A vulnerability scanning scheme based on attack graph for smart grid industrial control system

Kai Xu*1, Xiangqun Wang23, Hao Xu1, Ning Dong4, Meng Han1 and Xianfei Zhou1

1 State Grid Beijing Electric Power Company, Beijing, 100031, China
2 Global Energy Interconnection Research Institute Co. Ltd, Nanjing, 210003, China
3 State Grid Key Laboratory of Information & Network Security, Nanjing, 210003, China
4 Corresponding author’s e-mail: xukai1468@126.com

Abstract. As the core of national development, smart grid industrial control system has extremely high security requirements. However, due to the existence of many security vulnerabilities and lack of effective security protection measures, it is vulnerable to attacks from the Internet. Therefore, the vulnerability scanning of smart grid ICS has important research significance. Aiming at the problem that the smart grid ICS cannot bear the heavy system overhead, a safe and low system overhead vulnerability scanning scheme for smart grid ICS is innovatively proposed. This scheme introduces attack graph technology into vulnerability scanning, proposes vulnerability risk assessment indicators, and flexibly designs the scanning cycle according to the generated attack graph. Simulation results show that this scheme effectively reduces scanning costs while ensuring system security, and is better adapted to smart grid ICS.

1. Introduction
The electric power industry is the most important basic energy industry related to the economic development and social stability of a country, which is also the core of the country’s infrastructure[1]. The smart grid industrial control system is a typical industrial control system (ICS), which is an automatic control system composed of a computer and industrial control components together. However, the proposal and promotion of smart grids make ICS face higher security requirements. There are many security vulnerabilities in the smart grid ICS, and lack of effective security precautions. Once these vulnerabilities are exploited by criminals, it will have a serious impact on the national economy and politics. In 2010, the "Stuxnet" virus caused serious damage to Iran's nuclear power plants. In December 2015, the Ukrainian power grid was maliciously attacked by hackers, causing widespread power outages in residential areas. Therefore, the vulnerability scanning of smart grid ICS has important research significance.

Research on the safety of electric power systems is still in its infancy, but as a typical ICS, the existing research on ICS can be used as a reference for electric power system safety detection. Byres[2] et al. proposed an vulnerability assessment method based on attack tree for ICS. This method is suitable for ICS using Modbus and Modbus/TCP communication protocols. It describes the attack process through an attack tree model and helps security personnel take appropriate reinforcement measures. Wang[3] proposed a kind of ICS vulnerability scanning method based on hierarchical detection by studying the PROFINET real-time communication ICS protocol. It can better find the vulnerabilities in ICS. Jia[4]...
proposed a design process and system architecture scheme for the vulnerability scanning system of ICS, which meets the concurrent requirements of scanning through cluster deployment and multi-level storage structure and improves the scanning efficiency.

However, most of these studies did not consider the burden of vulnerability scanning for ICS. Unlike IT systems, smart grid ICS, has high requirements for business continuity and cannot withstand the burden of frequent scanning by traditional vulnerability scanners. Aiming at the problem that the smart grid ICS cannot withstand the system burden caused by too frequent vulnerability scanning, a smart grid ICS vulnerability scanning scheme based on attack graph is designed. This scheme includes a system information collection and processing module, an attack graph automatic generation module, and a smart grid ICS vulnerability scanning module. Attack graph technology is uniquely introduced into vulnerability scanning. Based on the generated attack graph, vulnerability risk levels of nodes in the target system are evaluated, and different scanning cycles are designed for nodes with different risk levels according to the evaluation results. Relatively frequent scanning is only performed for nodes with high risk levels, which can effectively save scanning cost.

The remainder of the paper is organized as follows: Section 2 introduces the smart grid ICS architecture and typical vulnerabilities, and describes the design of the vulnerability scanning scheme. Section 3 simulates the typical attack case of "Stuxnet" electric power as a prototype, and evaluates the time cost and security of the scheme proposed in this paper. Section 4 gives the final conclusion.

2.Materials and Methods

2.1 System architecture and vulnerability analysis

The smart grid ICS is an automation and remote control system composed of industrial control components and computer equipment. Its architecture is similar to a typical ICS. It consists of a Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS) and other control systems configured on key infrastructure, such as Programmable Logic Controller (PLC), etc.[6][10]. In the smart grid, the SCADA system is the communication network and the core of substation detection.

The network architecture of a typical smart grid ICS is shown in figure 1.

![Figure 1. Structure of typical smart grid ICS network](image)

As shown in figure 1, the smart grid ICS mainly includes power generation, transmission, transformation, distribution, power consumption and dispatching departments. It can be divided into production control system and management information system. There is one-way security between these two systems isolation. The production control system can be divided into real-time control zone I
and zone II, with logical isolation between zone I and zone II. Zone I includes dispatch automation system, power distribution automation system, etc. The management information system mainly includes the dispatching, monitoring and management network and the electricity consumption information collection system. Different security areas are set up according to different business requirements and logically isolated[7].

