Research on Industrial Control Devices Flaw Discovery Technology

Xi Chen[1, a], Qi Li[2]

[1]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2]Beijing University of Posts and Telecommunications, Beijing 100876, China

[a]572214342@qq.com

Keywords: ICS, flaw discovery, fuzzing, network security.

Abstract. Industrial Control System (in short, ICS) is an important part of state fundamental infrastructure whose safety concerns national economy development and people's property and life safety. Flaw discovery is the key of ICS defense. If attackers find flaws in ICS and use them for attack, the consequence will be unimaginable. The thesis focuses on researches about industrial control terminals flaw discovery and put forward a new flaw discovery method for industrial control terminals. We collect samples for test, basing on which we then make them produce variations. At last, we send those samples to target devices through dimmers to detect device flaws. The method uses cross-hardware and software programming data as test sample and applies genetic algorithms to design and achieve variogram, making the attack samples more comprehensive and effective.

Introduction

Industrial Control System(also, ICS)[1, 2] is a general name of control system applied in industrial production.ICS is widely used in industries like electricity, water conservation, oil, gas, manufacture, etc. Based on data sent back from remote control station, ICS can send advanced control instructions to control devices in remote workstations automatically or under the control of operators.

With the acceleration of industrial transformation and upgrade, the application of electronic computers and computer network technology becomes wider. Much industrial equipment has already equipped with fieldbus communication interfaces and industrial Ethernet communication interfaces of various types, thus have powerful uplink and downlink network communication capability.

However, while ICS intelligent, networking development accelerates industry development, it also brings many potential security problems. Hardware, software and communication protocol adopting in traditional ICS didn't concern communication security problems during connection on their design. Defense function of Enterprise management network and industrial control network are weak, or say, they almost have no separation function. For instance, if enterprise remote users connect with SCADA system (data collecting, monitoring and controlling system) through Internet, the system will face many security threats, for example, remote control and Internet invasion, and any part of the system being attacked will cause paralysis of the whole system. Also, the application of communication protocol, hardware and software, and large number of TCP/IP technologies in ICS makes ICS and traditional enterprise network highly integrated and at the same time brings information safety problems in traditional IT area[3]. In addition, only few enterprises are capable of providing industrial security vices.

Flaws discovery is fundamental in solving security problems of ICS. It can discover security problems existing in ICS before it breakout, then by precaution we can avoid flaws being employed to cause severe result.

Now we have made some progress in ICS defense research[4], but technology of ICS flaw discovery is comparatively few. Thus, there is an urgent need for research on ICS flaw discovery. It can not only repairs present flaws, avoiding enormous loss, but also provide technical support for ICS security assessment and testing to achieve comprehensive, systematic defense of ICS[5]. It will play an important role in strengthening ICS safety and building up a sound defense system.

Current Research Situation and Existing Faults

In Black Hat Conference 2007, ICCP (including TPKT and COTP), Modbus and DNP3 vague test modules (program samples) designed for Sulley were released by researcher Devarajan of Tipping Point Company in U.S. They can be used in detection of security flaws in industrial control network protocol on aspects like unauthorized command execution, unauthorized data transmission, possible service rejection, etc. [6] Roland Koch and other people from Augsburg University of Applied Science, Germany introduced Pro Fuzz [7], a type of fuzzing tool developed on Python version Scapy fuzzer base, which is compatible with Sulley's fuzz modules.

Through analysis on present researches, flaws detection methods for industrial control devices are mainly fuzzing passed network protocol and most of them basing on generated network protocol fuzzing [8]. These fuzzing have following disadvantages:

Great Difficulties on Industrial Control Protocol Analyzing. Now a serious problem of fuzzing is low test sample hit rate, especially in industrial control devices. Because of lack on relevant knowledge about industrial control protocol, industrial control devices refuse many test samples send from dimmers even cut off connection in the middle. As for some public protocols, they can refer to protocol files. But most protocols in ICS are private .What's more, there are lots of difficulties to overcome and many technologies needed in analysing private protocols.

Low Concentration. At present, most test samples used in fuzzing are generated basing on industrial control protocols. But how industrial control devices deal with these test samples has not been taken account of seriously. It results in blindness of test sample, or say, it doesn't focus on a specific processing procedure.

In this paper, we provides a new solution to the above problems, a fuzzing based on programming data input identification and variogram design of genetic algorithms.

