ISSN: 2414-1895
DOI: 10.6919/ICJE.202002_6(2).0005

Application of Fuzzing in Security Testing of Industrial Control Network Protocols

Rui Zhang, Guanyu Zhang*

Shenyang Jianzhu University, College of Information and Control Engineering, Shenyang, 110168, China.

*945816869@qq.com.

Abstract

In the test of the security and robustness of industrial control protocols, there are multiple test methods, such as black box test, white box test, and gray box test. However, the industrial control system is complex and changeable, and the transmission protocols are diverse. It is difficult to achieve unified testing with one method. As a black-box test method, fuzzy test has strong practicability and can solve this problem to a certain extent. This article will explain the main characteristics of industrial control protocol testing, and introduce the related research work of fuzzy testing applied to industrial control protocol testing. Finally, the future research directions of fuzzy control of industrial control protocols are forecasted.

Keywords

Fuzzing, Industrial control protocol, Vulnerability mining.

1. Introduction

All manuscripts must be in English, also the table and figure texts, otherwise we cannot publish your paper. Please keep a second copy of your manuscript in your office. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question.

The application range of industrial control systems involves various industries in industrial production, including power, commerce, defense, food, communications, public health facilities, energy and chemical industries, etc. These industries are inseparable from the normal operation of industrial control systems. In recent years, with the proposition and implementation of industrial-related strategic measures such as "Made in China 2025" and "Internet of Things", industrial manufacturing has received more and more attention from national development. These strategic measures use cyber-physical systems to improve the overall manufacturing Level, prompting China to gradually transform from a manufacturing country to a manufacturing country[1].

Since its birth, the industrial control system has gone through three phases: CCS (Centralized Control System), DCS (Distributed Control System), and FCS (Fieldbus Control System)[2]. With the development of industrial automation, industrial control systems have gradually integrated with the Internet, and have changed from a traditional relatively closed and stable environment to a more open and changeable environment. This greatly expands the system structure and improves the efficiency of data sharing. But at the same time, the accompanying information security problems have become more and more serious[3]. Because traditional industrial control systems are relatively closed and dedicated, they pay more attention to functionality at the beginning of the design, and they have insufficient consideration of security issues. Many key infrastructure control systems have few protective measures against accidents or malicious attacks. Especially with the extension and development of Internet technology in the field of industrial control, the number of open interfaces of industrial control systems has greatly increased, and they have been exposed to the Internet excessively. As shown in Figure 1, the security situation of industrial control systems in recent years is not optimistic[4].

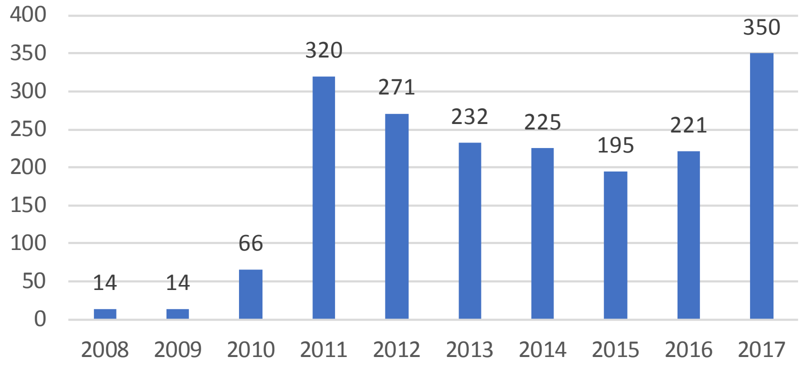

Fig. 1 Increasing number of industrial control safety incidents

As the information transmission carrier in the industrial control system, the industrial control protocol is the breakthrough that is most easily used by attackers. Therefore, the security of Industrial Ethernet is critical. According to the ISA99 reference model proposed by the American Instrument Association[5], the network of industrial control systems can be abstracted into a five-layer structure model as shown in Figure 2.

