A Vulnerability Mining System Based on Fuzzing for IEC 61850 Protocol

Tengfei Tu[1, a], Hua Zhang[1, b], Boqin Qin[1, c] and Zhuo Chen[1, d]

[1] Beijing University of Posts and Telecommunications, BeiJing 100876, China.

[a)]tutengfei.kevin@bupt.edu.cn, [b)]zhanghua_288@bupt.edu.cn, [c)] bobbqqin@bupt.edu.cn, [d)]chenzhuo0618@bupt.edu.cn

Keywords: Mining system, Fuzzing, Protocol

Abstract. In this paper, we proposed an effective vulnerability mining system for IEC61850 protocol in the Smart Grid. First of all, we introduce the basic structures and features of IEC61850 protocol. Next, we summarize the possible vulnerabilities of it. Finally a fuzzing tester named IECFuzzer is designed and implemented using the technique of fuzzing. A lot of simulation results show that IECFuzzer can not only be used to exploit the potential denial-of-service vulnerabilities of IEC61850 protocol, but also to verify the robustness of PLC devices using IEC61850 protocol.

INTRODUCTION

With the development and popularity of Intelligent Electronic Devices in industrial control systems, the attackers show growing interest in attacking industrial equipment. According to Amrein[1], the total number of the vulnerabilities in industrial control systems experienced rapid growth from 2015 to 2016. Among all the targets under attack, power systems are undoubtedly the focus of attention. Since power systems are of vital significance in the national economy and the people's livelihood, the frequent occurrence of power system intrusion has brought huge losses to many countries. In 2010, the Stuxnet worm [2, 3, 4] attacked Iranian nuclear power plant facilities and caused serious damage. The virus exploited the vulnerability of the Siemens SCADA systems, which is widely deployed in Iranian nuclear power plants. On December 23, 2015, Ukraine's power system suffered from a serious hacker attack. The attackers mainly targeted at the power companies, resulting in widespread blackout in Ukraine [5]. In view of the grim security situation in power systems, the security of the Smart Grid, the next generation of electrical grid, has become a hotspot in network security research.

IEC61850 [6] is a communication standard for electrical substation automation systems. the IEC61850 has many advantages over other industrial protocols in the Smart Grid, like reporting schemes, fast transfer of events, etc. [7] Therefore the IEC61850 has been supported by the majority of the industrial equipment vendors, while the security of the protocol has also become the focus of attention of the attackers.

In order to prevent the attackers from exploiting the vulnerabilities of IEC61850 protocol to perform attacks on the Smart Grid, it is essential to build a system to dig loopholes of the industrial devices supporting the protocol. Fuzzing [8] is a powerful means of mining vulnerabilities. It is widely used in exploiting the security vulnerabilities of various applications, especially of the protocols used in industrial control systems. Fuzzing supports a variety of industrial protocol tests, such as MODBUS, DNP3, OPC, etc. Compared with the above protocols, the IEC61850 has a more complicated structure and more features [6, 7]. The complexity of the IEC61850 increases the difficulty and cost of the security analysis. Consequently, although there have been a great many fuzzing tools for other industrial protocols like MODBUS, DNP3, OPC, to our knowledge, no professional open source fuzzing tool for the IEC61850 has been published so far.

In this paper, a fuzzing method for IEC61850 protocol is proposed based on the existing fuzzing technology, and a fuzzing tester called IECFuzzer is designed and implemented. The simulation results on industrial PLCs reveal that there are still some loopholes in the implementation of the protocol.

The remainder of this paper is structured as follows. Section 2 introduces the research of fuzzing technology for industrial protocols. The features and the potential vulnerabilities of IEC 61850

protocol is presented in Section 3. Section 4 details the design of a fuzzing model typically for IEC 61850 and the implementation of a fuzzing tester called IECFuzzer. The experiments on the industrial equipment with IECFuzzer are described in Section 5. Section 6 analyzes the simulation results. Finally, the conclusion is reached and the prospect of the future work is depicted in section 7.

