Device's Operation Tracking using Blockchain in Industrial Control System

Chien-Hsin Wu
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, 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 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-Fen Li
Department of Finance, National Formosa University
No.64, Wunhua Rd., Huwei Township, Yunlin County 632301, Taiwan
E-mail: {chwu, ihliu,}@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw, chufenli@gmail.com*
www.ncku.edu.tw, www.nfu.edu.tw

Abstract

Many producing, monitoring and controlling needs are met by using programmable logic controllers. But there is no effective mechanism to audit PLC behavior. So this research designed a mechanism based on Blockchain for the purpose of effectively recording the commands and response actions received by the PLC. Due to the characteristics of the blockchain, the integrity of the data is also guaranteed..

Keywords: Cyber Security, Blockchain, PLC, ICS Security

1. Introduction

A programmable logic controller (PLC) is composed of an I/O module, that is, an input-output module, sensors, and actuators. In a PLC control system, the sensor can detect the status of an on-site switching signal (such as a photoelectric switch, a material position switch, etc.) or an analog signal (such as on-site temperature, on-site pressure, etc.). The I/O module transfers the signal from the sensor to the PLC, which is processed by the CPU. The processed result will be converted into a control signal and sent by the output module to the actuator, which performs operations on the controlled object.

Due to the PLC's core advantages of being both simple and easy, durable and trusted, dependability is a very important factor when the machine may result in thousands to millions of dollars in losses. Control engineers and technical personnel need to know that they can rely on the PLC and thus perform simple troubleshooting quickly when an error occurs.

* Corresponding author's E-mail: jsli@mail.ncku.edu.tw

PLC was originally only used for automation control and development; its application scenario was extremely close and could hardly be shared with any third party outside the industry network equipment; however, with the rapid development of the Internet and the Internet of Things, and the emergence of intelligent hardware, industrial PLC has become more accessible to the public in recent years. If the instructions were recorded, it would be possible to know when the problems occurred and how to improve them. Therefore, this paper will use blockchain to establish a decentralized anti-tamper system to record PLC instructions, so that if the device fails, the record in the blockchain can be checked for the first time and the original instructions can be obtained.

2. Background

In this chapter, we mainly discuss the current attacks and risks of the ICS (Industrial Control System). At the 2016 Black Hat European Security Conference, Ali Abbasi, a graduate student, and Majid Hashemi, a Quarkslab R&D engineer, proposed that a malicious attacker can destroy and manipulate physical processes managed by a programmable logic controller (PLC) without being detected.[1]

2.1. *Ethernet*

PLC and Ethernet communication is based on the traditional Ethernet communication mechanism, using Ethernet and TCP/IP protocol as the basis for communication, in any case to provide absolute support for TCP/IP communication. In order to meet the real-time requirements of automation, the real-time communication channel is optimized based on PLC B network layer, which reduces the time occupied by communication and improves the performance of automatic data refresh. In the process of communication, there have been attacks on PLC.[2]

2.2. *PLC's operating mode*

The attacker modifies the operating state of the OT device. To obtain permission, PLC has many operating modes that can control the user's state and the API access of the controller, as well as the choice of physical mode. The attacker may try to modify the operating state of the PLC through various means. Some devices provide application programming interfaces (APIs) to facilitate information transfer between developers or machines. Attackers also have the opportunity to execute specific functions or malicious attack instructions through APIs.[3]

2.3. *Malicious PLC attack*

One technique uses data that is not necessarily part of the normal static or offline project files to weaponize PLCS and enable code execution during project connection or upload. Through this medium of attack, the target is not a PLC, such as the notorious Stuxnet[4] malware that secretly changes PLC logic to cause physical damage. Instead, they hope to use the PLC as a fulcrum to attack the engineers who program and diagnose it and gain deeper access to the OT network. Notably, all of the vulnerabilities they found were in the engineering workstation software, not in the PLC hardware. In most cases, they add, the vulnerabilities exist because the software completely trusts the data from the PLC without having to perform extensive security checks.

2.4. *Proof of work*

Here we use POW's proof-of-work algorithm. While processing transaction data, each node continuously performs hash calculation and obtains a hash value less than the network target value, which becomes the nonce golden number. The network target value is what we call the difficulty value, which will also be adjusted continuously with the operation of the whole blockchain system. When a miner in the whole network hashes the nonce, he will publish his packaged block. After receiving the block verification block, other nodes will agree that this block has been connected to the blockchain and continue to carry out the next block packaging and hash calculation.[5]

3. System Architecture

This section provides an illustration of the proposed method and general framework. Some adjustments have been made to the traditional network configuration and verification mechanism to make the blockchain running in PLC more compatible.

