The Study of Security Issues for the Industrial Control Systems Communication Protocols

Qu Wanying [a]，Wei Weimin [b*]，Zhu Surong [c]，Zhao Yan

Changyang Road, Yangpu District, Shanghai University of Electric Power, Shanghai, China

[a] melosy_qwy@163.com；[b] wwm@shiep.edu.cn；[c] 2628299182@qq.com

* Corresponding author：Wei Weimin(1970-), The main research directions are the digital forensics, information hiding, industrial control information security. This work was supported by the Natural Science Foundation of Shanghai (15ZR1418500)

Abstract: With the depth integration of informatization and industrialization and the rapid development of the Internet, the industrial control systems (ICS) communication protocols' risks have become increasingly prominent. This paper firstly analyzes the security issues of the current mainstream industrial control systems communication protocols, such as Modbus, DNP3 and OPC. Then the security recommendations are raised against such issues. The safety of the whole industrial control network can be improved by improving the security of communication protocols.

Keywords: ICS protocols; Modbus; DNP3; OPC; security

Introduction

Industrial control systems(ICS) is an important infrastructure of a country involved in electric power, energy and many other areas of people's livelihood. ICS has been using complex proprietary communication protocols, such as Modbus, Profibus, DNP3, IEC, ICCP, OPC etc, these communication protocols complete the ICS data exchange and acquisition, business monitoring and many other important functions. However, with the depth integration of informatization and industrialization and the rapid development of the Internet, which security issues have become increasingly prominent.

In June 2014, Havex virus was found by the security vendor f-secure. It took advantage of social engineering to send phishing emails that contain malicious spyware to the target users, and after the users download software that tampered, the malicious spyware code is automatically installed to the OPC client for data via OPC protocol [5]. This shows that the security of the ICS protocols is very worrying.

This paper firstly analyzes the security issues of the current mainstream ICS communication protocols, such as Modbus, DNP3 and OPC. Then the security recommendations are raised against such issues.

Analyses of Security Vulnerabilities of ICS Communication Protocols

ICS network architecture can be divided into three parts [11], business network, and regulatory network and control systems, as shown in Figure 1. The core components include supervisory control and data acquisition systems (SCDA), distributed control systems (DCS), programmable logic controllers (PLC), remote terminal (RTU), intelligent electronic devices (IED) and interface technologies that ensure all components can communicate[12]. Information transfer between these components use dozens of specialized industrial control communication protocols, such as Modbus, DNP3, OPC, IEC60870-6, and so on. There is a big difference between the communication protocols and TCP/IP protocol [2], so the security threats they face are not the same, the following analyses for Modbus, DNP3 and OPC.

