An efficient vulnerability scanning scheme of smart power grid based on hybrid scanning method

Qi Wang\textsuperscript{1,2*}, Xiaojian Zhang\textsuperscript{1,2} and Qigui Yao\textsuperscript{1,2}

\textsuperscript{1}Global Energy Interconnection Research Institute Co. Ltd, Nanjing, Jiangsu, 210003, China

\textsuperscript{2}State Grid Key Laboratory of Information & Network Security, Nanjing, Jiangsu, 210003, China

\textsuperscript{*}Corresponding author’s e-mail: wangqi@geiri.sgcc.com.cn

Abstract. As one kind of the industrial control networks, the increasing complexity of the advancing smart grid makes the network security risks greatly increased. Thus, it is necessary to ensure the safety of system. This paper proposed an efficient and low-cost comprehensive vulnerability scanning scheme. Considering the idea of non-intrusive detection without additional flow, the passive detection is proposed associated with PROFINET real-time protocol used in ICS. To reduce the redundant and save resource, fusion detection and connectionless detection are suggested separately adapted to Modbus TCP of ICS which utilizes TCP/IP model. Then passive detection and two active detections are adopted at different frequencies. The analysis results show that the proposed technique has higher efficiency, lower cost and improves the scanning concealment.

1. Introduction

With the development of industrial control system (ICS), grid systems have evolved from traditional grids to smart grids which are highly likely to trigger accidents. The computer virus Stuxnet, for example, targeted Iranian enrichment plant facilities, damaging centrifuges and resulting in a 30 percent drop in the capacity of centrifuges\cite{1}. The smart grid including subnets with different functions such as production control and transmission network has higher real-time requirements. Precisely because of such characteristics, it’s infeasible to migrate security techniques such as scanning for IT networks to smart grids directly. Therefore, it is of great significance to study the vulnerability scanning of smart grid industrial control system.

In order to meet the requirements of real-time and security scanning, a comprehensive vulnerability scanning method is proposed and the main contributions of this paper are as follows. Since the subnets in ICS have their own packaged traffic stored in redundant space, this paper suggests fusion detection and connectionless detection combined with Modbus TCP in association with normal working traffic to reduce the cost and improve the speed. The two active detections still bring additional traffic in device response which has already provided the needed information. It is unreasonable to ignore the information for repeated detection under high real-time requirements. Thus, the passive detection is applied to monitor existed information in flow which reduces the flow of repeated detection effectively. The information obtained by the above two techniques is limited and can be regarded as local detection. In light of increment mechanic and overall situation to power grids, comprehensive use of global detection and local detections is to obtain the optimal balance between security and business performance with reasonable strategy. For time strategy, global detection or local detection can be...
selected according to the different peak periods of each subnet. At the incremental angle strategy, the information obtained by local detection is compared with that of the latest global detection to determine the key information changes. The global detection is applied if variable trends change a lot.

The rest of the paper is organized as follows. Section 2 gives an overview of power grid ICS and the own combined databases used. Section 3 explains the detailed design including passive detection, fusion detection, and connectionless detection desperately. Section 4 contains performance analysis and section 5 provides future research directions.

2. Vulnerability scanning method for power grid ICS

2.1 Principle and structure
The power grid ICS mainly includes various business application systems used by power enterprises for production, dispatching, operation and management[2]. The power grid ICS is composed of management network and control network. The management network is divided into a monitoring layer, an analysis layer and a data layer, which refers to a dispatching monitoring management network. The control network contains a station control layer, an interval layer and a process layer, which is deployed in a substation[3]. Based on the architecture of the power grid ICS shown below, a comprehensive vulnerability scanning scheme with three detection techniques is designed in this paper.

![Figure 1. The architecture of the power grid industrial control system.](image)

2.2 Common security issues
Common problems are caused in three aspects: system network, system platform and security vulnerabilities. Network problems of ICS involve unreasonable design of network structure, inadequacy of physical protection of hardware equipment or improper network configuration[4][11]. System platform problems are reflected in the lack of intrusion detection, maintenance and testing. Additionally, there is a failure to update protection programs in time[4][11]. For the security vulnerability problem, the vulnerability database needs to be updated and maintained frequently, which is not suitable for the industrial control environment. The result is always a lag in vulnerability detection and defense. Besides, the high frequency of scanning brings more burden and scanning cost to be solved.