RELATED WORK

Fuzzing Technology

So far, the fuzzing technology has evolved from a completely random test to a more specific one. At first, fuzzing could only use randomly generated data as a test case. But now fuzzing is more intelligent than before. It can leverage the definition of the model to produce basic data changes and variants, generate some specific "abnormal" data, send the data to the target, and record the state and the responses of the target [8].

The most important and most difficult part of a good fuzzing tester is the generation of "valid" test cases. An "effective" test case can lead to crashes or errors, so that the tester can detect potential vulnerabilities in the target. There are two methods for generating test cases in fuzzing: one is based on the generation technique, and the other is based on the mutation technique [8]. Current fuzzing frameworks generally support both of the methods.

For the generation method, the test cases are usually generated from random test data produced by random functions. For example, in a 32-bit target system, a function of the protocol program accepts an input parameter that is an unsigned INT type (0-429467295). The fuzzing will pass a negative number or a number greater than 429467295 to the function. This operation is likely to cause an overflow in the program, and eventually cause the program to crash. As for the mutation method, a data model is leveraged to generate specific test cases. One typical application scenario is SQL injection, which requires "deformed" text content. Since the statements of SQL injection have fixed patterns, SQL injection fuzzer can generate "deformity" of the SQL statements based on the template variation of some of the patterns.

The generation method and the mutation method may affect the "validity" of the input data in different aspects, which will then directly affect the fuzzing duration and results. Thus the choice between the two methods will have a decisive impact on the efficiency of the fuzzing framework by the generation of different test cases.

As a commonly used technique of vulnerability detection, fuzzing technology has the same basic workflow as other techniques despite the different implementation of the generation and selection of the test cases. The basic workflow can be summarized as follows: data modeling, the generation of test cases, the selection of test cases, monitoring and recording the status and system information of the target, analysis of the test results. The basic workflow of a fuzzing tester is shown in Figure 1.

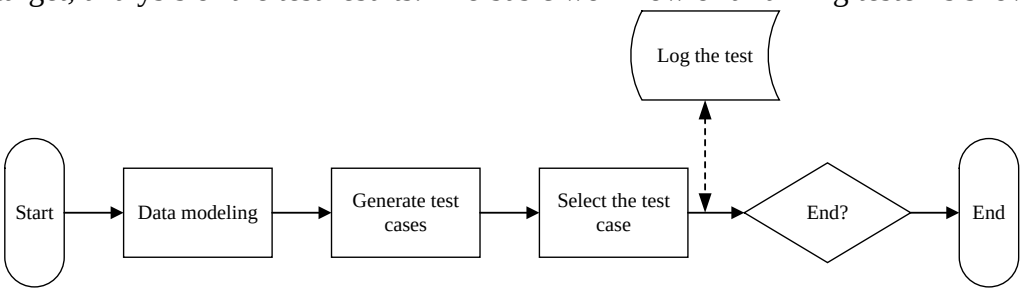

FIGURE 1. The workflow of a fuzzer

IEC 61850 Fuzzing Tool

Up to now, there has not been any professional open source fuzzing tools for IEC61850 protocol. The reasons for the slow progress of the research on IEC 61850 fuzzing are as follows: on one hand, the complexity of IEC61850 protocol increased the difficulty of the generation of user cases; on the other hand, the physical equipment using IEC61850 protocol is relatively uncommon and expensive.

Although there is no specific fuzzing tool designed for IEC61850 protocol, there are some common fuzzing frameworks, which support a variety of industrial protocols. For example, PROTO [8] can parse the structure of the protocol, generate the data model according to the protocol field, and generate some test cases according to the data model. Alarm Frame Random implements a fuzzing method for the profinet protocol. Ting Wang proposed a method for the OPC protocol fuzzing [9]. Xiong Qi et al. implemented an OPC-MFuzzer tool for OPC-based vulnerability exploiting based on the work of Ting Wang et al [10]. Devarajan designed the fuzzing framework for ICCP, MODBUS and DNP protocols [11]. Compared with the above traditional fuzzing tools, Sulley, the new generation of fuzzing framework, is much easier to use, in that it not only tests software in a physical machine, but also tests software in a virtual machine [8]. The flexibility and efficiency of Sulley makes it the basic framework of IECFuzzer in this paper.