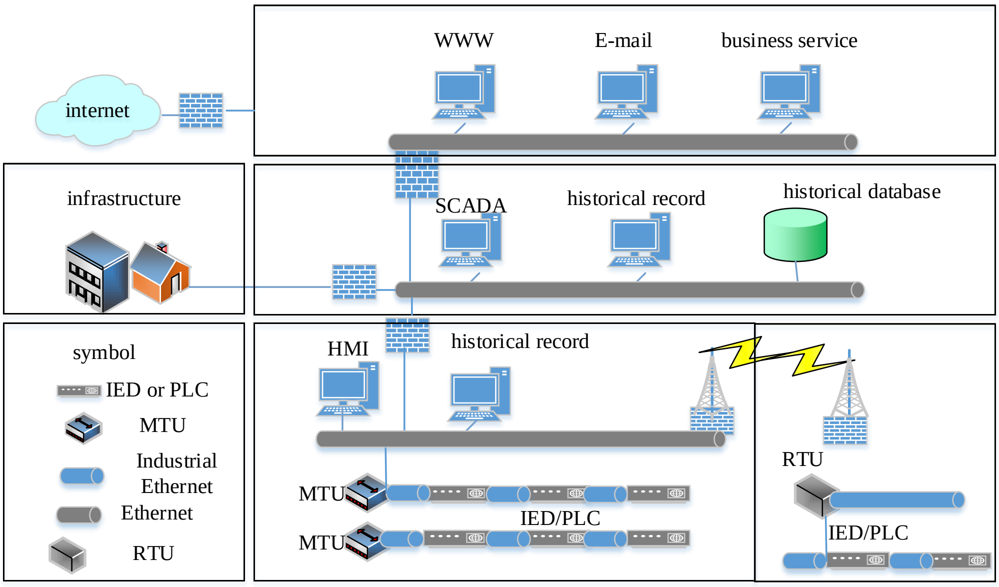

Figure 1 The system framework of ICS

The Security Issues of Modbus

Modbus protocol was invented in 1979 by Modicon. It is the world's first truly bus protocol for industrial. With the development of technology, Modbus protocol also appeared in many variants, such as those based serial link, MODBUS RTU, MODBUS ASCII, MODBUS PLUS and MODBUS TCP based on Ethernet [1]. Through these protocols, between the controllers, the controller via the network (Ethernet) and other devices can communicate. Since Modbus are truly open protocols in the manufacturing and infrastructure environment, widely supported by the industry. Modbus standard defines the protocol layers of the OSI 1/2/7, as shown in Figure 2.

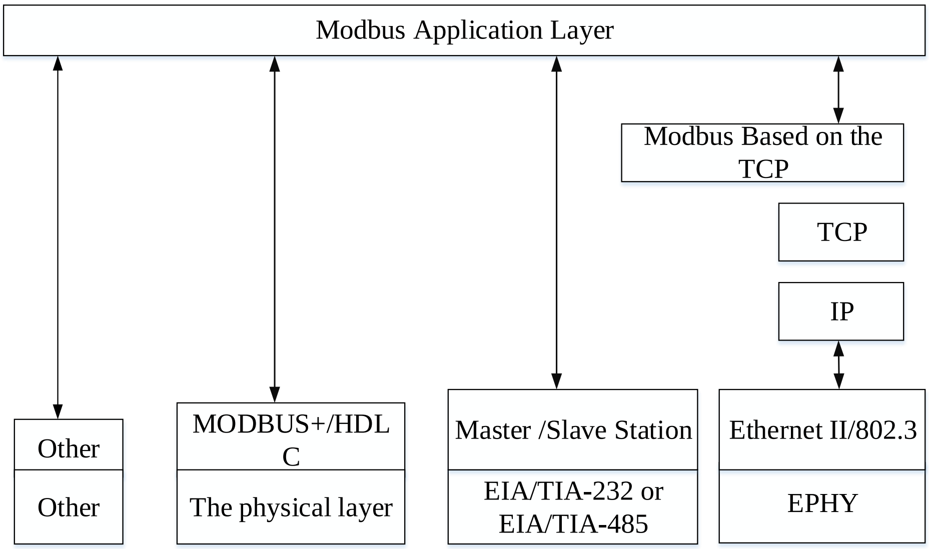

Figure 2 The stack of Modbus

Modbus Protocol uses master-slave structure, and provides communication between devices that are connected to a different type of client/server. However, due to only considered its implementation, efficiency and reliability when the protocol was designed and didn't take into account security issues. So there are several security issues:

Lack of certification: In Modbus protocol communication process, there is no constraint certification. The attacker can set up a Modbus communication session only needs to intercept messages and get a legitimate address, and then disrupt the whole or part of the control process.

Lack of authority: Various privileged actions need authenticate users with different privileges to complete so that you can reduce the probability of false operation. At present, the Modbus Protocol don’t have role-based access control, there is no classification of users and divide of the user's permission. All these can lead to arbitrary user perform any function.

Lack of encryption: Encryption can guarantee that the information is not illegal access by third parties. During the Modbus Protocol communication process, the address and commands all use plaintext, so that data can easily be captured by an attacker.

The Security Issues of DNP3

DNP3.0 was drafted in July 1993 by Canada HARRIS Company. It is a distributed network protocol that based on IEC 870-5 standard architecture, and it is widely used in North America and China. There are also multiple protocols, such as DNP3 serial link and Ethernet. The reference model of DNP3.0 is similar to the ISO-OSI model. As shown in Figure 3.

