RESEARCH PAPERS
FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

2021 Volume 29, Number 49

USE OF BLOCKCHAIN MECHANISMS IN PLC CONTROL AND SAFETY CRITICAL PROCESSES

Dušan HORVÁTH[1], Maximilián STRÉMY[1]

[1]SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA
ADVANCED TECHNOLOGIES RESEARCH INSTITUTE
ULICA JÁNA BOTTU Č. 2781/25, 917 24 TRNAVA
e-mail: dusan_horvath@stuba.sk, maximilian.stremy@stuba.sk
Received 6 May 2021, Accepted 13 May 2021, Published 24 November 2021

Abstract

In a few past years, a lot of cyber-attacks on industrial systems were accomplished. The main point of vulnerability of industrial control systems (ICS) is their connection to the Internet. Standard ICS rely on local solutions; however, with the revolution in the shape of Industry 4.0 concept, there are only a few industrial sectors with no connection to the global network. Some researchers have revealed critical vulnerability of the control systems. In this paper, we briefly summarize the current situation, and introduce our solution to the check of changes in PLC via other nodes in industrial network. The way how to do it is possible through using a checksum of actual code, and comparing with the checksums stored in other nodes.

Keywords

Blockchain, data integrity, ICS, security, Industry 4.0, PLC

INTRODUCTION

The concept of Industry 4.0 includes the technology like the Internet of Thinks (IoT), where the devices are connected to the Internet [1]. Everything connected to the Internet is endangered. The industrial production keeps growing [2], and the impact of industry on Gross domestic product (GDP) is enormous. In a few past years, critical cyber threats have occurred in industry [3]–[5], and some vulnerabilities on Programmable Logic Controllers (PLC) have been found [6], [7]. Industry depends on Industrial Control Systems (ICS); thus, it needs to use PLCs. The Ervurals predict [3], that the number of cyber-attacks will rise in the future, and their methods will be more and more sophisticated and complicated. It is clear, that it is absolutely necessary to build new strategies and security tools to secure production and ICSs in general. One of the possibilities and candidates to implement it is blockchain technology [8]–[10].

PRELIMINARIES

Blockchain is an autonomous P2P-like network with no central authority required [11]. It consists of networking, data management, cryptography and mechanisms providing all necessary operations to satisfy functional requirements [12]. Nowadays, blockchain is a technology used in many branches, e.g. logistics, finance sector, Internet of Thinks (IoT), transport, energy sector, computer sciences and many others [11]–[14]. Blockchain is a decentralized database independent from any trusted authority; all decisions are performed by the blockchain consensus mechanism.

Three types of cryptographic keys can be described: secret (private) key, public key and shared key. Secret key is a cryptographic key which is connected to only one node, and it is important to provide decrypting messages and signing data. It is also important to generate a public key that is a derivate of the secret one. Public key is a publicly known key, and is used for encrypting messages (data) and authenticated signed data. Shared key is a cryptographic key used in a communication between two nodes. The key is known by both sides of the communication, and is usually created while the connection is being established. Key exchange is a technique to change the shared key between communicating sides. Some of the well-known algorithms based on public key cryptography e.g. the Diffie-Hellman key exchange algorithm have been developed.

Symmetric cryptography uses one key to both, encrypt and decrypt data. A few secret ciphers are known, such as One-Time Pad (OTP, stream cipher), the Advanced Encryption Standard (AES, block cipher) or The Data Encryption Standard (DES, block cipher).

Asymmetric ciphers use a pair of keys; one key is used for data encryption and the other one is used for data decryption. A well-known asymmetric cipher is based on RSA (Rivest, Shamir, and Adleman). It is the only known reasonable candidate trapdoor permutation scheme [15].

The cryptography includes hash functions. The functions create fix-sized strings of data from input data string of variable length, and are very important and used in many applications, such as message authentication, message integrity, digital signatures and so forth [16].