Besides the open source fuzzing tools mentioned above, some commercial fuzzing tools are highly concerned by the security researchers. For example, SecuriTeam supports the fuzzing of the DNP3 protocol. Peach proves to be an excellent fuzzing framework, which supports a majority of industrial protocols. Although closed source commercial software has prevented us from directly applying it as the framework of IECFuzzer, the functionality of the commercial fuzzing tools has a reference value to us.

In conclusion, although the fuzzing technology has been the concern of a number of security researchers and a large quantity of related work has been done in this field, the use of fuzzing technology for IEC61850 protocol vulnerability research is still very limited. Thus it is urgent to develop an IEC 61850 fuzzing system to fill the gaps in the study of IEC 61850 fuzzing.

OVERVIEW AND ANALYSIS OF IEC 61850

The Introduction of IEC 61850

IEC 61850 is the only communication standard system proposed by International Electrotechnical Commission for the future of substation automation system [5, 11]. IEC 61850 defines an abstract data model that can be mapped to multiple protocols. Now common mapping protocols of IEC 61850 include the message specification protocol (MMS protocol), the general object-oriented substation events protocol (GOOSE protocol) and the sampling measurement values protocol (SMV protocol) [12]. MMS protocol is an application protocol based on TCP / IP, which is applied to intelligent substation with server and client model. GOOSE protocol and SMV protocol is a high-speed Ethernet protocol, mainly used in "real-time" requirements of higher substation automation systems. Figure 2 is a comparison between IEC61850 protocol stack and the five-layer protocol stack of the common computer network [12].

IEC61850 protocol is the basis for the future seamless telematics system. As the only substation automation system of international standards, it has four outstanding advantages:

(1) Supporting a comprehensive set of substation functions;
(2) Easy to configure and maintenance with a concise design;
(3) Higher-performance relay communication between multicast messages;
(4) Convenient to upgrade the system.

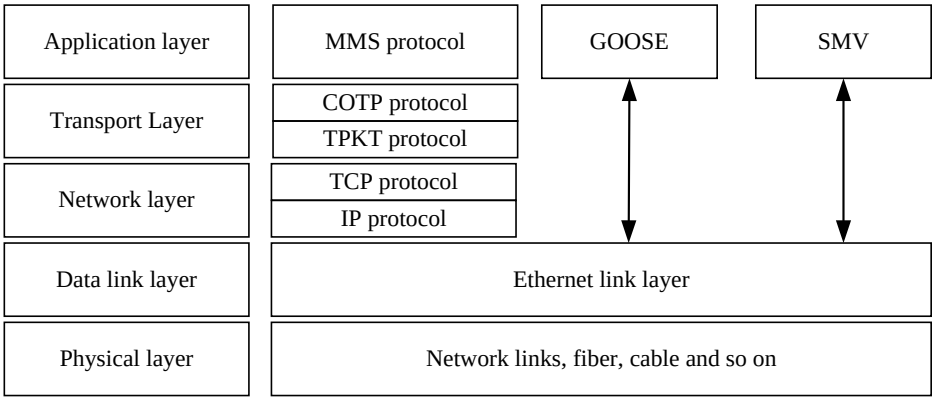

FIGURE 2. IEC61850 protocol stack

MMS Protocol Structure

ISO / IEC 9506 Manufacturing Message Specification, or MMS for short, is an international standard developed by the International Organization for Industrial Automation Technical Committee TC184. It implements the object-oriented modeling of the actual equipment to achieve the interoperability between different equipment manufacturers under the network environment.

The MMS specification is located at the application layer 7 of the ISO / OSI seven-layer reference model, which comprises a very large set of protocols. As shown in Table 1, it consists of six parts. MMS communication uses client / server model. The client generally runs monitoring systems, control centers, etc., while the server refers to one or more actual equipment or subsystems. In the substation automation system, the communication between the background monitoring system and the protection and testing device is typical client / server mode. The client represents the background host and the server represents the protection and monitoring device. In addition to the background monitoring host, the remote device and the protection device of substations are also the client.