Application Layer	Application Layer
Presentation Layer	
Ession Layer	
Transport Layer	
Network Layer	
Link Layer	Link Layer
Physical Layer	Physical Layer
ISO Reference Model	DNP3 Enhance performance model

Figure 3 DNP3 and ISO-OSI model

DNP3.0 mainly runs between the master and slave devices, such as RTU, IED and control station. DNP3.0 protocol is an open standard, so DNP3.0 protocol packet structure and data format is open. They did not consider too much security during design the DNP3.0, so in the process of communication, DNP3.0 protocol packet is easy to intercept, monitor, and modify, which greatly reduce the security of communications network [3]. Currently its main security threats are:

Middle attack: Data is transforming in the master station and slave station, intruder access to industrial control systems without the knowledge of the station, intercept the data, get equipment address of the current bus, then acts as main station or slave station of a system and send error messages to legal equipment, so that the system will not work[1].

Denial of service attacks: Relative to the request-response pattern of the Modbus, DNP3 add active reporting mode, but at the same time, this model also increases the possibility of loopholes. For example, slave station can send data to the master station without its permit, and this will increase the chance of a denial of service attack.

In a denial of service attack, an intruder enter the network, intercept and monitor normal message for the master station address, then acts as a station sending mass unsolicited messages, so make the master station too busy dealing with these pointless messages and other data cannot be processed, which will paralyze the system.

Hacking: The address and commands of DNP3.0 are transmitted in plaintext, so it’s easily capture and analysis. This does not cause harm to the system itself, but can cause leakage of important data.

The Security Issues of OPC

OPC Protocol is designed for process control of object linking and embedding (OLE), which works in client/server mode, and provide server the necessary parameters through remote procedure call (RPC). It has applications in many fields of industrial networks, such as historical records within the database data, data collection and monitoring, and so on. But now a report from security researchers shows that there are some serious problems in the standard:

OPC Server does not use a fixed port number [6]: For most communication protocols that use a single standard port, it will be able to better protect the client and the server by setting the firewall. But for the OPC Protocol, in communication, the client first need to query the server to obtain TCP port numbers needed for communication, and then connect to the server with the port number. In the process, the port number obtained by the OPC server randomly allocated dynamically, it is impossible to predict in advance. So, when using traditional firewall protection OPC server, it must allow a large range port number link between OPC client and server, which reduces the security of the firewall.

Therefore, at present, most OPC servers are running in a case without any firewall, making it vulnerable to attack from malware and other security threats [4].

OPC basic protocol are vulnerable to attack: The past few years, attacks from viruses and worms on the network protocol is growing, although due to test and patch of the operating system continues to improve and this influence has waned, a large number of worm attacks against security of OPC systems.

The Security Measures of ICS Communication Protocols

At present, the studies on the safety use of ICS communication protocols generally divide into two directions, one is how to avoid the incorrect protocols use, and the other is how to address security issues in design and description of protocols. This article concerns the latter, trying to make some targeted prevention recommendations to improve the protocols itself and its environment.

Security Protections of the Modbus

Combining with the use of Modbus Protocol and the security of its research in the industry, recommend the following security measures for the Modbus Protocol:

Increase authentication function: You can design an authentication type Modbus protocol, which can enhance the authentication function of Modbus protocol by using the Encrypt function and the hash chain, so that an attacker cannot masquerade as the host. It also uses a compression function to reduce the storage size of data [8].

Use a white environment: Different from traditional "blacklist", the "white" refers to only trusted devices, messages, and software are allowed to access the system. This method is through a collection and concentration analysis, develop a legitimate communication rules and classification of data stream, to identify information access system is legitimate.

Use Tofino technology: Tofino industrial safety solutions is a security platform build by a unique hardware and software, it can achieve zone isolation, deep inspection, communication control and real-time alarm functions to protect industrial control systems networks from attacks and destruction.

Different from traditional IT firewall, Tofino is specially designed for industrial environmental control network security. Therefore, even if a hacker or a virus through the main enterprise firewalls, they will also face the professional security equipment [3].

Security Protections of the DNP3

Compared with the Modbus request-response mode, DNP3 add active reporting mode, which increases the possibility of loopholes, so recommend the following security measures for the DNP3 Protocol:

Increase public-key authentication mechanism: This method is used to verify the legitimacy of the user, to overcome the "man in the Middle" attack.

User's public key authentication mechanism is to assign each user a pair of keys, which call the public key and private key, the private key is kept by the user, while the public key is open to all [7]. If the user can prove them hold the private key, and then prove his identity.