In Simatic safety F-PLCs (Fail-safe PLC), there is a possibility to use F_PROG_SIG tag, which is a part of F_GLOBDB Data block [17]. There is also possibility to exchange data between networked PLCs, e.g. by using shared Data blocks. Nowadays, industrial networks are built on the industrial Ethernet, what leads to a quick data exchange and extension of industrial networks by new possibilities via implementing the Ethernet mechanisms (e.g. routing, hi-speed communication…) [18].

STATE OF THE ART

Aloui proved [19], that injection of malicious code into PLC is not too difficult to perform. In case the ICS network is connected to the Internet (in any way), it can cause fatal consequences. Cyber threats from the past few years (e.g. STUXNET [4], Steel mill attack [3], [5]) show vulnerability of the ICS connected to the Internet. Critic security vulnerability in S7-1500 PLC was revealed by the researchers at the Tel Aviv University and the Technion Israel Institute of Technology [6], [7], which confirms an importance of researching new security mechanisms. For more information on attacks, see e.g. [3]. The important fact is, that injection of malicious code is an unnoticed stealth in many cases. That means, the consequences of changing the program can be found out after long time, e.g. when production speed is lower than expected, because malicious code slowed down the motion speed of devices in production lines.

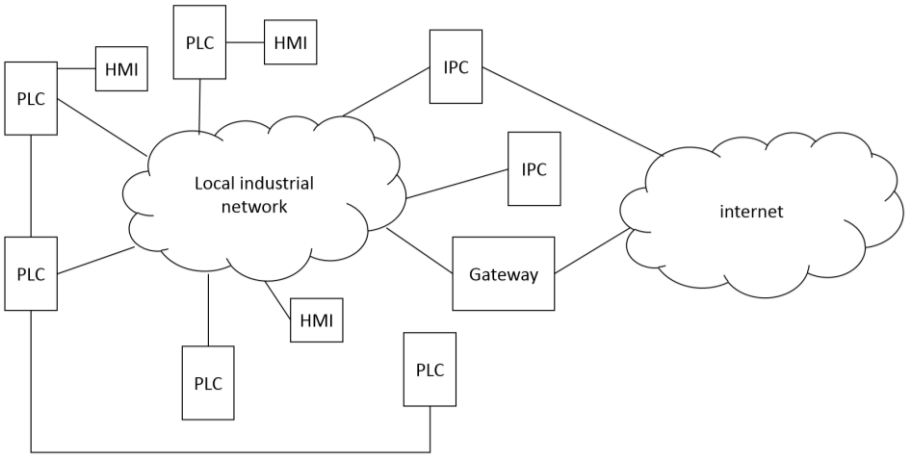

Fig. 1 *Industrial network topology – simplified example (PLC – programmable logic controller, IPC – industrial computer, HMI – human machine interface)*

The ICS are obviously based on the Master-Slave concept, which gives an attacker great power when controlling the Master node. In such a case, the attacker controls the whole system, and, for example, program can be modified.

Focusing on industrial technologies, especially on ICS, Mao et al. introduced their blockchain-based solution, which targets to network security in ICS [9].

Controller's programs can be checked by the CRC (cyclic redundancy check) functions (e.g. F-signature in Siemens PLCs [20]). This CRC information can be used to compare changes in PLC. If there is no match between actual program data, CRC signature and previous signature, the system can detect it and the service (e.g., operator, maintenance…) can be warned.

Cryptography is one of the columns of blockchain technology. It combines data protection, authentication, digital signature and so forth.