The primary task of the power system is to ensure the continuous operation of the system. There are a large number of known or unknown security loopholes in the smart grid ICS, and there is a lack of effective security protection methods. According to the description of vulnerabilities in the National Institute of Standards and Technology (NIST) report[7], the vulnerabilities of smart grid ICS can be divided into three categories: strategy and program vulnerabilities, system platform vulnerabilities and network vulnerabilities.

2.2 Overall design
Because of the high requirements for business continuity and limited system resources, the smart grid ICS cannot afford the excessive scanning overhead. In order to solve this problem, a vulnerability scanning scheme based on attack graphs for smart grid ICS is designed. This scheme abandons the fixed scanning cycle in the traditional scheme, but evaluates the vulnerability risk level of each node based on the generated attack graph, and designs different scanning cycles for nodes with different risk levels. This makes vulnerability scanning pay more attention to nodes with high risk levels, saving overall scanning overhead.

Attack graph is a technique for modeling system attack behavior in the form of graph, and it is often used for system vulnerability assessment. The attack graph analyzes the possible security threats and attack paths of the system based on the known information in the system, such as network topology, host reachability, and vulnerability scan reports, and displays them in a graphical manner[8].

This scheme is based on the MulVAL engine to generate attack graphs. MulVAL was designed by Qu et al.[9] based on the logic programming language Datalog. This tool can automatically generate attack graphs of target system based on files conforming to the Datalog syntax, and supports output in txt, pdf, eps, XML and Graphviz formats[8]. However, the MulVAL engine was originally designed for IT systems, so this article adjusts it to be suitable for smart grid ICS. The attack graph generated by the MulVAL engine has a large number of nodes and the relationship between nodes is complex. In order to facilitate subsequent analysis, this scheme optimizes the original attack graph.

This scheme proposes a vulnerability risk level evaluation index. Based on the optimized attack graph, the vulnerability risk level of the target system node is evaluated, and different scanning cycles are designed according to different risk levels. The design of the scheme is more flexible than the single scanning cycle design of the traditional periodic vulnerability scanning scheme, and can effectively save system overhead.

The overall frame design of the program is shown in figure 2. The program can be divided into three modules: system information collection and processing module, attack graph automatic generation module, and smart grid ICS vulnerability scanning module. The functions of each module are described as follows.

![Figure 2. Framework of vulnerability scanning scheme](image-url)
2.3 Design of each module

2.3.1 System information collection and processing module
This module mainly provides data support for attack graph generation. This module is composed of the smart grid ICS related vulnerability database, the vulnerability scanning report and the network topology information of the target system. In order to make the generated attack graph more accurate, the vulnerability database also contains the vulnerability information related to the smart grid ICS in the US National Vulnerability Database (NVD), the US Information Security Vulnerability Portal (CVE), and the National Information Security Vulnerability Sharing Platform (CNVD) vulnerability database. The scan report selects the scan report generated by the Nessus scanner. The network topology information is obtained by the network topology scanning tool, and the information is used as the input of the attack graph generation module.

2.3.2 Attack graph automatic generation module
This module is to generate the attack graph of the target system and provide support for the subsequent node vulnerability risk level assessment and vulnerability scanning scheme design. It is designed based on the MulVAL attack graph inference engine. It takes the collected information of the system information collection and processing module as input, adapts it through the smart grid ICS analyzer, and then combines its own attack rule library for logical reasoning to generate an attack graph and output in the required format. The output attack graph is used as the input of the vulnerability scanning module of the smart grid ICS for subsequent optimization and analysis.

In order to complete the adaptation of the smart grid ICS, this scheme refers to the paper[8] to design the smart grid ICS adapter. The adapter designs the smart grid ICS authority rule library according to the grammar and rule format supported by the MulVAL inference engine.

2.3.3 Smart grid ICS vulnerability scanning module
The design of smart grid ICS vulnerability scanning module framework is shown in figure 3.

![Diagram](image)

Figure 3 Framework of smart grid ICS vulnerability scanning module
This module first optimizes the original attack graph. It has too many vertices and the relationship between the vertices is complicated, which is not conducive to subsequent analysis and utilization. Therefore, referring to the optimization method in the paper[8], the final result is that only the host is the vertex. Optimize the attack graph as a basis for node risk assessment.

According to the optimized attack graph, each host is used as a node to evaluate the vulnerability risk level of each node in the system. For this reason, a node evaluation index: vulnerability risk level is proposed. This indicator is designed with reference to the paper[5]. The vulnerability risk level includes the probability of vulnerability being exploited and the exploit value of the vulnerability.

