SUGISAKA MASANORI

Journal of Advances in Artificial Life Robotics
Vol. 3(4); March (2023), pp. 205–208
ON LINE ISSN 2435-8061; ISSN-L 2435-8061
https://alife-robotics.org/jallr.html

Research Article

Utilizing Blockchain to Monitor the Functioning of Devices in Industrial Control Systems

I-Hsien Liu[1], Chien-Hsin Wu[1], Jung-Shian Li[1], Chu-Fen Li[2]

[1]*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[2]*Department of Finance, National Formosa University, No.64, Wunhua Rd., Huwei Township, Yunlin County 632301, Taiwan*

ARTICLE INFO

Article History

Received 08 October 2022
Accepted 04 May 2023

Keywords

Cyber security
Blockchain
PLC
ICS security

ABSTRACT

Programmable logic controllers, or PLCs for short, is ubiquitous in the field of industrial automation. These devices are used to control and monitor a variety of processes related to production, ensuring that everything runs smoothly and efficiently. Unfortunately, there are currently no reliable means of verifying the accuracy and reliability of these devices, which can lead to serious consequences in the event of an error or malfunction. To address this issue, researchers are exploring the use of advanced technologies such as blockchain to provide greater transparency and security PLC operations.

1. Introduction

In control systems, a programmable logic controller (PLC) serves as a crucial device comprised of various components, such as an input-output module (I/O module), actuators, and sensors. Within the system, the sensors are responsible for detecting either a switching signal, which may involve a photoelectric switch or a material position switch, or an analog signal such as temperature or pressure from a given site. Subsequently, the I/O module proceeds to transfer the signal from the sensor to the PLC, enabling the central processing unit (CPU) to initiate the signal process. The output module then converts the processed signal into a control signal and dispatches it to the actuator. The actuator subsequently carries out a specific operation on the controlled object, marking a vital step in the overall control process.

In light of the Programmable Logic Controller's (PLC) foundational advantages, encompassing its straightforwardness, sturdiness, and dependability, the criticality of ensuring its reliability is amplified when the equipment involved holds the potential to cause significant financial losses, ranging from thousands to even millions of dollars. Maintaining a high degree of confidence in the dependability of the Programmable Logic Controller (PLC) is paramount for control engineers and technical staff, as it allows for seamless and expedient troubleshooting in the face of errors. The original design of the PLC revolved around its function as an automated control and development tool, with a highly circumscribed scope of application, primarily confined to industry network equipment. Consequently, the device's limited adaptability proved a significant obstacle to its wider utilization by external third-party entities, beyond the industry network's purview..; however, with the rapid development of the Internet and the Internet of Things, and the contingency of intelligent

Corresponding author's E-mail: jsli@mail.ncku.edu.tw, chwu@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, chufenli@gmail.com URL: www.ncku.edu.tw, www.nfu.edu.tw

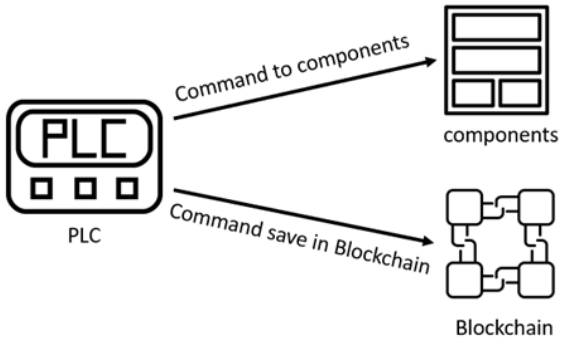

Fig. 1. System architecture.

hardware, industrial PLC has become more accessible to the public in recent years. In order to effectively identify and address issues, proper documentation of instructions can play a crucial role in enhancing performance. To achieve this, blockchain technology can be utilized to develop a decentralized anti-tampering system for Programmable Logic Controller (PLC) instructions. By recording these instructions on the block chain, any potential tampering or security breaches can be detected, with the original instructions retrievable from the unalterable blockchain ledger. This approach would provide a secure and trustworthy means of preserving the integrity and security of PLC instructions, mitigating the risk of tampering and related failures.

2. Background

In this chapter, we Chiefly 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 hostile attacker can destroy and manipulate natural operations managed by a programmable logic controller (PLC) without being detected [1].

2.1. *Ethernet*

Witness as Ethernet and TCP/IP protocols unite in a dance of communication, forming the very foundation upon which this technological marvel stands! In every conceivable circumstance, TCP/IP communication is fully supported, beckoning forth a world of seamless interconnectivity. Real-time communication for automation is optimized using the PLC B network layer, improving data refresh performance. However, malicious attacks on the PLC during communication have been observed, making ongoing defense and adaptation crucial [2].