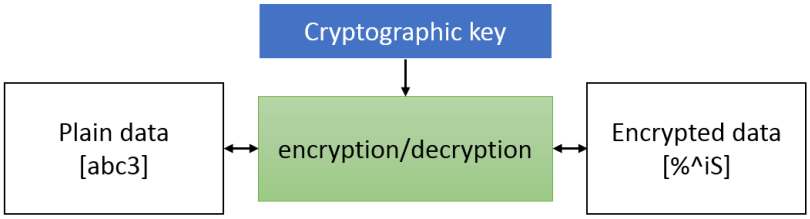

Fig. 2 *Data protection with symmetric cipher*

Basic data protection is based on a password scheme. The concept is implemented in many of the known PLCs. This protection is not secure enough, as e.g. Sara Bitan showed in her presentation [7], when the researchers could use vulnerability in the S7 protocol.

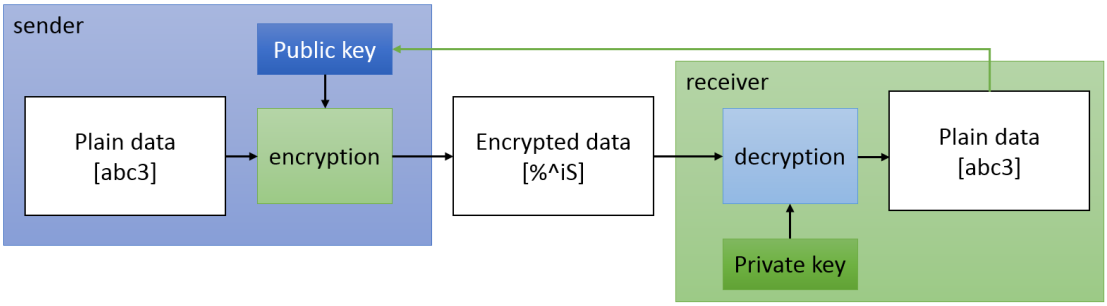

Fig. 3 *Data protection with asymmetric cipher*

SOLUTION PROPOSAL AND METHODS OF FUTURE RESEARCH

Industrial control systems are based on the Master-Slave centralized architecture. On the other hand, blockchain is based on a decentralized concept. In the first case, a decision, "what to do" is performed in the following way: a "slave" listens and "master" commands. In the other case, a decision "what to do" is performed based on the consensus of all nodes in the blockchain network. When combining the two approaches, we can get a mixed architecture, where the system is controlled strictly by the Master-Slave method in the real time (what is absolutely necessary), and some tasks (program modification etc.) are evaluated by the blockchain networks, and then performed.

Nodes share their F-signature of data stored in the multiple nodes provided by shared DB inside all of them. All these nodes provide a comparison of the actual signature with the stored one, and, in case of change, a subroutine is called to execute warning (Figure 4). Shared data block (SHARED_DB) can be accessed for reading only by all nodes in network. All PLCs can provide a comparison of signatures, and if a mismatch is found (by changing any of signatures), the system can perform an alert. An acceptance of changed signature can be validated by an operator, and, after the operation, the new signature can replace the old one.

