Obstructing PLC Operations through Modbus Command Manipulation

Nai-Yu Chen
M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Cheng-Ying He
M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, 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 701401, Taiwan

Chu-Sing Yang
Department of Electrical Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

E- mail: nychen@cans.ee.ncku.edu.tw, cyhe@cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw, csyang@ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw *
www.ncku.edu.tw

Abstract

Security vulnerabilities in Programmable Logic Controllers (PLCs) within Industrial Control Systems (ICS) using the Modbus/TCP protocol pose significant risks, particularly through stop-and-start command injection attacks that impact PLC operations and cause severe industrial consequences. Supported by Taiwan's National Science and Technology Council (NSTC) and the Water Resources Agency, this research establishes a cybersecurity testbed for water resource systems to investigate these threats. Unauthorized or forged commands are shown to manipulate PLC configurations and ladder logic diagrams, revealing critical weaknesses. Flowchart analyses and Modbus packet examinations highlight the risks and offer actionable insights into effective defense mechanisms for enhancing ICS security.

Keywords: Industrial Control Systems, Programmable Logic Controller, Modbus/TCP, Cybersecurity

1. Introduction

The integration of industrial control systems (ICS) with information technology (IT) has heightened the role of programmable logic controllers (PLCs) in automation [1]. However, this integration has also introduced significant cybersecurity risks. The Modbus protocol, designed for isolated industrial networks, lacks encryption and authentication, making it vulnerable in environments where Modbus TCP is widely used [2].

Recent cyberattacks, such as the 2022 Industroyer2 attack in Ukraine, have demonstrated these vulnerabilities [3]. Attackers exploited weaknesses in the Modbus TCP protocol to manipulate PLCs and disrupt critical infrastructure operations. Due to the protocol's lack of security features, such as encryption and authentication, it is highly susceptible to these types of attacks [4].

This study examines the CVE-2021-22779 vulnerability in PLC commands under the Modbus TCP protocol, involving an authentication bypass that allows unauthorized access via deceptive Modbus communication between engineering software and the controller. The vulnerability poses a significant security risk, enabling unauthorized command execution. Schneider Electric's TwidoSuite programming software was used to simulate various attack scenarios, demonstrating how system security can be compromised through manipulation of PLC configuration files and commands. Modbus TCP packets captured using Wireshark were analyzed to assess the impact of these

attacks on ICS operations. Additionally, UMAS, a protocol based on Modbus TCP and commonly used in Schneider Electric devices, shares similar vulnerabilities, further emphasizing the importance of robust security measures to protect PLC systems from unauthorized access and manipulation [5].

This research aims to highlight the cybersecurity threats posed by such attacks and provide data to support future defense strategies, especially in environments limited by the inherent vulnerabilities of the Modbus protocol, where enhancing ICS security is critical.

2. Background

2.1. The risks of PLC's misconfigurations

In ICS, the configuration and programming of PLCs are essential for system security. Manufacturers provide development environments like Siemens' TIA Portal and TwidoSuite for PLC configuration. When integrated into ICS via Ethernet, default settings can expose vulnerabilities, allowing attackers to infiltrate the network [6] and execute unauthorized operations on PLCs [7].

Attackers can exploit TwidoSuite to control a PLC by configuring "Programming Mode" and entering the PLC's IP address to connect to the network. Once connected, TwidoSuite reveals configuration details, including I/O statuses and Ethernet statistics. Attackers can then download and modify the PLC program, adjusting I/O settings, creating new control commands, or altering parameters like temperature sensors or time controllers. They can upload the modified program back to the PLC, leading to malicious code execution and system failures.

TwidoSuite also allows attackers to monitor and capture operational data, including command executions and variable changes, facilitating continuous monitoring for more advanced attacks. These steps highlight the risks of using tools like TwidoSuite without proper security measures, emphasizing the need for enhanced PLC security in ICS environments [8].

2.2. Using Modbus Protocol to Control PLC

Modbus TCP is a widely used protocol in industrial control systems (ICS) for communication between PLCs and devices over TCP/IP networks [9]. It uses a TCP connection to transmit packets containing function codes and data, with responses indicating success. Modbus TCP packets consist of the Modbus Application Data Unit (ADU) and the Modbus Protocol Data Unit (PDU). The ADU contains the TCP header, address, function code, data, and checksum. The TCP header manages the connection, the address identifies the target device, the function code specifies the operation, the data field contains the relevant information, and the checksum ensures data integrity during transmission [10].

PLCs have two modes: Operation mode for normal tasks and Development mode for updates. Development mode, while useful, poses risks such as unauthorized memory access or control logic changes.