The probability of exploiting a vulnerability refers to the probability of an attacker successfully launching an attack using the vulnerability, which is calculated by the defense strength, the probability of the vulnerability, and the cost of the attack. Vulnerability exploit value refers to the degree of damage to the system after the vulnerability is successfully exploited by the attacker. It is related to the actual value of the component where the vulnerability is located in the target system and the vulnerability attack mode, and its value range is \((0,1)\).

Vulnerability risk value refers to the loss caused to the system after the vulnerability is successfully exploited. Its calculation can comprehensively refer to the above two indicators, and the vulnerability risk value can be expressed as:

\[
P = p_i \times q_i \quad (1)
\]
In equation (1), $P$ represents the vulnerability risk value, $p_i$ represents the probability of vulnerability $i$ being exploited, and $q_i$ represents the exploit value of vulnerability $i$.

According to the vulnerability risk value and expert opinions, the nodes in the target system are divided into three vulnerability risk levels: high, medium, and low. With reference to different risk levels and expert opinions, design different scanning cycles for nodes with different vulnerability risk levels, and adjust them in real time according to the actual situation of the target system. The entire vulnerability scanning process does not affect the normal operation of the system, and a scanning analysis report can be generated, showing the type of vulnerability and the corresponding risk level, and providing reference for vulnerability repair.

3. Results & Discussion

In this section, a typical attack case of “Stuxnet” smart grid ICS is taken as an example to evaluate the designed smart grid ICS vulnerability scanning scheme from the aspects of scanning scheme overhead and security. The simplified simulated attack scenario of “Stuxnet” is shown in figure 4.

![Figure 4. Attack scenario of simulated "Stuxnet" case](image)

The ultimate goal of “Stuxnet” is to destroy key power generation facilities by changing the speed of the centrifuges enriching uranium. Therefore, it is necessary to use various loopholes in the smart grid ICS to control the PLC directly connected to it. Refer to paper [8], the attack process of the "Stuxnet" case is: first, the attacker penetrates into the target network and infects a host through a USB device infected with Stuxnet virus. Then use the exploitable vulnerabilities to obtain the control authority of the PLC in the target system. In the end, the attacker used a directly connected PLC to control key industrial facilities and carry out attacks. In order to make the simulation effect clearer, unnecessary system components are omitted during the simulation.

As shown in figure 4, the simulated "Stuxnet" attack case is divided into two levels: internal network and external network. The attacker launches an attack from an external network. The internal network is a typical smart grid ICS. The attacker penetrated the internal network through a virus-infected USB device. The vulnerability information contained in the system is as follows:

| Vulnerability number | Position | Vulnerability information | Vulnerability description |
|----------------------|----------|---------------------------|--------------------------|
| 1                    | l1       | CNNVD-201007-238          | Microsoft Windows multiple product shortcut LNK file automatic execution file vulnerability |
| 2                    | p1, p2   | CNNVD-201009-132          | Windows Print Spooler service input verification vulnerability |
| 3                    | r1, r2   | CNNVD-200810-406          | Windows Server service RPC request buffer overflow vulnerability |
| 4                    | r1       | CNNVD-201007-241          | System hard-coded password permissions and access control vulnerabilities(Only exists in the winCC system and PCS 7 SCADA system) |

The vulnerability information listed in table 1 is described in detail in the China National Information Security Vulnerability Database (CNVD) and the United States National Vulnerability Database (NVD).
This article gives the vulnerability numbers in CNVD.

MulVal supports scan reports generated by Nessus and OVAL. Nessus can be used to scan the target system for vulnerabilities and obtain a scan report in xml format, which is then converted into an input file of Datalog syntax supported by MulVAL, and an attack graph is generated. This article directly edits the MulVAL configuration file according to the input Datalog syntax, and optimizes the original attack graph generated. The optimized attack graph obtained is shown in figure 5.

![Smart grid ICS optimization attack graph of simulated "Stuxnet" case](image)

Figure 5. Smart grid ICS optimization attack graph of simulated "Stuxnet" case

An important configuration in this simulation is the WinCC working environment of the r1 host. "Stuxnet" virus uses a hard-coded vulnerability (CNNVD-201007-241) to attack the PLC. This vulnerability only exists in winCC-related versions of the system. WinCC is an operating system based on the Windows platform, which provides monitoring and data collection for the target system. For comparison, this vulnerability is not configured for the r2 host in the simulation of this article. Analyzing and optimizing the attack graph shows that there are a total of 5 vulnerable nodes in the simulation system. When the target of the attack is to destroy key power generation facilities by controlling PLC, there are two possible attack paths: l1-r1-PLC2 and l1-r1 -PLC3, because r2 does not have hard-coded vulnerabilities, PLC4 is not attacked.