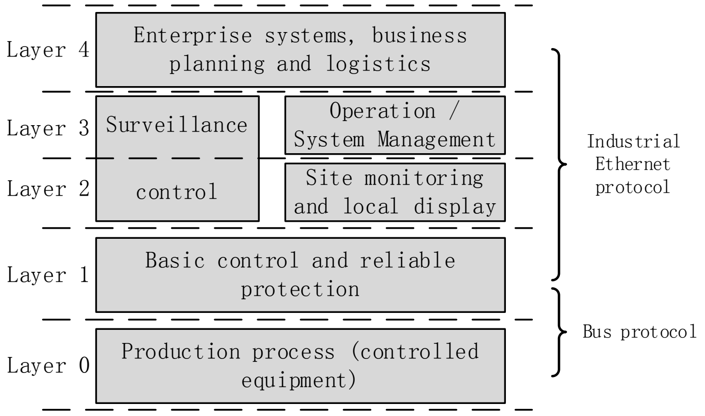
Layer 4
Enterprise systems, business planning and logistics
Layer 3
Surveillance
Operation / System Management
Layer 2
control
Site monitoring and local display
Layer 1
Basic control and reliable protection
Layer 0
Production process (controlled equipment)
Industrial Ethernet protocol
Bus protocol

Fig. 2 Five-layer reference model of industrial control system

Layer 0: Process layer

This layer is the various controllers, sensors, actuators and other equipment connected on-site in the industrial control system. It belongs to the physical space in the entire model and includes most of the physical equipment in the system.

Layer 1: Basic monitoring layer

This layer implements functions including sensors and operating physical processes. PLC, DCS, RTU, etc. are all devices in this layer.

Layer 2: Monitoring control layer

This layer is responsible for monitoring tasks in the system and controlling the production process. It mainly includes human-computer interaction interface, production data collection and storage, and monitoring and control status.

Layer 3: Operations Management

The operation management layer is mainly responsible for managing the workflow required for production, including operation/system management, generation scheduling, and system function guarantee.

Layer 4: Enterprise system layer

The enterprise system layer is a systematic management organization layer, which is mainly responsible for organizing the organization to manage business-related activities required by industrial production. Generally, it is completed by conventional computer technology.

In the five-layer structure model of the industrial control system, it can be seen that the communication between the various layers is mainly carried out through the industrial Ethernet protocol and the bus protocol. Industrial control protocols generally work between the first layer of equipment and the second, third, and fourth layers. The data transmission between common devices in the first layer, such as various controllers such as PLC and DCS, and other layers, needs to be completed by the bus control protocol used by the system. Common protocol types are Modbus, CANBUS, IEC101, etc. The agreements in question mainly refer to these agreements. The introduction of this article mainly introduces the basic concepts of industrial control safety and the network model of industrial control system. The subsequent chapters will mainly introduce the characteristics of fuzzy testing and its application in industrial control protocol testing, and analyze its advantages and disadvantages. Finally, the possible future development direction is prospected.

2. Fuzzing technology introduction

As early as the 1880s, some software engineers have been using software like "fuzzy testing" to test software, the most famous of which is the testing tool called The Monkey[6]. The tool quickly and randomly sends various inputs to the test target continuously, such as random keyboard input, mouse click and drag, and so on. Security testing at this time is still in its infancy and has not even tested related concepts. In the 1990s, due to the outbreak of large-scale and widely deployed buffer overflow attacks, people gradually realized the importance of security testing, and gradually added syntax testing and other related testing links in the software development process.

With the increasing importance of security testing, fuzzing, as a simple deployment and highly portable fuzzing method, is gradually favored by testers. The concept of fuzzing was first proposed by Professor Barton Miller of the University of Wisconsin. He used a tester to test the robustness of UNIX applications in his course on advanced operating systems and named the tester FUZZ. The fuzzer has begun to take its shape. Barton Miller believes that if we treat the program as a complex finite state machine, then all we have to do is traverse the state space randomly to find undefined states, which will cause the program to fail. Hang or crash.

After the concept of FUZZ was proposed by Barton Miller, fuzzing began to develop gradually, and gradually improved, as shown in Figure 3 is the general process of fuzzing.