2.2. *PLC's operating mode*

The perpetrator alters the operational status of the Operational Technology (OT) device. Behold, the insidiousness of the malefactor as they lay siege to the heart of Programmable Logic Controller (PLC) technology. Cunningly, they deploy a plethora of nefarious methods to manipulate the operational status of these machines, leaving chaos and destruction in their wake. Alas, in their devilish quest, they may exploit the portals of data exchange known as APIs - gateways that facilitate communication between machines and developers. Will we rise to the challenge and thwart the attacker, or fall prey to their treachery? Attackers also have the opportunity to execute specific functions or malicious attack instructions through APIs [3].

2.3. *Malicious PLC attack*

Exploiting Programmable Logic Controllers (PLCs) can involve using data that's not typically included in static or offline project files. This method can turn the PLCs into weapons, allowing for the execution of code 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. Their objective is not to directly attack the PLC itself, but to leverage it as a pivot point for targeting the engineers responsible for its programming and maintenance, in order to gain more extensive entry into the OT (Operational Technology) network. Researchers have discovered that all vulnerabilities in automation security were found in the engineering workstation software, not in the PLC hardware. This underscores the importance of securing not just the hardware, but also the software components of the system. Typically, the reason why vulnerabilities exist is due to the complete trust the software places in the data originating from the Programmable Logic Controller (PLC), rendering the software vulnerable to attack and eliminating the need for exhaustive security checks.

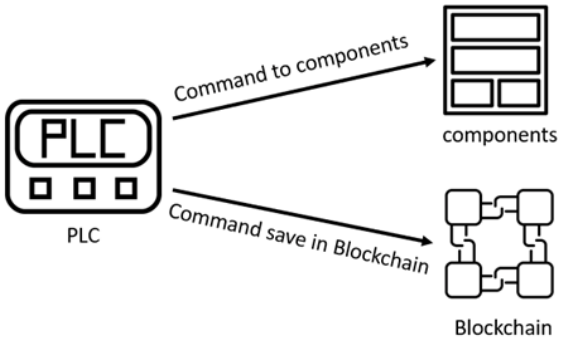

Fig. 2. System architecture.

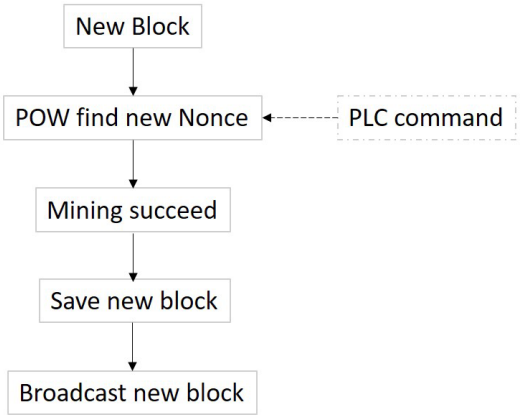

Fig. 2.Transaction Process

2.4. *Peer-to-peer*

In traditional web architecture, all resources are placed on the same server, and users who need to search the server. Peer to Peer (P2P) networks are all responsible for storing all or parts of all data. In addition to making requests to other IP addresses, they also need to be responsible for processing received requests, acting as both Client and Server [5].

3. System Architecture

This section provides an overview of the proposed approach and framework. Some adjustments have been made to the traditional network configuration and confirmation system to make the blockchain running in PLC more compatible.

3.1. *Network model*

The architecture we designed shown in Fig.1. to implement block chain on PLC execution. When the PLC sends instructions, they are connected to the block chain simultaneously.

In this model, the functioning of a chain of PLCs is outlined. As each instruction is executed, it is sent to the blockchain program in real-time and transformed into input data within the blockchain. The information contained within the Modbus packet is placed in the "nonce" field and subsequently transmitted onto the blockchain. By leveraging the immutable nature of blockchain technology, it becomes possible to effectively manage information stored within Programmable Logic Controllers (PLCs) and record the transaction process. If the transaction log is secured in a block, the log contents are not easily changed.

3.2. *Blockchain-based transaction process*

When chaining blocks together, four fundamental components are utilized, namely: the hash value of the previous block, transaction information, a nonce variable, and the hash of the current block. The set up is shown in Fig.2.

Step 1: PLC outlet instructions, including gateswitch and so forth.
Step 2: When an instruction is sent, they are sent to the blockchain as well to exchange information.
Step 3: Override the hash code feature in the block, wrap the information and 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

As time progresses and technology advances, the methods employed to attack Industrial Control Systems (ICS) are becoming increasingly diverse, thus making ICS network security a pressing research topic.To safeguard the integrity of ICS packet information during transmission, this paper proposes utilizing the immutable nature of blockchain technology to record the instructions for PLC packet transmission. This way, in the event of a future attack, unaltered records can be accessed to determine where the issue originated.

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. R. Gaeta and M. Sereno, "Generalized Probabilistic Flooding in Unstructured Peer-to-Peer Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 12, pp. 2055-2062, Dec. 2011

Authors Introduction

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. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University.

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. 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.

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.