When used as an identity authentication, users will use its private key as an encryption key, encrypt the data required for the verifier, and then passed them to the verifier, and the verify decrypt the data based on the user previously provided public key in order to verify that the information is sent by the user, and then authenticate the user's identity.

In order to prevent eavesdropping, encrypt the transmitting message: Encrypt the codes in the packet header of the link layer and application layer can prevent eavesdropping effectively.

Use depth protection system: Depth protection system includes the technology of firewall and intrusion prevention technology.

ICS firewall must have the status analysis function in addition to traditional firewall functions, which can track all data, analysis and maintenance of the state, improve the accuracy and reduce the workload, so that can meet the real-time performance Claim. In addition, industrial control systems firewall must be able to support professional industrial protocols.

For intrusion prevention technology, the researchers have devised a statistical-based intrusion detection system [9]. Its statistical model can divide the network traffic into normal or abnormal in order to detect whether the device access system are security.

Security Protections of the OPC

The Havex viruses found in 2014 was through malicious spyware code into OPC clients and then access to data through OPC protocol. Therefore, it’s urgent to resolve the OPC agreement security problems. Following are recommended several measures for the OPC Protocol:

Use OPC security variants (OPC-UA): The integrated OPC UA data encryption capabilities comply with international safety standards. It provides a guarantee for the Internet and corporate network remote access and data sharing, communication between the client and the server; OPC UA delivery data that are encrypted and it can achieve the security control for communication connection and data [9]. This new variant of security can guarantee reliable delivery of original equipment to MES, ERP system.

Take other security measures: OPC server should be isolated to only partition that contains only authorized devices and adopt standard of depth defense strategy; use authentication technology that is the originator of all communication requests must go through rigorous identity certification, and only after authentication request are allowed; all content of the communication must be encrypted [10].

Conclusions

In this paper, we analyzed the security problems of three mainstream and widely used communication protocols in ICS, and then proposed the corresponding security measures for their shortcomings, which has the practical significance for reduce the security risks. Security strategies presented in this article can solve safety problems in ICS communication protocols to some extent, but it must refer to the actual use of different industries environmental for break through the limitations of each security policy.

Reference：

[1] Dong, J., D.M. Nicol and Y. Guanhua. An event buffer flooding attack in DNP3 controlled SCADA systems[C]. Proceedings of the2011 Winter Simulation Conference,2011. Phoenix, AZ. P2614-2626

[2] Fu Ge，Zhou Nianhong，Wen Hong. The Communication Protocols Security Research of Smart Grid Industrial Control System[J]. Information Security and Technology, 2014

[3] Hao Xin，Zhou Feng，Chen Xi. The Security Analysis and Research of DNP3.0 of SCADA System[J]. Industrial Technology Innovation, 2014, 6（1）

[4]http://wenku.baidu.com/link?url=GuARdWzhrGqO5hj1-Y86Z9n1a-tPv8GYTNN0BHvnBoobG SAzOzi48uZZHWG1A2uIsiId042IBAs9uql1TFQg_bUnIbS1SJmf0-RoKShS8Ru

[5] Li Hongpei, Yu Yang, Hu Chaolian. Industrial Control System and Its Security Study [R]. NSFOCUS.2012

[6] Liu Zhengan. Industrial OPC Communication Security Solutions[J]. The Academic Papers of the 10th Annual Meeting of China Petroleum and Chemical Industry Automation [C], 2011

[7] Majdalawieh, M.A., Security framework for supervisory control and data acquisition (SCADA) [D]. George Mason University. 2006. P84

[8] Peng Yong，Jiang Changqing，Xie Feng. The advances in information security of Industrial control systems. Journal of Tsinghua University, 2012，52（10）

[9] Roosta T，Nilsson D，Lindqvist U，et al. An intrusion detection system for wireless process control system[C].The 5th IEEE International Conference on Mobile Ad Hoc and Sensor System. Atlanta，USA：IEEE Press，2008:866-872

[10] Song Shigui. Tofino technology is applied to implement industrial OPC communications security solutions [J]. Heilongjiang Science and Technology Information, 2014（21）

[11] Sun Limin. The Industrial Control Systems Security from Internet[R].Institute of Information Engineering of Chinese Academy Sciences, 2014, 11

[12] Xiang Dengning, Ma Zengliang. Industrial Control System Security Analysis and Solutions[J]. Information Security and Technology, 2013,4（11）