2.3 The optimized solution to power grid
Vulnerability scanning technique first looks for open ports and services by sending probes, and then scans after discovering the list of available services for further information, including configuration weaknesses, known vulnerabilities and encryption weaknesses. Finally, a report is returned to the user and the corresponding solution to the problem is provided. The basic principle is shown in figure 2.

![Figure 2. The basic principle of vulnerability scanning.](image)
The common national information security vulnerability database includes Common Vulnerabilities and Exposures (CVE), China National Vulnerability Database (CNVD) and China National Vulnerability Database of Information Security (CNNVD)[5]. These three databases are the national information security database used in vulnerability analysis and scanning and provide strong data support for the basic security services in China. This paper proposes an optimized solution to power grid combining three kinds of vulnerability database to form its own database, and automatically matches the integrated database according to the type, the address of the equipment and so on, so as to detect whether there is a known vulnerability.

3.Research and design based on three detection techniques
In this section, the principles and application of the new detection method are presented.

3.1 The design of system architecture
The designed system consists of six modules: task management module, ICS detection module, data transmission module, policy management module, report generation module and log management module.

The task management module is responsible for arranging the testing plan module. The data transmission module is in charge of the information interaction between the modules. The policy management module can set the scanning strategy. The report generation module is to store and export the data when the system discovers and analyzes all kinds of security hidden dangers. The log management module provides storage of user's operation records and the view operation function.

The detection module of system is a very significant module in detection technique. It is responsible for collecting the basic information of target system. We focus on the combination of passive detection, fusion detection and connectionless detection. The system architecture is shown in figure 3. Since scanning technique needs to send a large number of packets in the detection of the surviving host and the determination of the open port, it will interfere with the normal service. Also, it will produce a lot of overhead and the scanning speed is too slow. Therefore, the power grid must be adjusted accordingly. A new comprehensive technique is designed to collect basic information.

3.2 Passive detection
The traditional vulnerability scanning is mainly active scanning which has more cost. Due to the shortage of traditional scanning technique, this paper designs a passive device scanning scheme. The principle of this design needs to add data acquisition module or listener to read information in the network architecture with no need for active detection packets. The device can be identified according to device properties, firmware, communication protocol and other information.

ICS detection mainly depends on the PROFINET real-time protocol, which is the industry technical standard for data communication through industrial Ethernet. It aims to collect data from industrial systems and control equipment. It is especially good at completing data delivery in time[6]. During the process of network detection, the protocol packets PROFINET are actively monitored by listeners and the basic information can be extracted based on the design principle of passive detection. The information includes the type of industrial control equipment, station name, device address and so on. The equipment type of PROFINET consists of IO controller, IO monitor and IO equipment itself. This

Figure 3. The system architecture of the comprehensive detection technique.
process can detect the device only by passive monitoring of protocol package shown in figure 4.

**Figure 4.** The process of passive detection of industrial control system.

### 3.3 Fusion detection

TCP packet has a segment header and a data section shown in figure 5. The header section contains a 20-byte required field and an optional extension field. The data section is to transmit with payload which is after the first part. Fusion detection associates scanning behavior with normal business by trying to connect to public ports that support industrial control protocols. The data packet sent during scanning is partly integrated into the vulnerability scanning behavior and also meets the requirements of the industrial control protocol. The segment header of the packet conforms to the TCP protocol[7].

**Figure 5.** The structure of TCP packet.

Modbus is used by many sites for transmission since its simplicity and open use. Modbus TCP protocol is produced which can send and receive Modbus Serial data by combining with the TCP protocol under the modernization. Modbus TCP enable Modbus protocol to be transmitted on TCP/IP Ethernet utilizing TCP/IP model in the communication. Finally, the ICS transport layer can use TCP communication protocol to complete data transmission or service. To take the email sending as an example in figure 6(a), the user A sends B an email. Attaching a TCP header to the front of the application layer data, TCP provides a reliable transmission from application layer to the target port with the message “I’m Deeson” smoothly. Figure 6(b) shows the data section is replaced by vulnerability scanning behavior in fusion detection.

**Figure 6.** (a) Data flow of normal business, (b) Data flow incorporating the scanning behavior.
3.4 Connectionless detection

3.4.1 Connectionless scanning
The connectionless scanning mode, that is, ACK scanning, sends ACK package directly to the target port. Since the TCP/IP should be initiated by the SYN package according to the protocol state, the port receives SYN as an exception. If the target port is closed, there is no response. If the target port is open, it will send RST. The status of the port can be distinguished[8] according to the response of the server. A schematic diagram of the TCP connectionless scanning is shown in figure 7.