UMAS (Unified Messaging Application Services), Schneider Electric's proprietary protocol, extends Modbus TCP with custom function codes for advanced tasks like memory manipulation and program updates. However, both protocols lack encryption and strong authentication, leaving them vulnerable to interception, replay attacks, and manipulation.

3. Exploiting UMAS Protocol vulnerabilities to disrupt PLC control

This study examines how attackers can exploit vulnerabilities in the UMAS protocol to interfere with PLC control, sending malicious packets to achieve unauthorized operations. To simulate these attack scenarios, a PLC and the TwidoSuite programming software were utilized. The experimental setup included an unencrypted PLC connected to a network switch, with the switch configured to mirror all traffic to an analysis computer for monitoring. Wireshark was employed to filter and analyze the captured UMAS protocol packets [11] (Fig. 1).

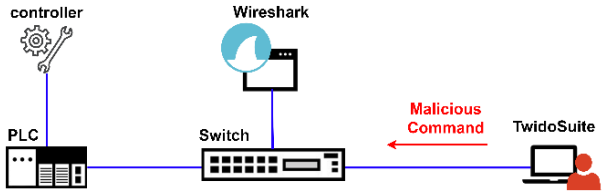

Fig. 1. PLC, Switch, Wireshark, and TwidoSuite Integration Architecture.

Using Wireshark, abnormal commands for stopping and starting the PLC, simulated through TwidoSuite, were intercepted to observe their impact on PLC operations. A packet with code 5a and function code 90 was detected. This function code, also known as "Unity Schneider," is a specialized command in Schneider Electric's systems used to execute stop and start instructions for the PLC [12].

Typical malicious commands include stopping and starting the PLC. The stop command, designed for emergencies, can be exploited to halt production or

damage equipment. Conversely, the start command can lead to unintended operations or production accidents (Fig. 2).

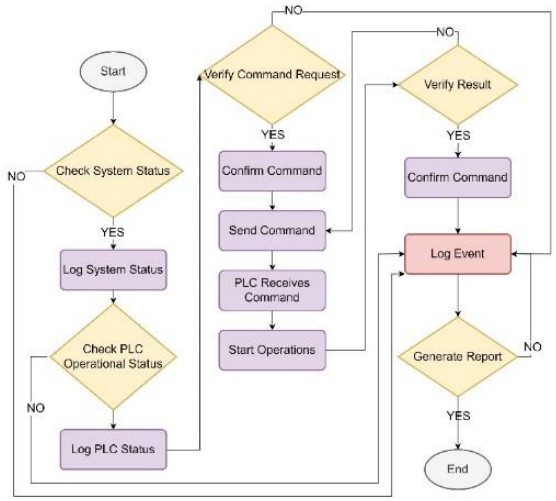

Fig. 2. The Flow Chart of PLC Stop Command Execution.

4. Experiments and Analysis

4.1. *Experimental Design*

The experimental design includes the following key steps:

1) PLC and Network Connection: Ensuring the PLC and switch are on the same network segment, with a mirror port routing traffic to the analysis computer, simulates an industrial control environment for monitoring PLC activities.

2) Malicious Command Simulation: Potential attack methods are simulated, including the modification or imitation of legitimate commands to send malicious instructions to the PLC. These actions are designed to disrupt or take control of system operations.

3) Packet Capture and Analysis: Wireshark is used to capture and analyze Modbus TCP packets from the PLC, focusing on data fields, function codes, and potential security risks.

4.2. *Experimental Results*

A detailed packet analysis was conducted on PLC communication, revealing that for the stopping PLC command, 213,229 packets were sent, with 212,840 successfully intercepted, resulting in a match ratio of 99.81%. Similarly, for the starting PLC command, 219,640 packets were sent, and 219,556 were intercepted, achieving a match ratio of 99.96%. These results indicate a high interception rate, demonstrating that the commands were effectively captured and potentially executed (Fig. 3). The analysis identified critical packet segments that require prioritization in the development of defense mechanisms and their associated potential attack methods (Table 1). To mitigate risks, recommended defense strategies include encryption to protect sensitive data, packet filtering to block unauthorized traffic, and anomaly detection systems to identify and respond to abnormal activities, thereby enhancing the overall security of the PLC system.

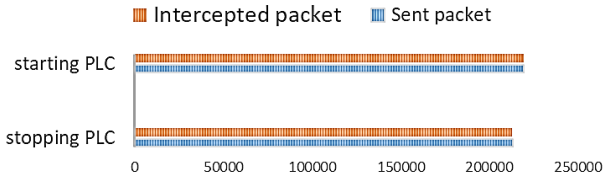

Fig. 3. PLC Command Packet Interception Comparison.