The node vulnerability risk level evaluation method proposed in the previous section is used to evaluate the nodes in the simulation system. The evaluation results are shown in table 2.

| Node name | Risk level |
|-----------|------------|
| l1        | high       |
| p1        | Medium     |
| p2        | Medium     |
| r1        | Medium     |
| r2        | low        |

According to the node vulnerability risk level evaluation results in table 2, combined with expert opinions, a feasible vulnerability scanning scheme specifically for the target system is given below. Assuming a single scan period is T, then for the high-risk node l1, the scan period is set to T; for the medium-risk nodes p1, p2, the scan period is set to 2T; for the low-risk node r2, the scan period Set to 3T.

First, evaluate the time cost of the scheme proposed in this paper and compare it with the time cost of the traditional IT system scanning scheme. The comparison results are shown in table 3.

| Scanning plan | Scanning overhead |
|---------------|-------------------|
| Traditional IT system scheme | 5p |
| Our scheme    | 7/3p |

In the "Stuxnet" simulation case, the number of nodes is 5 and all the hosts in the system are reachable. Assuming that the system overhead of scanning each host using the same vulnerability scanning technology is p. The traditional IT system vulnerability scanning solution scans all hosts in the network every time it scans, and the system overhead caused by scanning every T time period is equal to the order of the number of all hosts in the system, that is, 5p. The scanning scheme designed in this paper only scans for part of the hosts during each scan, and the average system overhead caused by scanning in each T time period is 7/3 p, which is significantly less than the scanning overhead of traditional IT systems. It can be seen that the vulnerability scanning scheme for industrial control systems designed in this paper can effectively save system overhead.

In addition, the vulnerability scanning scheme designed in this paper is based on the vulnerability
database of the US National Vulnerability Database (NVD), the US Information Security Vulnerability Portal (CVE), and the National Information Security Vulnerability Sharing Platform (CNVD) vulnerability database to compare vulnerabilities to ensure comprehensive, accurately match the latest smart grid ICS vulnerability information to ensure the accuracy of the vulnerability scan results and the security of the system.

4. Conclusions
Aiming at the problem that smart grid ICS has high security requirements and many security vulnerabilities, but cannot afford excessive scanning overhead, the attack graph technology is introduced into smart grid ICS vulnerability scanning. And a vulnerability scanning scheme based on attack graph for smart grid ICS is proposed. This scheme uses MulVAL engine to generate attack graphs based on multiple public ICS vulnerability databases, which can be well adapted to smart grid ICS. And the vulnerability risk level evaluation index is proposed to evaluate the nodes in the system based on the optimized attack graph, and the scanning cycle is flexibly designed according to the node vulnerability risk level. This scheme abandons the single scan cycle design of the traditional scheme. While ensuring the safety of the smart grid ICS, it effectively saves the system overhead of vulnerability scanning, and is better suitable for the security detection of the smart grid ICS.

In the follow-up study, we will focus on the lightweight scanning of the smart grid ICS to further reduce the burden on the system.

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] Yang, Y. (2019) A Thesis for the Master Degree of Science in Engineering. Shenyang Ligong University: 1-3.
[2] Byres, E., Franz, M., Miller, D. (2004) The use of attack trees in assessing vulnerabilities in SCADA systems. ResearchGate.
[3] Wang, H.H. (2015) Research on Vulnerability Scanning Technology of Industrial Control System. Beijing University of Posts and Telecommunications: 8-10.
[4] Jia, B.L., Huang, S.B. (2020) Research on Design of Internet Industrial Control Vulnerability Scanning System. Process Automation Instrumentation, 41:103-106.
[5] Peng, H. (2019) Research on Risk Assessment Method of Industrial Control System. Civil Aviation University of China.
[6] Zhang, Z.G. (2019) Research on Intelligent Network Security Situation Awareness Technology for Power Monitoring and Control System. Information Engineering University.
[7] Keith, S., Victoria, P., Marshall, A. (2015) Guide to industrial control systems (ICS) security. NIST special publication 800(82r2).
[8] Wang, J.T. (2016) Research on Attack Graph Vulnerability Analysis Technology Applied to Industrial Control System. Beijing University of Posts and Telecommunications.
[9] Qu, X.M. (2005) A logic-programming approach to network security analysis. The U.S. Princeton University.
[10] Lai, Y.X., Liu J., Liu Z.H., Zhang J.W. (2020) Review on Vulnerability Analysis and Vulnerability Mining Technology of Industrial Control System. Journal of Beijing University of Technology, 46: 571-582.