Design of Adaptive Detection Algorithm for Mobile Social Network Security Vulnerability Based on Static Analysis

Fang Qian(✉), Qiang Chen, and Lincheng Li

Engineer of China Southern Power Grid Ultra High Voltage Transmission Company, Guangzhou 510000, China
qianfang202304@163.com

Abstract. In order to improve the accuracy of adaptive detection of security vulnerabilities in mobile social networks and achieve the ideal effect of high-precision adaptive detection of vulnerabilities, static analysis is introduced and an adaptive detection algorithm design of security vulnerabilities in mobile social networks based on static analysis is developed. Use plug-in technology to scan mobile social network ports, databases, operating systems, Web, security baselines, weak passwords, and industrial control systems to obtain network data. The abnormal data propagation rules are used to preprocess the scanned data and extract the network abnormal data. The static analysis of the extracted abnormal data defines the corresponding rules of network security vulnerabilities by building an abstract simulation of network applications, extracts the corresponding relationship between abnormal data and network security vulnerabilities, calculates the final score of network security vulnerabilities according to the basic evaluation utilization factor, and identifies and detects the security vulnerabilities of mobile social networks. The experimental analysis results show that the designed algorithm has a vulnerability detection rate of more than 90% with and without security protection mechanism, and the adaptive vulnerability detection rate is high.

Keywords: Static Analysis · Mobile Social Network · Loophole · Adaptive · Testing

1 Introduction

Nowadays, people can't live and study without social networks for a long time. Social networks are the hubs connecting people. The purpose of information transmission through software or websites via the Internet is social networks (SN). Social networks generally allow users to have their own network space to save and share relevant information, such as email, online cloud disks, etc. With the progress and application of intelligent mobile terminal devices, network sensors and other devices, the use of mobile terminal devices to access social networks has become the mainstream. People have also moved from the original social model to mobile social networks, so mobile social networks are

L. Yun et al. (Eds.): ADHIP 2023, LNICST 548, pp. 389–402, 2024.
https://doi.org/10.1007/978-3-031-50546-1_26

developed from social networks [1]. With the wide spread and use of social software such as WeChat, Weibo and QQ, the popularity of mobile social networks among people has been further promoted. With the combination of mobile devices and communication technology, people can access massive information anytime and anywhere using the network, which has a huge impact on people's social activities and work learning. Mobile social networks collect and summarize the information of mobile devices to achieve communication through social networks. Mobile networks provide various network services for mobile users, including LBS. In the global population of more than 7 billion, more than 77% of users can enjoy the services provided by the network. On this basis, mobile social networks have contributed a lot. It is precisely because of the large number of mobile social network users and the huge amount of information transmitted on the network, many security problems will arise when people use mobile social networks to experience the services brought by LBS.

In network security attacks, mobile social network nodes are the main targets of attacks. Since mobile social network nodes can receive all information on mobile network devices, and can realize real-time detection and analysis of information, it is considered that node detection plays a vital role in network security. However, there are many types of network nodes in mobile social networks, and most of them exist in a highly decentralized state in the network environment. With the increasing attention paid to the security of mobile social networks, the detection of security vulnerabilities of mobile social networks has become an indispensable and crucial part of Internet security. With the continuous increase of mobile social network data scale, mobile social network attacks have become more complex and diversified. Traditional vulnerability detection algorithms cannot meet the security detection requirements of mobile social networks. How to use new computer algorithms to quickly and accurately detect known vulnerabilities under massive data, and achieve effective prevention and security precautions against mobile social network attacks, has become a hot topic of research institutes and researchers. In the work of in-depth research in this area, we found that static analysis is a method of using mathematical methods to process and analyze data. Compared with other data processing methods, this method can improve work efficiency. By collecting a large number of mobile social network data samples, we can judge and identify whether the samples are abnormal, and through appropriate processing of data, we can improve the node's computing ability. The purpose of simplifying the calculation. Therefore, this paper introduces static analysis in this research, and designs an adaptive detection algorithm for mobile social network security vulnerabilities, with a view to improving the security of mobile social network node transmission information, and improving the ability to detect mobile social network security vulnerabilities.

2 Design of Adaptive Detection Algorithm for Mobile Social Network Security Vulnerabilities Based on Static Analysis

2.1 Mobile Social Network Security Vulnerability Scanning

Obtaining data is the first step of adaptive detection of security vulnerabilities in mobile social networks, which is a basic work. Here, we use network vulnerability scanning to obtain abnormal data. The scanning objects mainly include mobile social network ports,

databases, operating systems, Web, security baselines, weak passwords and industrial control systems. Considering the large scanning range and complex scanning object types, this time we use plug-in technology to obtain data, write plug-ins in C language, connect the plug-in interface with the network interface, and insert a plug-in for each scanning object, as shown in Table 1.