TABLE 1. Packet Header Segment Monitoring

Segment	Bytes	Possible attack methods
Ethernet Header Segment	0-13	MAC Spoofing, ARP Spoofing
IP Header Segment	14-33	IP Spoofing, IP Fragmentation Attack
TCP Header Segment	34-53	TCP Sequence Prediction, RST Attack, SYN Flood Attack
Data Segment	54-63	Command Injection, Data Manipulation

5. Conclusion

This study highlights the security risks of PLCs in ICS due to the lack of encryption and authentication protections. Simulated attack scenarios demonstrate that attackers can exploit PLC vulnerabilities to execute malicious actions, such as stopping or starting equipment, potentially disrupting processes or damaging machinery. Experimental results show that development mode enables attackers to manipulate configurations and ladder diagrams through unauthorized commands, while intercepting, simulating, or altering packets to send malicious instructions further compromises system integrity.

In addition to Modbus TCP, the study examines UMAS, a protocol based on Modbus TCP, revealing similar risks such as weak authentication and lack of encryption. Addressing these vulnerabilities requires measures like intrusion prevention systems, encryption protocols, and enhanced authentication. This research provides an empirical foundation for strengthening ICS security, with contributions to mitigating risks associated with both Modbus TCP and UMAS.

Acknowledgment

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 113-2634-F-006-001-MBK, and by the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) in Taiwan under contract number MOEAWRA1130243.

References

1. I-H. Liu, C.-C. Lai, J.-S. Li, C.-C.Wu, C.-F. Li, C.-G. Liu, “An Emulation Mechanism for PLC Communication

Features," Journal of Robotics, Networking and Artificial Life, Vol. 8, No. 3, pp. 175-179, 2021.
2. Wang, Yusheng et al. "Intrusion Detection of Industrial Control System Based on Modbus TCP Protocol," 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), 2017.
3. P. Kozak, I. Klaban, T. Šlajs, "Industroyer cyber-attacks on Ukraine's critical infrastructure," 2023 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 2023.
4. K.-M. Sudar, P. Deepalakshmi, P. Nagaraj, V. Muneeswaran, " Analysis of Cyberattacks and its Detection Mechanisms," 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Bangalore, India, 2020.
5. L Rajesh, P. Satyanarayana. "Detection and Blocking of Replay, False Command, and False Access Injection Commands in SCADA Systems with Modbus Protocol," Security and Communication Networks, 2021.
6. I-H. Liu, K.-M. Su, J.-S. Li, "The Security Issue of ICS: The Use of IT Infrastructure," Journal of Robotics, Networking and Artificial Life, Vol. 8, No. 1, pp. 29-32, 2021.
7. K.-M. Su, I-H. Liu, J.-S. Li, "The Risk of Industrial Control System: Programmable Logic Controller Default Configurations", ICS 2020, Tainan, 17-19, December, 2020.
8. N.-Y. Chen, P.-W. Chou, J.-S. Li, I-H. Liu, "A Case Study of Network-Based Intrusion Detection System Deployment in Industrial Control Systems with Network Isolation", ICAROB 2024, Japan, 22-25, February,2024.
9. Ferst, Matheus K. et al. "Implementation of Secure Communication With Modbus and Transport Layer Security protocols," 2018 13th IEEE International Conference on Industry Applications (INDUSCON), 2018.
10. G. B. M. Guarese, F. G. Sieben, T. Webber, M. R. Dillenburg and C. Marcon, "Exploiting Modbus Protocol in Wired and Wireless Multilevel Communication Architecture," 2012 Brazilian Symposium on Computing System Engineering, Brazil, 2012.
11. Rahman, Ayesha et al. "Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms," Int. J. Crit. Infrastructure Prot. 39, 2022.
12. S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by penetration testing using Wireshark," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), India, 2017.

Authors Introduction

Ms. Nai-Yu Chen

She is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Bachelor of BioBusiness Management, National Chiayi University, Taiwan in 2021. Her interests are ICS Security and Network-Based Intrusion.

Ms. Cheng-Ying He

He is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. He received his B.B.A. degree from the Bachelor of Information Management, National Taiwan University of Science and Technology, Taiwan in 2022. His interests are ICS Security and Network-Based Intrusion.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.

Dr. Chu-Sing Yang

He is a researcher in the Department of Electrical Engineering at National Cheng Kung University, Taiwan. He obtained his PhD in Electrical Engineering from National Cheng Kung University, Taiwan. His research interests include cybersecurity and network management.

Dr. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests are Cyber-Security, OT Security, and Wired & Wireless Communication. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).