. Because in the real-world scenario, once the tank is keeping overfilled without having alerts or countermeasures, it may cause severe damage to the industrial equipment and operators along with the water tank.

V. HACKING IMPLEMENTATION

In this section, different attack vectors are presented to emphasize the significance of cybersecurity in ICS and show security weakness existing in the Allen Bradley MicroLogix 1100 PLC.

A. *Brute-force Web Server Authentication*



```
GET /dataview.htm HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/xaml+xml, application/x-ms-xbap, */*
Referer: http://9.55.253.90/navtree.htm
Accept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727;
.NET CLR 3.0.30729; .NET CLR 3.5.30729)
Accept-Encoding: gzip, deflate
Host: 9.55.253.90
Connection: Keep-Alive
Authorization: Digest username="administrator",realm="1763-L16BWA B/00.00",nonce="a4b8c8d7e0f6a7b2c3d2e4f5a4b7c5d2e7f",uri="/
dataview.htm",cnonce="9aec1ca831192e6a1a0f977a1bb008db",nc=00000001,algorithm=MD5,response="4911244cf11f2af0e9cfd9209e1186b6",q
op="auth"
```

Fig. 7. Authentication Packet Captured by Wireshark

The web server in the MicroLogix 1100 PLC uses the HTTP digest authentication method to encrypt the user password. However, the username and firmware version of PLC can still be easily revealed by sniffing the traffic between the web browser and web server. Attackers can do researches for the vulnerabilities of this type of PLC and its corresponding firmware version according to the captured information. From the Fig.7, the username is “administrator”, and the realm indicates the model of PLC used. From the model “1763-L16BWA B”, the attacker can infer that the MicroLogix 1100 series B is the PLC type used, and the default administrator account provided for this model is “administrator/ml1100”, according to the MicroLogix 1100 Programmable Controllers Reference Manual[10].

Besides, HTTP digest authentication is an application of MD5 cryptographic hashing with the usage of nonce values to prevent replay attacks. According to the definition from Wikipedia, the final response is a combination of hashing involving all the parameters captured in this packet[11].

- Because the algorithm directive's value is "MD5", then

  $$HA1 = MD5(username : realm : password)$$

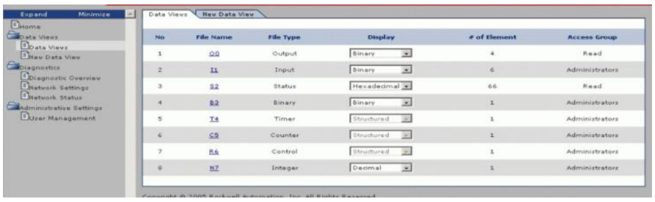
- Because the qop directive's value is "auth", then

  $$HA2 = MD5(method : digestURI)$$

- Because the qop directive's value is "auth", then compute the response as follows:

$$response = MD5(HA1:nonce:nonceCount:cnonce:qop:HA2)$$

The way to brute force the authentication is guessing the password to match the generated response with the actual response in the packet. Once it matches, the attacker can use this password along with the username to log into the webserver, which allows us to read and write the data values in the PLC memory. These values are associated with the output device such as pump and valve; therefore, by overwriting certain values into the memory location, it may trigger the pump or valve to start working when they are not supposed to. Also, account management can be modified when attackers have obtained administration privileges. He/she can potentially cancel the user accounts, change the password, or modify the permissions for each account.



No	File Name	File Type	Display	# of Element	Access Group
1	O0	Output	Binary	4	Read
2	I1	Input	Binary	6	Administrators
3	S2	Status	Hexadecimal	66	Read
4	B3	Binary	Binary	1	Administrators
5	T4	Timer	Structured	1	Administrators
6	C5	Counter	Structured	1	Administrators
7	R6	Control	Structured	1	Administrators
8	N7	Integer	Decimal	1	Administrators

Fig. 8. Data View of PLC on Web Page

To mitigate this vulnerability, Rockwell Automation provides following methods[9]:

Update firmware to the latest version for these supported features:

- When a controller receives two consecutive invalid authentication requests from an HTTP client, the controller resets the Authentication Counter after 60 minutes.
- When a controller receives 10 invalid authentication requests from any HTTP client, it will not accept any valid or invalid authentication packets until a 24-hour HTTP Server Lock Timer timeout.