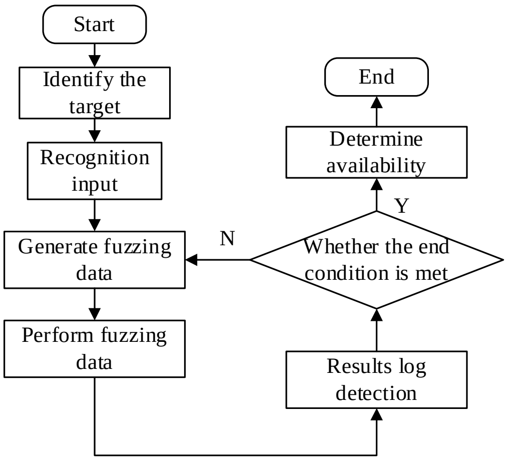

Fig. 3 The general process of fuzzing

As the fuzzing technology matures, various fuzzing test suites have gradually appeared. In 1999, the University of Oulu's secure programming team was influenced by the University of Wisconsin research team and earlier years of grammar testing, and launched the PROTOS project[7]. The project is mainly to solve the tedious testing workflow in traditional testing, as well as coordination and repair of vulnerability mining, and it is expected that the security research results will be transplanted to software and other devices in the later stage. This project has developed corresponding free fuzzing test suites for multiple interfaces, such as WAP-WSP, WMLC, HTTP-reply, SNMP, etc., among which SNMP has the most extensive impact. Since then, fuzzing has developed rapidly and has gradually become an indispensable test method in security testing.

In 2002, Dave Aitel developed the famous fuzzing framework SPIKE using C language[8]. The framework provides a set of interfaces that allow efficient development of network protocol fuzzers, allowing security developers to quickly develop usable protocol fuzzers. In addition, as the framework is licensed under the GNU GPL open source, after subsequent modifications, the SPIKEfile tool appeared to implement fuzzing of file formats and expand the scope of application.

The Peach fuzzing framework[9], which was subsequently released in 2004, is also an open source fuzzing framework developed using Python. The biggest feature of this fuzzing framework is the flexible architecture organization and high code reuse rate. The test components in Peach can be used flexibly, and some components support user customization, which greatly improves the use scenario of the framework. The test objects cover file formats, ActiveX, network protocols, APIs, etc.[10].

3. Research results of Fuzzing in industrial control protocol testing

During the development of fuzzing test, its excellent portability and applicability have gradually been favored by industrial control safety researchers. In addition to open source and business-related testing tools, there are also relevant theoretical workers who conduct related research on fuzzing and its application in protocol testing.

Artemios G. Voyiatzis et al. Designed a fuzzer[11]. The fuzzer adds a detection phase during the test, which is mainly used to detect the functional information of the target under test, and it is expected to adjust the attack vector and use this As a guideline for testing, to reduce the randomness of fuzzing, the tester hit a denial of service vulnerability using only a small number of test cases; in[12], Greg Banks et al. The disadvantage of poor support for protocol fuzzing is to design a flexible security-oriented network protocol fuzzing tool that can effectively identify noise problems during network protocol testing, allowing testers to describe the various states of the protocol and obtain Messages that need to be generated in each state. In addition, the tool also provides vulnerability category detection, enabling testers to find vulnerabilities faster; Ruilian Zhao proposed a new method to automatically generate test cases from the output domain[13], using a neural network to create a model instead of the software under test, using The genetic algorithm searches for the model input, and finally can realize the fully automatic generation and prediction of test cases; Byres uses the attack tree modeling method to analyze the vulnerability of a communication system of an industrial control SCADA system based on the Modbus protocol stack[14]; Lai Yingxu[15]and others used fuzzy concept to introduce the concept of mutation factor, which is the vulnerability characteristics of industrial control system, to generate the use case data required for Modbus / TCP protocol testing, and to determine the validity of the use case by bypass monitoring In the end, fuzzy testing was proved to be effective in the testing of industrial control protocols. In order to solve the problem of low use case coverage and unable to accurately evaluate the test results, Tu Ling et al. Proposed protocol deformation and dynamic characteristics in paper [16]. Parallel mixed test case generation method, which improves the use case coverage while reducing Results and vulnerability reporting rates[16]. Zhang Yafeng and others proposed state-based fuzzy control technology for industrial control protocols, and designed a test sequence generation algorithm based on protocol state machines, which solved the problem that protocol interaction states, test methods, and detection methods were not considered in previous protocol tests. A higher vulnerability hit rate and target coverage[17].