Table 1. Scan plug-in class table

Scan plug-in ID number	category	name	explain
1100	Port scanning	Port	Service analysis
1200	Database dictionary scanning	Dict	Oracle and MySQL vulnerability scanning
1300	system scan	NteBIOS	Windows vulnerability attack
1400	Web Scan	HTTP	Web Service Scan
1500	Security Baseline Scan	SNMP	Third party network access security analysis
1600	Weak password scanning	General	Scanning for weak passwords existing in the system
1700	Industrial control scanning	Overflow	Safety analysis of industrial control system

Table 1 shows that a plug-in file is constructed for each mobile social network vulnerability class. The plug-in file contains the vulnerability scanning function corresponding to the vulnerability of the mobile social network. The mobile social network can be scanned by calling the corresponding scanning function to avoid confusion of the plug-in during the mobile social network scanning [2]. Among them, plug-ins exist in the form of compiled Windows DLLs. Each plug-in has a corresponding plug-in identity document (ID), and a unique function name [3] is designed for each scanning function. The function name is the index value of the mobile social network vulnerability in the plug-in plus the plug-in ID. The prefix symbol of the function name is designed as "_" in the form of "_1 * 00 * *". The specific scanning process is shown in the following figure (Fig. 1).

Make the mobile social network running, and scan the network one by one according to the plug-in sequence in Table 1. First, scan the mobile social network ports, which are the entry end of mobile social network attacks. Use 1100 plug-ins to scan all network ports and analyze whether the network port service is normal. Second, scan and check the firewall, router and server in the network operating system environment [4]. Thirdly, use 1200 plug-in to scan database dictionary and detect system tables and fields in database dictionary. Fourth, in the development process, due to programming logic errors, the website has SQL injection, cross site, dark chain and other problems, which may cause the website and website data to be tampered with, core data such as account

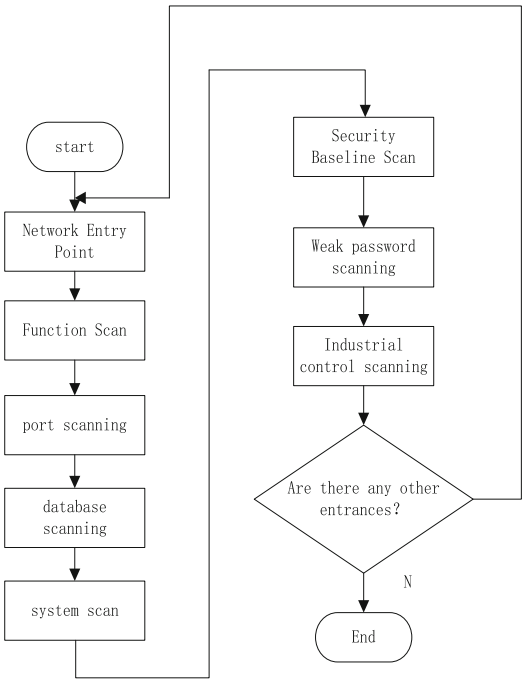

Fig. 1. Network Security Vulnerability Scanning Process

information to be stolen, the website server to become a dummy host and other problems. The 1400 plug-in can scan the website for Web vulnerabilities defined by OWASP Top 10. Fifth, security configuration verification is the basic work of security management and an important technical means of security operation and maintenance. Security configuration verification should first establish a baseline that meets the security configuration requirements of the organization's information security management system. Sixth, use the 1500 plug-in to scan the specific products of these support systems, such as Windows, Oracle, WebLogic, switches, firewalls, etc. Seventh, use the 1600 plug-in to detect the weak password existing in the system. The plug-in supports well-known protocols such as Telecom Network Work Protocol (TELNET), File Transfer Protocol (FTP), Secure Shell (SSH) protocol, Post Office Protocol Version 3 (POP3), Server Message Block (SMB)Simple Network Management Protocol (SNMP), Remote Display Protocol (RDP), Simple Mail Transfer Protocol (SMTP), Remote DictionaryServer (REDIS), Oracle, etc. The default dictionary library is built in and supports uploading customized dictionary library [5]. Eighth, use 1600 plug-ins to comprehensively scan industrial control systems, including Siemens, Schneider, AB, Rockwell, domestic Hollysys, central control and other mainstream programmable logic controllers (PLC), distributed control systems, DCS), Supervisory Control And Data Acquisition (SCADA) equipment, etc., to collect vulnerability attack data on current mainstream production business equipment and software.

Store all scanned data in the network vulnerability attack information database, edit the scanning file name according to different scanning objects, and store the scanned abnormal data by category for subsequent static analysis.