It would be much safer to shut down the webserver by closing the port 80 dedicated to HTTP service. If the web server functionality is needed, Rockwell also recommends configuring user accounts to have READ only access to the product so those accounts cannot be used to make configuration changes.

B. *DoS Attack*

This DoS attack is a reimplementation of the vulnerability that Francisco and his research teams discovered, which was reported as ICSA-17-138-03[2]. Specially crafted Programmable Controller Communication Commands (PCCC) packet can be sent to controller, which could potentially cause the controller to enter a DoS condition. This fault can only be cleared by power-cycling the device and resetting through RsLogix programming software.

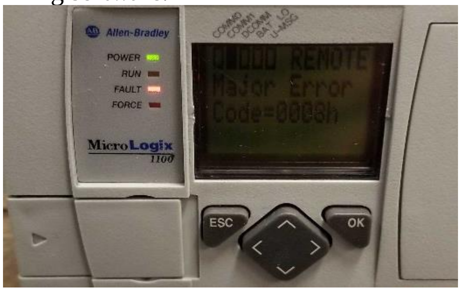
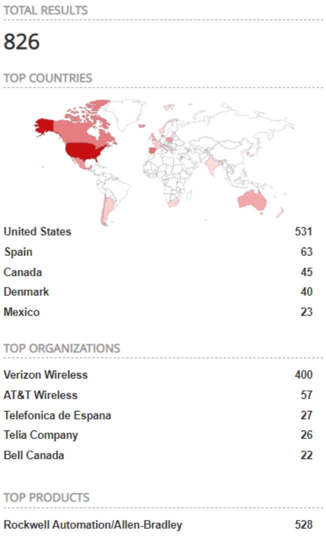


Fig. 9. Major Error Code on Affected PLC

Instead of doing the fuzzing test, a specially crafted Execute PCCC Service packet is directly sent to the PLC by accessing certain Data Files with an invalid File Type.

Any combination of File Number 0x02-0x08 and File Type 0x48 or 0x47 will trigger a Major Error (0x08), displayed in Fig. 9. To accomplish that, the source code of the pycomm module is modified, which was originally used to communicate PLC with PC through EtherNet/IP. A new file type “Z” is added to indicate the invalid packet with the specific file number and type.



TOTAL RESULTS

826

TOP COUNTRIES

United States	531
Spain	63
Canada	45
Denmark	40
Mexico	23

TOP ORGANIZATIONS

Verizon Wireless	400
AT&T Wireless	57
Telefonica de Espana	27
Telia Company	26
Bell Canada	22

TOP PRODUCTS

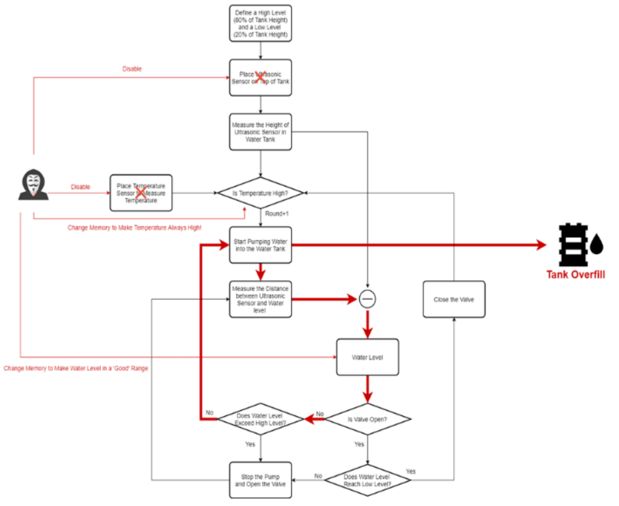
Rockwell Automation/Allen-Bradley	528

Fig. 10 Internet-exposed Port 44818 from Shodan

Shodan is a search engine for Internet-connected devices. From the Fig. 10, using search criteria 'Allen Bradley port:"44818" 1763' on the Shodan, there are hundreds of internet-exposed PLCs with open port 44818. Due to the vulnerability in EtherNet/IP protocol, this can potentially cause massive malfunctions. Considering this type of flaws across multiple products from Allen Bradley, the way of handling legacy products needs to be brought to the attention of vendors and manufacturers.

The way to mitigate this vulnerability is provided on ICSA-17-138-03: block all traffic to EtherNet/IP or other CIP protocol-based devices from outside the Manufacturing Zone by blocking or restricting access to Port 2222/TCP and UDP and Port 44818/TCP and UDP using proper network infrastructure controls, such as firewalls, UTM devices, or other security appliances[7].