The fuzzy test started from the initial random test and gradually developed to become one of the commonly used test methods in the testing field. In recent years, it has been cross-fused with other fields, adding research results in intelligent optimization algorithms and artificial intelligence, and gradually applied In a wider field. After years of development, the fuzzy testing of industrial control protocols has gradually realized automation and intelligence. With the continuous deepening of researchers, the safety testing of industrial control protocols has become more efficient and sound, and the security testing system has been gradually improved.

4. Summary

After years of development and improvement, Fuzzing has gradually become one of the most commonly used testing technologies by security testers. With the rise of related emerging technologies such as the Industrial Internet of Things, fuzzing tests have gradually played their role in the security testing of industrial control protocols. However, there are certain shortcomings in traditional fuzzing tests, such as the difficulty in catching anomalies, the complexity of the industrial control environment, and the difficulty to implement, which cannot meet the testing requirements of typical industries and private networks. This paper deeply analyzes the conventional application scenarios of fuzzing, and combines the industrial control network environment to analyze the problems and deficiencies of the fuzzing test of the industrial control protocol. The main fuzzing tools and research results are analyzed in detail.

References

[1] ZHANG Yuqiang, GAO Shiwei, WANG Fu, et al. Review of Research on Industrial Control System Security Technology[A]. Chinese Association of Automation. Proceedings of the 2018 China Automation Conference (CAC2018)[C], 2018: 6.

[2] XIONG Qi, PENG Yong, YI Shengwei, et al. Survey on the fuzzing technology in industrial network protocols[J]. Journal of Chinese Computer Systems, 2015, 36(3):497-502(in Chinese).

[3] WEI Qi. Review on Information Security of Industrial Control Systems[J]. Telecom Power Technology, 2019, 36(05):225-226.

[4] SANGFOR, Cyber Security Situation Insights Report. 2019-01[EB/OL]. (2019-02-28),[2019-11-25]. http://www.sohu.com/a/298534561_244641

[5] Peng Yong, Jiang Chang-qing, Xie Feng. Research progress of the security technology for industrial control system[J].Tsinghua University Journal of Natural Science, 2012, 10:1396-1408.

[6] Kargén, Ulf, Shahmehri N. Turning programs against each other: high coverage fuzz-testing using binary-code mutation and dynamic slicing[C]// Joint Meeting on Foundations of Software Engineering. ACM, 2015.

[7] Ari Takanen, Jared DeMott, Charlie Miller. Fuzzing for Software Security Testing and Quality Assurance[M], Artech House Print on Demand, 2008.6:23-24.

[8] Aitel D. The advantages of block-based protocol analysis for security testing[J]. Immunity Inc, 2002.

[9] Peach[EB/OL].[2019-12]. http://peach.tech/.

[10] H. Zhao, Z. Li, H. Wei, et al. "SeqFuzzer: An Industrial Protocol Fuzzing Framework from a Deep Learning Perspective," 2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST), Xi'an, China, 2019, pp. 59-67.

[11] VOYIATZIS A G, KATSIGIANNIS K, KOUBIAS S, et al. A Modbus/TCP Fuzzer for testing internetworked industrial systems[C]. 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). IEEE, 2015.

[12] Banks G, Cova M , Felmetsger V, et al. SNOOZE: Toward a Stateful Network protocol fuzzer[C]Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings. DBLP, 2006.

[13] ZHAO R, LV S. Neural-Network Based Test Cases Generation Using Genetic Algorithm[C].Pacific Rim International Symposium on Dependable Computing. IEEE, 2008.

[14] BYRESE J, FRANZ M. The use of attack trees in assessing vulnerabilities in SCADA system[C]. International Infrastructure Survivability Workshop (IISW’04).Lisbon, Portugal: Institute of Electrical Electronics Engineering,2008.

[15] LAI Yingxu, YANG Kaixiang, LIU Jing, et al. A Vulnerability Mining Method for Industrial Control Network Protocol Based on Fuzz Testing [J/OL]. Computer Integrated Manufacturing Systems: TP 20180511, 1-22.

[16] TU Ling, MA Y, CHENG C, et al. Hybrid Protocol Deformation Based Web Security Fuzzy Testing and Utility Evaluation Approach[J]. Computer Science,2017, 44(05):141-145.

[17] ZHANG Yafeng, HONG Zheng, WU Lifa, et al. Form-syntax based Fuzzing method for industrial control protocols[J]. Application Research of Computers,2017, 44(05):132-140.