MMS services can be divided into two types: Confirmed and Unconfirmed.

(1) As shown in Figure 3, the communication service described is initiated by the client and the server is required to finally return a confirmation message (Confirm). The communication process between the client and the server is carried out in five steps. Such services are known as Confirmed Service.

TABLE 1. MMS specification document composition

ID	Doc	Description	Year
1	ISO/IEC 9506-1 Services	Service specification, the core part	1990
2	ISO/IEC 9506-2 Protocol	Protocol specification, the core part	1990
3	ISO/IEC 9506-3 Comp. Standard for Robots	Robot companion specification	1992
4	ISO/IEC 9506-4 Comp. Standard for Numeric Control	Digital control with specifications	1993
5	ISO/IEC 9506-5 Comp. Standard for Programmable Logic Controller	Programmable logic controllers with specifications	1997
6	ISO/IEC 9506-6 Comp. Standard for Process Control	Process control systems are accompanied by specifications	1994

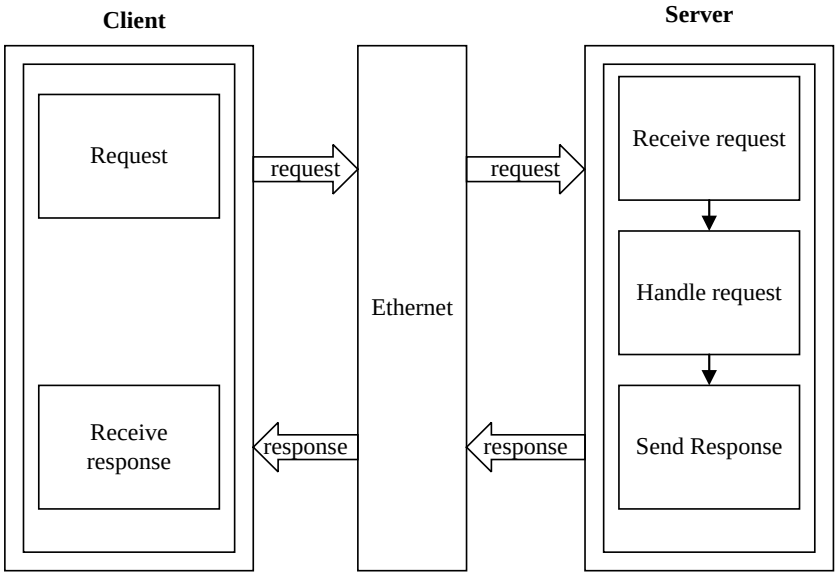

FIGURE 3. MMS with a confirmation of the communication process

(2) In MMS, there is a class of services which requires the server to automatically send the service response to the client from time to time rather than requires the client to send the service request. Such services are known as the service without confirmation (Unconfirmed Service), as shown in Figure 4.