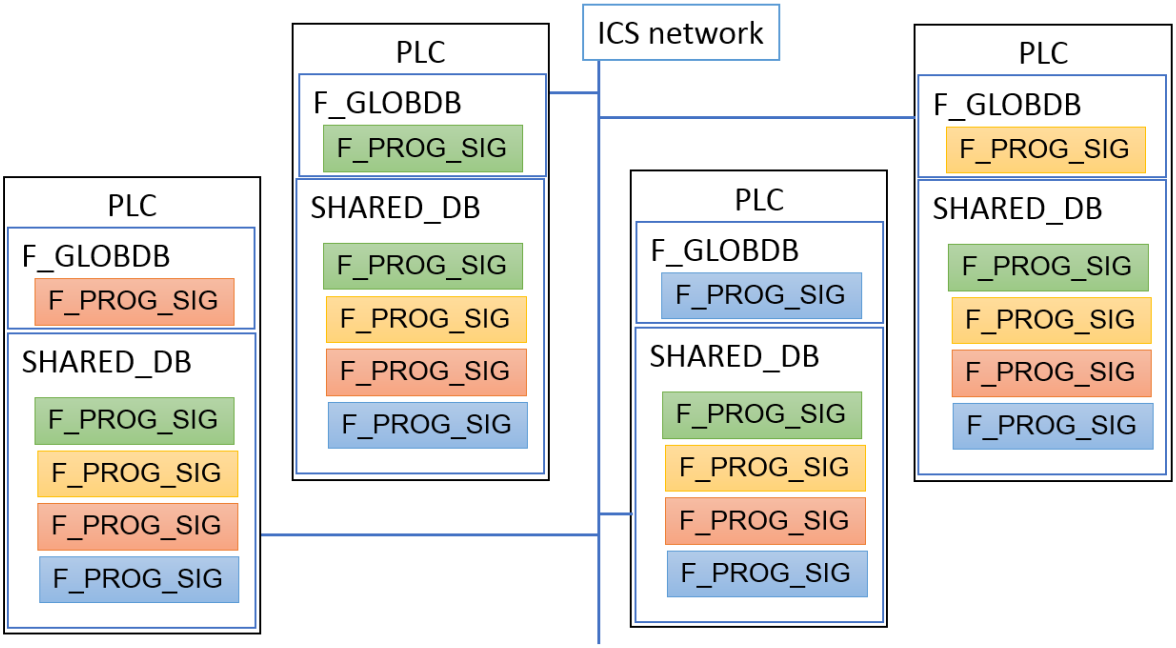

Fig. 4 *Signature distribution among PLCs (Safety PLC S7 example)*

An advantage of this concept is that it can be evaluated by an experiment by using a virtual PLC (e.g. PLCSim), which is a cheaper solution than the one built on physical PLC. Since it is not necessary to check signatures during every cycle, we propose to use a Time-of-day (ToD) Interrupt Organization Block (OB10 to OB17) for instruction programming. The ToD OB can be set to be called e.g. once an hour; this scheme will not affect the cycle time too often. More about cycle time can be read in [21].

CONCLUSION

Digital age requires digital tools. Almost all industry world-wide is built upon network technologies. One of the technologies is blockchain, a decentralized database network based on the idea of peer-to-peer concept. In the close past, the world has known new types of cyber-

attacks on industry. Every single system connected to the world-wide network is potentially in a risk. Protection of data and the industrial networks (which were, by the way, conceived as isolated networks without the Internet connection) is a hot priority for many of organizations. With rapid implementation of the IoT technologies into industrial sector in these years, the new challenges appear. Use of ICS and adaptation to the new technologies is necessary to be successful in the competitive struggle. On the other hand, there are a lot of vulnerabilities inside the known systems, and thus there is also the need to research new technologies to protect data. Our solution, briefly described in this paper, provides a "springboard" to the further research aimed at the ICS protection.

Acknowledgement

This publication was supported by the Operational Program Research and Innovation for the project: "Scientific and Research Centre of Excellence SlovakION for Material and Interdisciplinary Research", code of the ITMS2014+: 313011W085 Project co-financed by the European Regional Development Fund.

References

[1] TAY, S., CHUAN, L. TE., AZIATI, A., AHMAD, A. N. A. 2018. An Overview of Industry 4.0: Definition, Components, and Government Initiatives. *J. Adv. Res. Dyn. Control Syst.*, Vol. 10, p. 14.

[2] YARDENI, E., JOHNSON, D., QUINTANA, M. 2021. *Global Economic Briefing: Industrial Production*. p. 21.

[3] ERVURAL, B. and ERVURAL, B. *Overview of Cyber Security in the Industry 4.0 Era*. 2018, pp. 267–284.

[4] BAEZNER, M. and ROBIN, P. 2018. *Stuxnet*.