![Figure 7. Connectionless scanning (a) closed port, (b) open port.](a)

3.4.2 Identification of ICS based on connectionless scanning
In industrial control networks, the situation is different. ICS protocols are mainly used to interconnect equipment and systems in different suppliers. Modbus protocol[10] is a general communication protocol which has been widely used in ICS. It describes the process of a controller requesting access to other devices, how to respond to requests from other devices, and how to detect errors and record them. It requires establishing a TCP connection between the client and the server adopting master-slave communication. Since the Modbus TCP is based on TCP communication, it is necessary to establish a complete three-way handshake process. After shaking hands, the client sends three Modbus requests to the server without waiting for the first request for reply. After receiving all the replies, the client normally closes the connection[9]. Figure 8 shows a complete Modbus TCP communication process. Under the principle of TCP three scanning modes, if the server receives abnormal packets (ACK), the server cannot return the response when the target port is closed or returns an exception response otherwise. Thence, the system can identify the status of the port only utilizes the protocol stack to deal with the abnormal data packet. This kind of approach doesn’t need to complete 3-way handshake process. It reduces a lot of overhead in packet, improves scanning speed and is not easy to detect, so it is an ideal method for port scanning.

![Figure 8. The complete process of Modbus TCP communication.](a)

4. Performance analysis
The results analysis about the proposed comprehensive method are as follows:
- Improvement of scanning concealment:
  The required data is obtained through the data acquisition module or listener and there is no need to participate in any network flow for active detection. It has the extremely high concealment.
- Reduction in the cost of scanning:
  By using passive detection, the system extracts information from the packets and does not need to
send active detection packets which can reduce the cost of scanning.

- Avoidance of business interruption losses:
  Fusion detection not only completes the vulnerability scanning, but also does not trigger the vulnerability of the equipment. Thence it can avoid the influence of abnormal operation.

- Improvement of scanning speed:
  The scanning speed is improved and relatively stable without 3-way handshake. The speed does not change with the different number scanning systems. Thus, it can save scanning time.

5. Conclusions
The interconnection of smart grid is gradually enhanced but there is no special information protection construction. So, the risks and threats faced by power grid ICS are expanding. Based on these, a comprehensive vulnerability scanning system with a low cost and high efficiency is proposed through architecture design, module introduction, principle analysis and detection combination. It can improve the accuracy and ensure to detect the vulnerabilities in time, reduce resource utilization and cost.

In future, more research is needed to improve the security. A variety of information security means such as formation security products deployment, multiple security lines settings can also be utilized in order to guide smart grid information security to a new defense stage.

Acknowledgments
This work was supported by the science and technology project of State Grid Corporation of China "Development of special cyber security toolbox for electric power supervisory and control system" (Grand No. 525500190016).

References
[1] Wu J.Q., LI X., Zhan Z.H., Xie Xiang., Wang T. (2019) Research of information security in the power industry control system. Journal of AnHui electrical engineering professional technique college, 24: 123.
[2] Wikipedia. Concept and introduction of industrial control system. (2020) https://en.wikipedia.org/wiki/Industrial_control_system.
[3] Zhong Z.S., (2017) Security monitoring technology of power grid industrial control system based on network traffic abnormal detection. Electric power ICT, 15: 99.
[4] WIN ICS SECURIT. (2017) Common safety problems in industrial control system. https://www.sohu.com/a/160988596_723268.2020.09.14.
[5] Jia B.L., Huang S.P. (2020) Research on design of internet industrial control vulnerability scanning system. Process automation instrumentation, 41: 105.
[6] Wikipedia. The concept and introduction of PROFINET. (2020) https://en.wikipedia.org/wiki/PROFINET. 2020.09.24
[7] Wang C.D., Zhang X.F., Luan S.Q. (2019) Application of lightweight scanning technology in industrial control network. China academic journal electronic publishing house, 38: 87.
[8] Chen Z. (2018) Design and realization of scanning platform of industrial control system based on stateless connection. Network Technology Research Institute, 10–11.
[9] Zhang L. (2016) Basics of Modbus and Modbus/TCP. https://wenku.baidu.com/view/c2a9e1cc376ba1f6d4fad5c.html.
[10] Thomas M., Rayford V., Yoginder D. (2012) A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems. In: 2012 45th Hawaii International Conference on System Sciences. Hawaii. pp. 2338-2345.
[11] Peng J., Liu L. (2011) Industrial Control System Security. In: 2011 Third International Conference on Intelligent Human-Machine Systems and Cybernetics. Zhejiang. pp. 156-158.