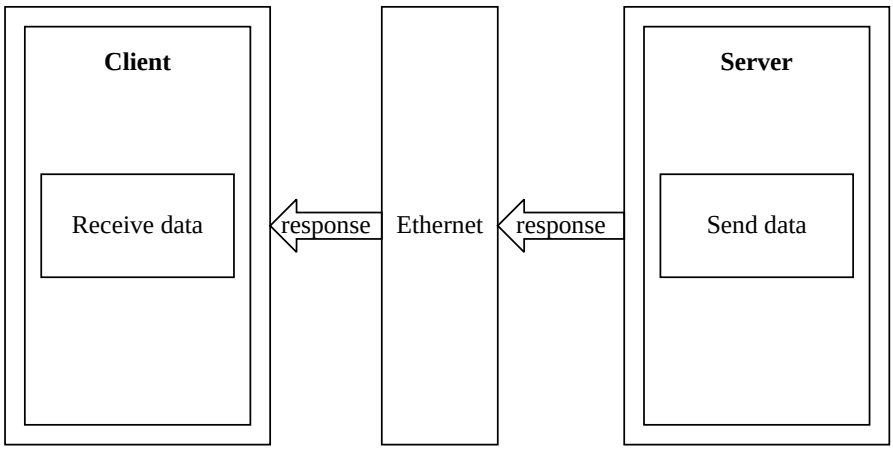

FIGURE 4. MMS without confirmation of the communication process

ISO 9506 defines a total of 85 kinds of MMS services. All the services can be mapped into a bit string, with each bit corresponding to an MMS service. For example, if the value of bit 0 in the bit string equals to 0, it means that the device support the status service; otherwise, it means that the device does not support the status service. Table 2 shows the bit numbers of the 14 MMS services in IEC61850 protocol.

TABLE 2. 14 kinds of commonly used MMS service corresponding bit serial number

Bit ID	MMS Service	Bit serial number	MMS Service
1	getNameList	65	readJournal
4	read	72	fileOpen
5	write	73	fileRead
6	getVariableAccessAttribute	74	fileClose
11	defineNamedVariableList	76	fileDelete
12	getNamedVariableListAttributes	77	filedirectory
13	deleteNamedVariableList	79	informationReport
46	obtainFile	83	conclude

Vulnerability Analysis of IEC 61850

The IEC61850 protocol is the main communication protocol in the intelligent substation, and its security also determines the security of the whole substation system. A simplified intelligent substation network organization chart is shown in Figure 5.

According to the distribution of various components of intelligent substation, there are many different types of network security attacks.

(1) Denial of service attacks. Denial of service attacks are common attacks to stop the target from providing services by attackers through some means. An example of a denial-of-service attack in the Smart Grid is that the hacker attacks the instrument on the substation bus by simulating a workstation by some means, making the instrument unusable [13].

(2) Malformed packet attacks. Malformed packet attack is a workstation or relay or instrumentation to receive abnormal packets, resulting in various components of the exception does not work [12].

(3) Address protocol analysis to deceive attacks. In Figure 5, Once a compromised computer is connected to the substation bus, it is used to send ARP packets to all the IPs connected to the bus, and the data is collected in the computer. The attack can be used to steal the data in the substation.

(4) Man-In-the-Middle attack. The man-in-the-middle attack can lead to the communication leak of equipment information to the third party. For example, in Figure 5, after the workstation receives a man-in-the-middle attack, the communication between the workstation and the equipment or relay may be attacked by a third-party.

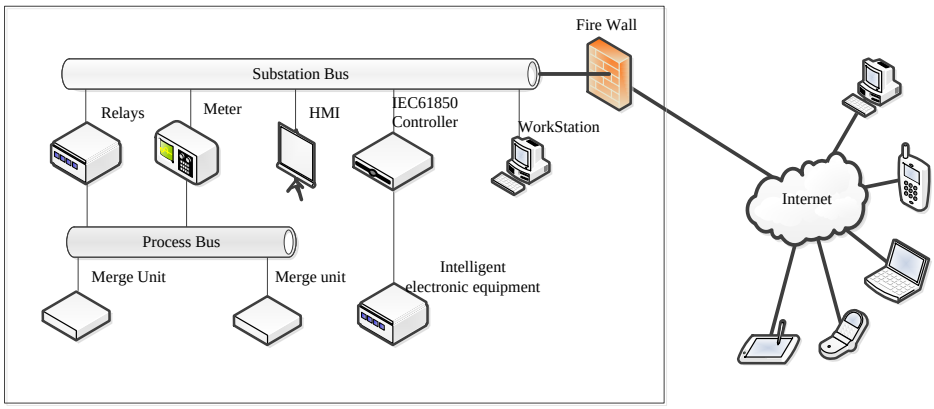

FIGURE 5. The structure of intelligent substation organization

IECFUZZER MODEL

IECFuzzer mainly consists of four modules: the mutator module, the mutator selection module, the data reorganization module and the survival of the verification module. In order to leverage the definition of the data model of MMS test, this paper divides the mutator module into six components according to the structure of the MMS protocol structure: TCP layer variator, TPKP mutator, COTP mutator, SES mutator, PRES mutator, MMS mutator. The structure of IECFuzzer is shown in Figure 6.