[5] LEE, R. M., ASSANTE, M. J. and CONWAY, T. *ICS Defense Use Case. 2014.* Accessed: May 04, 2021. [Online]. Available at: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

[6] Researchers compromise secure Siemens PLC in cyberattack 1," *eeNews Europe*, Aug. 09, 2019. https://www.eenewseurope.com/news/researchers-compromise-secure-siemens-plc-cyberattack (accessed May 04, 2021).

[7] BITAN, S. 2020. Rogue7: *Rogue Engineering Station Attacks on Simatic S7 PLCs.* Accessed: May 04, 2021. [Online]. Available at: https://www.cs.technion.ac.il/~biham/Workshops/Cyberday/2020/Slides/sara-bitan.slides.pdf.

[8] PAN, X., WANG, Z. and SUN, Y. 2020. Review of PLC Security Issues in Industrial Control System. *J. Cyber Secur.*, **2**(2), pp. 69–83. doi: 10.32604/jcs.2020.010045.

[9] MAO, M., XIAO, H. 2018. Blockchain-based Technology for Industrial Control System CyperSecurity. Presented at the 2018 International Conference on Network, Communication, Computer Engineering (NCCE 2018). China, Chongqing. doi: 10.2991/ncce-18.2018.151.

[10] ANDRIAN, H., BUDI KURNIAWAN, N., and SUHARDI, S. 2018. *Blockchain Technology and Implementation : A Systematic Literature Review*, p. 374.

[11] PANDA, S. K., ELNGAR, A. A., BALAS, V. E. and KAYED, M. 2020. *Bitcoin and blockchain: history and current applications*.

[12] XU, X., WEBER, I. and STAPLES, M. 2019. Cost, in *Architecture for Blockchain Applications*. Springer Nature Switzerland AG, pp. 175–195.

[13] F. ul HASSAN et al. Blockchain And The Future of the Internet: A Comprehensive Review. *ArXiv190400733 Cs*, Nov. 2020, Accessed: Apr. 22, 2021. [Online]. Available at: http://arxiv.org/abs/1904.00733.

[14] SANKA, A. I., IRFAN, M., HUANG, I. and CHEUNG. R. C. C. 2021. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Comput. Commun.*, **169**, pp. 179–201. doi: 10.1016/j.comcom.2020.12.028.
[15] BONEH, D. and SHOUP, V. 2020. *A Graduate Course in Applied Cryptography*. Stanford University.
[16] SOBTI, R. and GANESAN, G. 2012. Cryptographic Hash Functions: A Review. *Int. J. Comput. Sci. Issues*, **9**, pp. 461–479.
[17] Siemens, "SIMATIC Safety - Configuring and Programming." Accessed: May 05, 2021. [Online]. Available: https://support.industry.siemens.com/cs/document/54110126/simatic-industrial-software-simatic-safety-configuring-and-programming.
[18] KIM, D. S. and TRAN DANG, H. 2019. An Overview on Industrial Control Networks. In: *Industrial Sensors and Controls in Communication Networks: From Wired Technologies to Cloud Computing and the Internet of Things*, D.-S. Kim and H. Tran-Dang, Eds. Cham: Springer International Publishing, pp. 3–16.
[19] Nidhal BEN ALOUI. *Industrial Control Systems Dynamic Code Injection*, presented at the GreHack, Grenoble, FRANCE, Nov. 2015, Accessed: May 04, 2021. [Online]. Available: https://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Industrial Control Systems Dynamic Code Injection.pdf.
[20] Siemens, *Safety Programming Guideline for SIMATIC S7-1200/1500*. Accessed: May 04, 2021. [Online]. Available: https://support.industry.siemens.com/cs/ww/en/view/109750255.
[21] Siemens, *Cycle and response times.* Accessed: May 05, 2021. [Online]. Available: https://cache.industry.siemens.com/dl/files/558/59193558/att_895996/v1/s71500_cycle_and_reaction_times_function_manual_en-US_en-US.pdf.

ORCID

Dušan Horváth 0000-0003-4138-5966
Maximilián Strémy 0000-0003-2918-0714