C. Water Heat Exchange System Attack



Define a High Level (80% of Tank Height) and a Low Level (20% of Tank Height)
Disable
Place Ultrasonic Sensor on Top of Tank
Measure the Height of Ultrasonic Sensor in Water Tank
Disable
Place Temperature Sensor to Measure Temperature
Is Temperature High?
Round+1
Change Memory to Make Temperature Always High!
Start Pumping Water into the Water Tank
Tank Overfill
Measure the Distance between Ultrasonic Sensor and Water level
Close the Valve
Water Level
Change Memory to Make Water Level in a 'Good' Range
No
Does Water Level Exceed High Level?
No
Is Valve Open?
Yes
Yes
Stop the Pump and Open the Valve
No
Does Water Level Reach Low Level?
Yes

Fig. 11. Hacking Diagram for the Control System

In this subsection, a specific demonstrable control system is introduced about how it can be hacked and cause serious consequences. During the hacking process, when attackers disable the Modbus communication between Arduino and PLC, the data reading from the sensors are not going to be written into the memory of PLC. By changing the memory data values that corresponds to temperature and water level using pycomm, a faked temperature value will trigger the pump to work and start filling the water tank. However, because of the stop of the ultrasonic sensor, the water level will not be updated, meaning the valve will always see the water level in a “safe” range. Then, the water level will keep increasing until the tube on the top position of the water tank starts to drain the water out. This process will not stop until the presenter hit the “fix” button to make the control system back to normal. During the hacking, because of the faked value on the PLC memory, the HMI connected should also display the false values to trick the operator, making the attack being conducted in an unnoticeable way. In Fig. 11, the operator sees a normal range of water level (6cm) and relatively high temperature (23°C), meaning the water pump starts working. However, in Fig. 12, the water tank on the left-hand side and OLED on the right indicate a high water level (9cm) (close to the upper limit) and a normal temperature value (23°C).

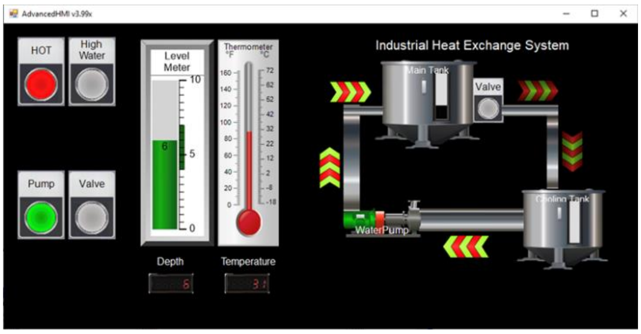


Fig. 12. The HMI View of the Control System

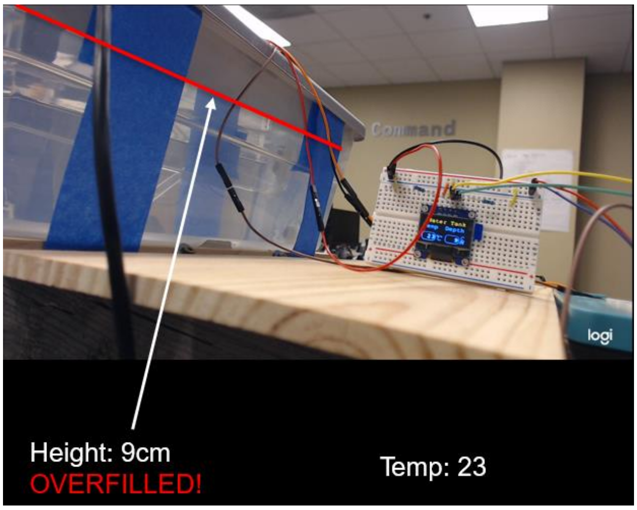
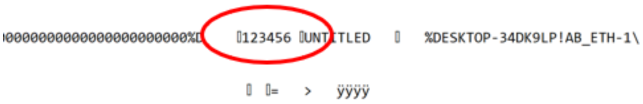