1) Mutator Selector Module

During the fuzzing, IECFuzzer invokes some fields randomly selected by the mutator selector module to mutate. The mutator selector module can choose to mutate the data in the IP field or the data in the TPKP and COTP fields, or even the data in the MMS field. In a fuzzing, you can select one or more fields to mutate.

2) Mutator Module

The mutator module provides various mutable fields, mutation modes and mutation strategies for each layer (e.g., IP layer, MMS protocol layer, etc.).

First, we provide a set of normal IEC 61850 communication data as a sample space. The mutator will extract the corresponding variable fields from the sample space variation. Some fields, such as

IP layer Destination field, are forbidden to mutate. The results are returned according to different variation. There will be a judge which will decide on increasing or decreasing the corresponding score in the variance of the field weight, to make a more accurate future test in the field. As to whether the returned result is normal or abnormal, it will be verified by the survival verifier module.

There are two kinds of variants used in the mutation: one is based on the random generation method; the other is based on the sample data variation method.

Random generation is used to generate random length or indefinite length of the binary data. Generating random binary data of fixed length can expand the coverage of variability. It can be used to discover the available unknown opcode, status code, etc. So the more effective mutation data is generated. The random binary data of indefinite length randomly generates binary data of different lengths, which can produce too long or too short of the data to find possible problems, such as overflow and so on. The disadvantage is that the resulting data may be very small, and most of them will be discarded because of unrecognition.

The method of mutation based on the sample data is to extract the value of the field to be mutated from the data packet in the sample space, and then expand, reduce, transform, replace, and so on.

3) Data Reorganization Module

Data reorganization module adds the data packet after the mutation into the variation packet, and then sends it to the target PLC.

4) The Survival Verifier Module

The survival verifier module communicates with the target PLC in real time and obtains the status of the PLC. When the target PLC rejects the unresponsive service because of an exception, the survivor verifies the target exception and retains the test case that caused the target exception.

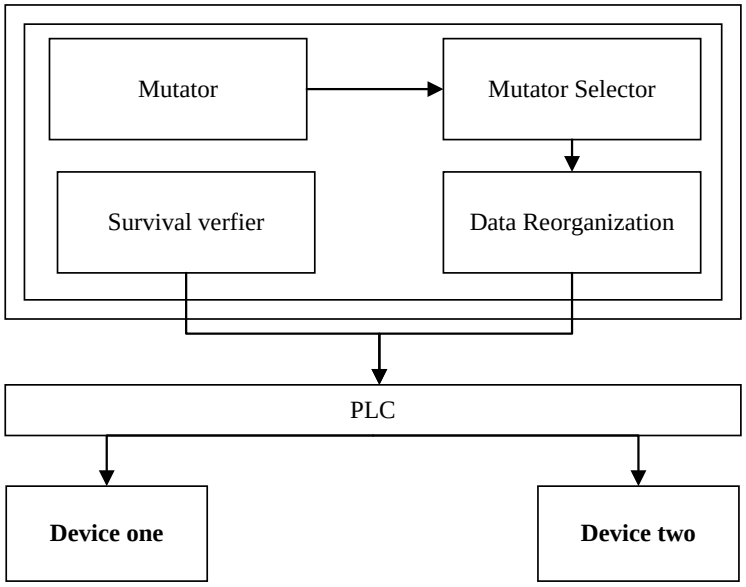

FIGURE 6. The structure of IECFuzzer

EXPERIMENTS

In this paper, the data of TPKT layer, COTP layer, SES layer, PRES layer and MMS layer of IEC61850 protocol are tested for variation. The test target is a group of PLC devices produced by Rockwell Allen-Bradley. The duration of the experiment is 7 x 24 hours.

In order to verify the robustness of the IEC51850 protocol to the maximum extent, several test experiments were carried out from the TPKT layer, COTP layer, SES layer, PRES layer and MMS layer, respectively, and the experimental results were summarized. IEC61850 protocol experimental results are shown in Table 3.