3.1. *Network model*

We designed the architecture shown in Fig.1. to implement block chain on PLC execution. When PLC

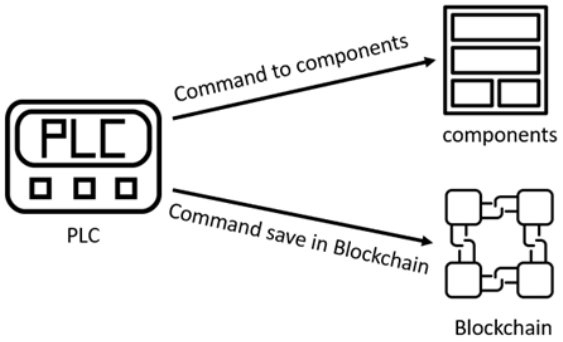

Fig. 1. System architecture.

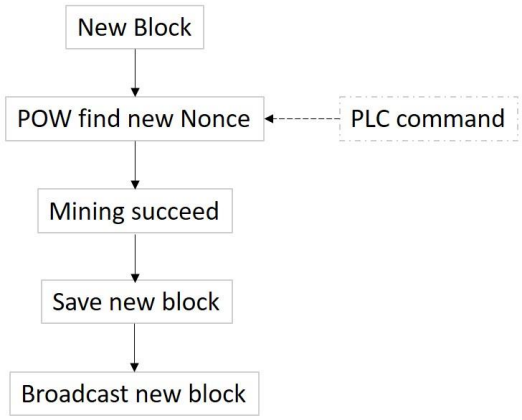

Fig. 2.Transaction Process

sends out instructions, the instructions will be connected in the block chain at the same time.

The model describes the operation of a PLC chain. When the instruction is completed, it is simultaneously transmitted to the block chain program, and the instruction is converted into input information in the block chain. After function conversion, the attached value will be generated into a nonce variable. We put the contents of the Modbus packet in the field "nonce" for transmission on the blockchain. Combined with the unchangeable characteristics of blockchain, information in PLC can be effectively managed and the transaction process can be recorded. If the transaction log is sealed in a block, the log contents are not easily changed.

3.2. *Blockchain-based transaction process*

During the chaining process, there are four basic elements: the hash value of the previous block, the transaction information, the nonce variable, and the hash of the current block. The set up is shown in Fig.2.

Step 1: PLC outgoing instructions, including gate switch and so on.
Step 2: When the instructions are sent out, they are also sent to the blockchain to share information.
Step 3: Overload the hash code function in the block, wrapping the information and the time it was obtained as a Nonce variable.
Step 4: Set the difficulty to get the hash value.
Step 5: Hash through the blockchain

4. Conclusion

Due to the evolution of time and technology, the attacks on ICS are becoming more and more diversified, and ICS network security has become a hot research topic today.

To ensure the reliability of ICS packet information during transmission, this paper uses the immutable characteristics of an emerging technology called blockchain to record the instructions of PLC packet transmission. If the system is attacked in the future, it can find the untampered records to see where the problem occurred.

Acknowledgment

This work was supported by the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) and the National Science and Technology Council (NSTC) in Taiwan under contract numbers 111-2218-E-006-010-MBK.

References

1. Abbasi A., & Hashemi M., “Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack”, Black Hat Europe 2016(pp. 1-35).
2. Wikipedia contributors. (2022, November 4). Ethernet. In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Ethernet&oldid=1120015826
3. ATT&CK for ICS - Execution(2).(2021) https://ithelp.ithome.com.tw/m/articles/10275404
4. Wikipedia contributors. (2022, November 14). Stuxnet. In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=1121937222

5. Ayokomi L, & Sonya H, "Consensus Mechanism in Enterprise Blockchain", 2019 IEEE International Conference on Intelligence and Security Informatics (ISI)

Authors Introduction

Ms. Chien-Hsin Wu

She was born in Tainan, Taiwan in 1999. She is acquiring the master's degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. She received her B.S. degree from the Department of Communication Engineering, National Taipei University, Taiwan in 2021. Her interests are Cyber Security.

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

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 wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.

Prof. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.