General Idea of Flaw Detecting Method

To solve industrial control protocols analysing problems and low concentration of the existing fuzzing methods, the paper designs a fuzzing based on programming data. Details of its structure are shown in Figure 3-1 below:

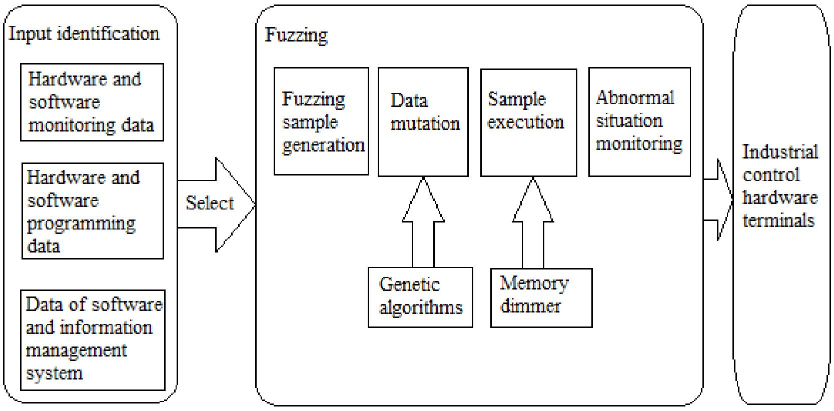
Input identification
Hardware and software monitoring data
Hardware and software programming data
Data of software and information management system
Select
Fuzzing
Fuzzing sample generation
Data mutation
Sample execution
Abnormal situation monitoring
Genetic algorithms
Memory dimmer
Industrial control hardware terminals

Figure 3-1 General idea of ICS hardware flaw detection

As the figure shown, we select hardware and software programming data, input them, and after fuzzing, detect flaws in industrial devices. There are 4 links included in fuzzing:

Generation of Test Samples. First, we need to solve the problem of samples' resource. Industrial control software controls hardware's core logic by programming, meanwhile, programming data reach its operating system which makes flaw discovery more efficient. So, the paper selects this data as data resource in fuzzing.

Data Mutation. Data mutation is the core in fuzzing. Its function is to generate large number of unexpected data only which is likely to trigger security bugs.

Test Sample Execution. In order to avoid huge waste causing by blind issue of patches and improve efficiency, we need to analyse and adjust object system, and set up test process to improve fuzzing efficiency.

Abnormal Situation Monitoring. This is key part of fuzzing. An important character of bug triggering is abnormality occurrence. Abnormality monitoring aims at capturing abnormality and then analysing whether it is a security bug.

Key Technologies of Improved Bug Detection Method in ICS

Generating Method Design of Test Samples Based on Programming Data. Analysis on ICS Network Data Flow. ICS network is divided into three parts: information network, monitoring network and site network. These 3 levels of network include large amounts of data, and we roughly divide these data into 3 types in this paper. They are software and hardware programming data, software and hardware monitoring data, and software and information management network communication data. Refer to the figure below:

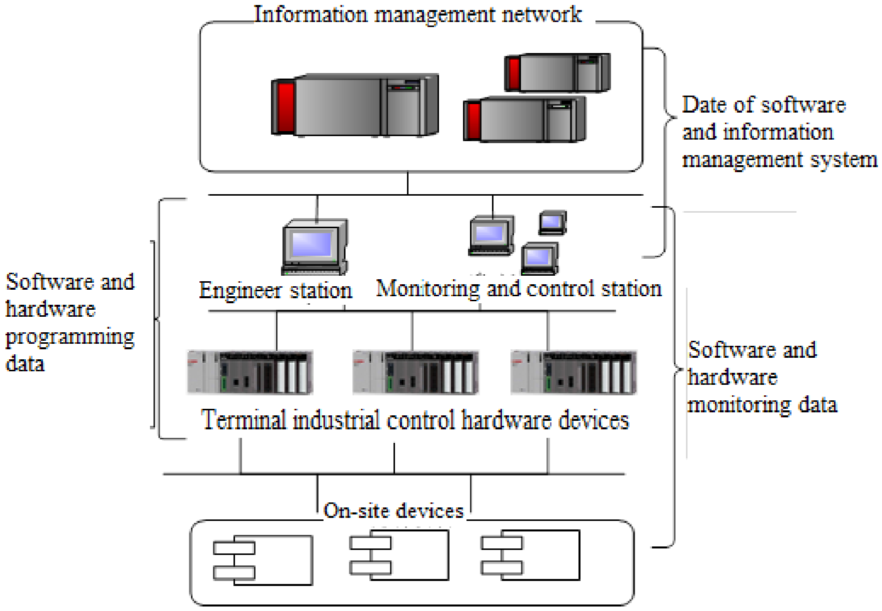
Information management network
Date of software and information management system
Software and hardware programming data
Engineer station
Monitoring and control station
Software and hardware monitoring data
Terminal industrial control hardware devices
On-site devices

Figure 4-1 Schematic diagram of ICS data flow

Selection of Test Samples Based on Programming Data**.** Current input identification methods are mainly basing on network protocol. This kind of identification method doesn't take account of the real meaning of data input, but executes input according to the type of network protocols. What this kind of identifications usually do is analysing network protocols, however, most industrial control protocols are private and the number of this kind of protocols is large. Thus, using this kind of method to identify input will meet lots of difficulties. This paper fully takes account of the real meaning of data input and put forward input based on programming data.