Table 3. The result of fuzzing PLC

Protocol	Field	Testing Time (hour)	Denial of Service times
TCP	Package Length	7 X 24	106
TPKT	Source Reference	7 X 24	14
COTP		7 X 24	20
SES		7 X 24	12
PRES		7 X 24	17
MMS		7 X 24	15

After a number of experiments, the experimental results were analyzed in detail. In the experiment, by using the package length field of the fixed-length variant in TPKT protocol layer, an unresponsive exception (denial of service) is generated when the contents of AF 6D, 9D 7F, 86 EE or CB D7 are transmitted. By using the variation based on the sample data, we found that when the value of the source reference field in the COTP protocol layer is C3 37, it will result in an unresponsive denial-of-service exception and the MMS protocol layer with a Length field of 00 or EB will result in an unresponsive denial-of-service exception. In addition, this experiment also tried to establish TCP connection to the PLC for 10,274 times in 7x24 hour. Through analysis of the experiment results, we discovered that when TCP connection resources are occupied many times in a long period of time, the denial of service anomaly frequently appears in the PLC devices.

The above experimental results prove that IECFuzzer can effectively mine the potential loopholes in the PLC devices using IEC61850 protocol.

CONCLUSION

In this paper, IEC61850 protocol is introduced and a fuzzing tester called IECFuzzer based on fuzzing technology for IEC61850 protocol is proposed, and the effectiveness of IECFuzzer is verified through experiments. IECFuzzer can test IEC61850 protocol based on the potential PLC vulnerabilities.

IECFuzzer is primarily used to test the target PLC by sending variation of IEC 61850 packets observed after the target PLC's response, thus it can not directly give the specific reasons for the occurrence of denial of service anomaly. In the future, not only will we improve the efficiency of IECFuzzer, but also analyze the specific causes of the anomalies and dig out more potential vulnerabilities.

ACKNOWLEDGMENTS

We thank our reviewers for their valuable comments. This work is support by NSFC(Grant Nos. 61300181, 61502044), the Fundamental Research Funds for the Central Universities(Grant No. 2015RC23). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1]. Amrein, A., et al. "Security intelligence for industrial control systems." IBM Journal of Research and Development 60.4 (2016): 13-1.

[2]. Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." IEEE Security & Privacy 9.3 (2011): 49-51.

[3]. Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5 (2011): 6.

[4]. Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication 800.82 (2011): 16-16.

[5]. Lipovsky, Robert, and A. Cherepanov. "Blackenergy trojan strikes again: Attacks ukrainian electric power industry." (2016).

[6]. Mackiewicz, R. E. "Overview of IEC 61850 and Benefits." 2006 IEEE PES Power Systems Conference and Exposition. IEEE, 2006.

[7]. Kumpulainen, Lauri, et al. "Benefits and performance of IEC 61850 Generic Object Oriented Substation Event-based communication in arc protection." IET Generation, Transmission & Distribution (2016).

[8]. Sutton, Michael, Adam Greene, and Pedram Amini. Fuzzing: brute force vulnerability discovery. Pearson Education, 2007.

[9]. Wang, Ting, et al. "Design and Implementation of Fuzzing Technology for OPC Protocol." Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on. IEEE, 2013.

[10]. Devarajan, Ganesh. "Unraveling SCADA protocols: Using sulley fuzzer." Defon 15 Hacking Conf. 2007.

[11]. Yang Y, Jiang H T, McLaughlin K, et al. Cybersecurity test-bed for IEC 61850 based smart substations[C]//2015 IEEE Power & Energy Society General Meeting. IEEE, 2015: 1-5.

[12]. Sidhu T S, Yin Y. Modelling and simulation for performance evaluation of IEC 61850-based substation communication systems[J]. IEEE transactions on power delivery, 2007, 22(3): 1482-1489.

[13]. Rashid, M. T. A., Yussof, S., Yusoff, Y., & Ismail, R. (2014, November). A review of security attacks on IEC 61850 substation automation system network. In Information Technology and Multimedia (ICIMU), 2014 International Conference on (pp. 5-10). IEEE.