Fig. 13. The Actual Reading from OLED

In order to perform this type of attack, it requires attackers to have a certain knowledge of industrial infrastructure and memory location sets that are used to program the PLC. One of the ways to perform the reconnaissance is to upload the current program from PLC to see the functions. Some of the programming files may be password-protected to prevent unauthorized persons to modify the program and download it to PLC. However, it turns out the password is simply embedded inside the programming file. The attacker can patch some related critical bytes to reveal the password.



```
000000000000000000000000%D    123456 UNTITLED      %DESKTOP-34DK9LP!AB_ETH-1\

                                 =    >    ÿÿÿÿ
```

Fig. 14. The Embedded Password in Programming File

Also, for other versions of Allen Bradley controllers, they may have a master password used to clear all the protections. For example, it is widely known in the industry that a universal password, "ABUNLOCK", is for PLC-5 controller. Also, since the SLC controller requires a numerical password, and requires translation to numbers using the telephone keypad code; therefore, "ABUNLOCK" = 22865625. This works on SLC500, but not MicroLogix controllers[12].

The way to mitigate this kind of attack is to secure the network by creating DMZ, VPN tunneling, and restricting access to EtherNet/IP ports. DMZ will allow the network administrator to deploy an additional layer of security. This approach can prevent a threat been propagated to the whole network once it infects one partition of the network. Multiple DMZs are proved to be effective against large network architectures[5]. Also, multi-factor authentication is recommended when using the PLC programming software.

VI. Conclusion

In this paper, researchers have designed a demonstrable control system combining OT and IT to reveal the vulnerabilities of the PLC-based ICS environment. With the less relevance of the Purdue Model, there are multiple ways for attackers to take control of such PLC-based systems and perform harmful actions. It has been proved that the security of computers inside the enterprise intranet is so vital that any infected computer may cause the propagation of attacks because of the lack of security of communication protocols existing in the ICS. In order to mitigate such risks, multiple security methods, such as firewalls, DMZs, and restricting service, are provided based on corresponding vulnerabilities. However, the legacy products and protocols cannot make those approaches always promise complete protection for a PLC-based control system. With the development of IoT, providing adequate security and not degrading the performance excessively at the same time are the goals people need to reach in the future.

Acknowledgment

This research is supported by IBM X-Force Cybersecurity team in Atlanta, US. The paper is written by Zezhou, and the content of the paper is the result of joint work with his co-authors. A jointly authored paper is in preparation for public dissemination.

References

[1] “NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems”. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-205a. [Accessed: 04-Aug.-2020].

[2] Francisco Tacliad, Thuy D. Nguyen and Mark Gondree, "DoS Exploitation of Allen-Bradley's Legacy Protocol through Fuzz Testing", *Proceedings of the 3rd Annual Industrial Control System Security Workshop*, December 05-05, 2017.

[3] “Is the Purdue Model Still Relevant?|Automation World”. [Online]. Available:https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant. [Accessed: 05-Aug.-2020].

[4] “What Is Stuxnet? | McAfee”. [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html. [Accessed: 05-Aug.-2020].

[5] G. P. H. Sandaruwan, P. S. Ranaweera and V. A. Oleshchuk, "PLC security and critical infrastructure protection," *2013 IEEE 8th International Conference on Industrial and Information Systems*, Peradeniya, 2013, pp. 81-85, doi: 10.1109/ICIInfS.2013.6731959.

[6] “Common Industrial Protocol (CIP™) | ODVA Technologies”. [Online]. Available: https://www.odva.org/technology-standards/key-technologies/common-industrial-protocol-cip/. [Accessed: 05-Aug.-2020].

[7] “Rockwell Automation MicroLogix 1100 Controllers | CISA”. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSA-17-138-03. [Accessed: 05-Aug.-2020].

[8] “ruscito/pycomm: pycomm is a package that includes a...- GitHub”. [Online]. Available: https://github.com/ruscito/pycomm. [Accessed: 05-Aug.-2020].

[9] “Rockwell Automation ControlLogix PLC Vulnerabilities | CISA”. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03. [Accessed: 05-Aug.-2020].

[10] Allen Bradley. 2011. MicroLogix 1100 Programmable Controller Instruction Set Reference Manual. Milwaukee, WI.

[11] “Digest access authentication - Wikipedia”. [Online]. Available: https://en.wikipedia.org/wiki/Digest_access_authentication. [Accessed: 05-Aug.-2020].

[12] “TechTalk : RSLogix 500 – How-To Unlock PLC Logic – Xybenertics”. [Online]. Available: http://xybernetics.com/techtalk/rslogix500-lockedplclogic/. [Accessed: 05-Aug.-2020].