We will analyse features of the 3 types of ICS data and the possibility of using them in fuzzing respectively. Then choose a kind of data as fuzzing input for industrial control hardware devices.

Table 4-1 Comparison of industrial control data feature

Data	Collecting difficulties	Targeting degree of industrial control devices	Data logic
Data of software and information management system	Easy	Not target on industrial control devices	Illogical data
Software and hardware monitoring data	Difficult	Target on industrial control devices	Illogical data
Software and hardware programming data	Easy	Target on industrial control devices	Strongly logical data

Data of software and information management system embodies features like large amount, easy to collect, etc. However, it is direct transmission data between software, so it doesn't adapt to industrial control terminal hardware devices well.

Software and hardware monitoring data refers to direct communication data. It has strong targeting nature, but its amount is also very large. Considering ICS's high demand on promptness, data collecting difficulties, and lack of logic in data, it is not suitable for using as the source of fuzzing test samples.

Software and hardware programming data is communication data between software and hardware. It highly focuses on hardware. Industrial control software controls hardware core logic by programming. Programming data can reach operating system of industrial control hardware .When software programs on hardware, the system usually doesn't operate at that time. If we collect data then, it will not have much effect on operation of ICS.

In summary, the paper selects software and hardware programming data as test sample in fuzzing.

Design of Variogram Based on Genetic Algorithms. Traditional variogram mainly processes test samples with simple, heuristic mutation. The mutating method which performs a simple mutation on samples produces samples with comparatively simpler variation and doesn't take account of possible bugs caused by the combinations of several samples. Thus, the paper introduces genetic algorithms to cause mutation on data, and then generates test samples.

Genetic algorithms is a kind of calculating modal produced by combining simulation of natural selection in Darwin's biological evolution theory and biogenetics.

A flow chart of variogram based on genetic algorithms design is shown in the following figure(Figure 4-2):

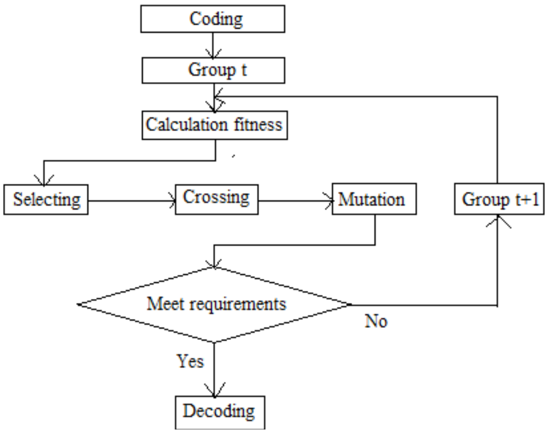

Figure 4-2 Flow chart of variogram based on genetic algorithms

The variogram can be divided to several steps:

Coding. It includes initializing groups and coding individuals. According to the features of programming data of industrial control terminals, the thesis analyses advantages and disadvantages of a series of common coding methods like binary encoding, tree encoding, interchangeable coding, etc. Then the thesis chooses binary encoding to code individuals.

Fitness. The result of fitness calculation has great influence on genetic algorithms. Bigger the fitness value we get, better the answer is. Fitness is core and motion of the whole algorithm. The selection of fitness calculation should be threat differently in different problems. Individual fitness decides heredity opportunity and it's also the criterion in individual evaluation.

Selecting. It's survival of the fitness in fact. Using fitness value algorithms designed in Step 2, we select individuals with high fitness and let them pass on their gene. We do these to ensure better solution.

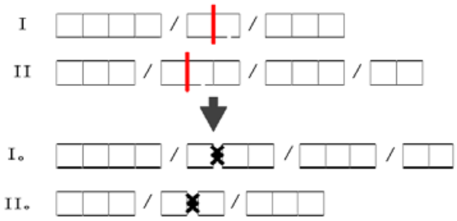

Figure 4-3 Schematic diagram of crossing calculation

Crossing. The major function of crossing calculation is to generate new individuals. By exchange of partial genes such as genetic chromosomes between two individuals paired successfully, new individuals will be generated. These new individuals own some characteristics of the two samples at the same time which increases the rate of triggering bugs. Figure 4-3 shows crossing calculation used in this thesis:

Mutation. The result of mutation operation is generating new individuals as well. It achieves this by change some gene loci of individuals generated. As a subordinate method, mutation operation works together with selecting and crossing to complete a search.

Experimental Verification

Basing on the design above, the paper selects several typical ICS hardware for bug detection and finds out many bugs. Next, we will cite PLC (Programmable Logic Controller) as an example to give a detailed illustration.

PLC, also called Programmable Logic Controller, plays an irreplaceable role in 80% ICS designs. Security bugs in PLC have a direct influence on the safety and stability of the whole control system. The concrete detecting processes designed by the paper are as follows:

Bug Detecting Scene. Bug detecting scene is as follow:

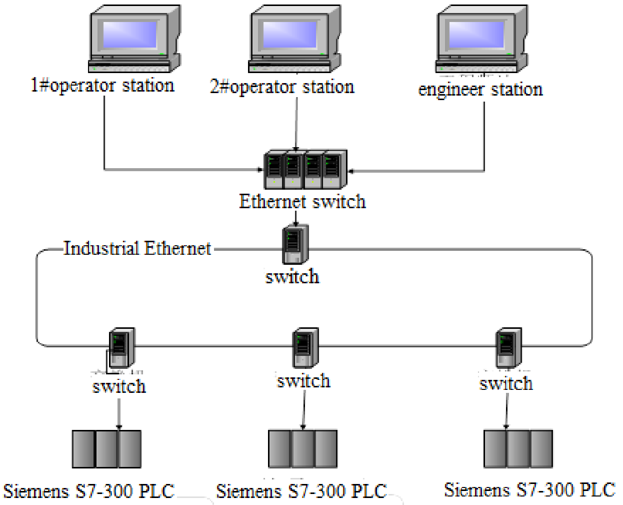

Figure 5-1 Bug detecting scene

PLC bug detecting scene consists of the following essential components:

Engineer stations: Engineer stations are used by controlling engineers in industrial process. Through the stations, engineers can configure, program or modify computer systems.

Industrial Ethernet: Industrial Ethernet is strong local area network and unit network based on IEEE 802.3 (Ethernet). On the base of traditional Ethernet, it adds some rear-time designs.

PLC: Programmable logic controller is a kind of electronic system, specially designed for application in industry, run by digital operation .The PLC adopted here is Siemens s7-300.Siemens PLCs account for a large share of PLCs in ICS which are also the major devices involved in Stuxnet incident.

Bug Detail. The method found a case of service rejection .There are service rejection bugs in S7-300,which means attackers can send carefully constructed packet by industrial Ethernet to trigger those bugs, and what’s more, S7-300 can not be restarted once it stops operating.

Figure 5-2 A picture of bug triggering

Comparison of Experimental Data. Because the protocol used in communication of STEP7 and PLC is tpkt of ICCP. The paper also uses sulley program test sample mentioned in Document[6], as a contrast of the method introduced in this paper ,in PLC fuzzing to try to detect bugs.

Table 5-1 Figure of experimental data comparison

Tool	Test sample amount	Test time	Bugs triggered
Sulley	20000	12.5 hours	0
Method used in the paper	100	1 hour 20 minutes	1

The experimental data shows: Compared with some existing tools, the method put forward by this paper are more targeted on bug detection of industrial control hardware terminals and it can significantly improve the efficiency of bug detection.

Conclusion

As a new research field of security researches, ICS security has received widespread concern. But at present stage, there are few researches on bug detection in ICS security researches. What's more, bug detection methods in IT system are not perfectly adaptable to ICS. So, there is an urgent need of bug detecting method for ICS. The paper starts research from here and puts forward a new bug detecting method. First, collecting test samples and then mutating these samples selected. At last, sending those mutated samples by dimmers to object devices to detect bugs. Using the method in this paper, we detect bugs in a typical industrial control terminal device and successfully detected a case of service rejection bug. Besides, the paper also used another published industrial control network protocol fuzzing method to do the same test and then compared the two results. It shows that the method introduced in this thesis is more efficient.

Acknowledgment

This work is supported by National Natural Science Foundation of China Project (61302087, 61401038).

References

[1] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82.

[2] Zhang Shuai, ICS Security Risk Analysis Information Security and Communication Privacy 2012(3) 15-19.

[3] Oman P, Schweitzer E, Frincke D. Concerns about intrusions into remotely accessible substation controllers and SCADA systems// Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference. 2000, 160.

[4] Dzung D, Naedele M, Von Hoff T P, et al. Security for industrial communication systems. Proceedings of the IEEE, 2005, 93(6): 1152-1177.

[5] Ralston.Cyber security risk assessment for scada and dcs networks.ISA transactions, 2007, 46: 583-594.

[6] Devarajan.G. Unraveling SCADA protocols: Using Sulley fuzzer. presented at the Defcon 15 Hacking Conference. http://www.defcon.org/html/defcon-15/dc15-speakers.html.

[7] Koch,R.Profuzz.https://github.com/HSASec/ProFuzz

[8]Wu Zhiyong, Xia Jianjun, Sun Lechang. Summary of Multidimensional Fuzzing Technology. Research on Computer Application, 2010, 27(8) 2810. 2813.