2.2 Exception Data Extraction

Abnormal data refers to data related to vulnerability attacks on mobile social networks. The mobile social network is in an abnormal state [6] when there is a vulnerability in the mobile social network, but it is not attacked by the mobile social network attacker. Therefore, the data obtained through scanning is not completely related to mobile social network vulnerability attacks, but may also include mobile social network vulnerability data, so it is necessary to extract valuable abnormal data from the scanned data. There are essential differences between the two types of data. When the mobile social network is attacked by vulnerabilities, the abnormal data in the mobile social network is dynamic. In order to achieve the attack task, abnormal data needs to be transferred from one location to another. The mobile social network has loopholes, but has not been attacked. At this time, the abnormal data in the mobile social network is static, and the abnormal data extraction is based on the data propagation rules. The abnormal data is extracted through data inspection. The following figure is the abnormal data extraction flow chart.

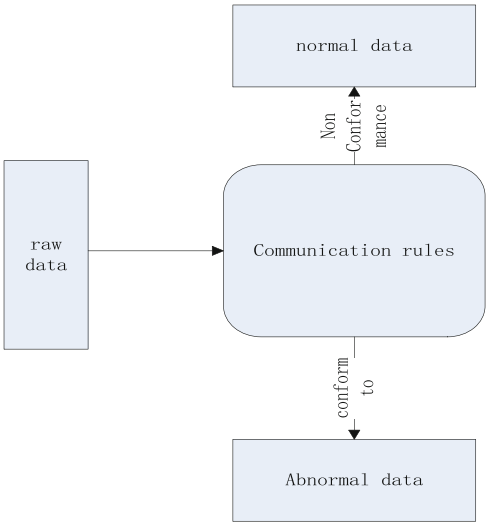

Fig. 2. Schematic Diagram of Abnormal Data Extraction

As shown in Fig. 2, the exception data propagation rule is designed according to the difference between the two, and the calculation formula of the rule is;

$$P_{uhd}(ins) = P_{uhd}(x, z) = isTa\text{int}(z) \tag{1}$$

Where, $P_{uhd}(ins)$ Represents the mobile social network exception data propagation rules; P_{uhd} Abnormal data indicating that there are instructions for mobile social network

access; x Indicates the memory address of read network access; z Indicates the address returned after the network instruction is executed; Use formula (1) to check the scanned data and whether it conforms to the rule [7]. If this rule is met, it will be determined as abnormal data generated by network vulnerability attacks, extracted and set up abnormal data sets.

2.3 Static Analysis of Abnormal Data

Using static analysis technology to analyze abnormal data, the mobile social network security vulnerability adaptive detection algorithm based on static analysis assumes that the abnormal data is contaminated data, and uses data flow to judge the value that can be controlled by the attacker. Therefore, it requires to know where the data enters the mobile social network program, how it is transmitted in the program, and finally the vulnerable operation. Static analysis is the key to identify many input validation flaws and represent flaws. In this way, if a mobile social network application contains an exploitable vulnerability, it almost always contains a path from receiving user input functions to vulnerable operations [8]. Therefore, vulnerabilities in mobile social networks can be detected through static analysis of abnormal data. The static analysis of abnormal data includes the following parts: (1) building an abstract simulation of the network; (2) Define the source rule, transmission rule, purification rule and receiving rule corresponding to the vulnerability; (3) Analyze mobile social network application vulnerabilities.

Since the mobile social network security vulnerability adaptive detection algorithm based on static analysis is a network data flow based detection algorithm, the network data flow model [9] must be established before vulnerability analysis. A mobile social network application can be represented as the mapping of HTTP requests and the current state of Web applications to replies, application dependency graphs, and new Web application states:

$$P_{uhd}(ins) : R \times S \rightarrow P \times E \times D \tag{2}$$

Where, R Represents HTTP requests submitted to mobile social network applications; S Indicates the current status of mobile social network applications; P Represents the HTTP reply of the mobile social network application; E Represents the control flow and data flow used by network applications to process a given HTTP request; D Indicates the status after the network application request is completed.

Exception data propagation includes a series of source rules, transmission rules, acceptance rules and purification rules, as shown in the following figure.

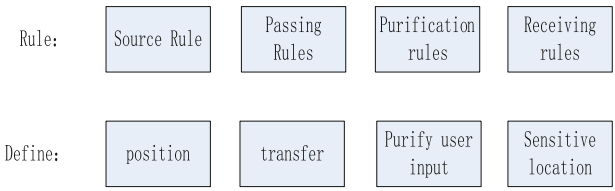

Fig. 3. Abnormal Data Rules

As shown in Fig. 3, these rules explain how the source function in the network generates pollution data, and how the receiving function is used. If the pollution data is not purified by the purification unit before being transmitted to them; It also explains how the pollution data is transferred through the transfer function. Source rules define where contaminated data enters the network application; The transfer rule defines the way in which the function manipulates the contaminated data, that is, how the contaminated data is transferred in the network; Purification rules define functions or modules used to purify user input in network applications to prevent potential cross site scripts. They are a form of transfer rules. The receiving rules define the sensitive locations of network applications that should not accept contaminated data. The source rules obtain data from HTTP requests. The receiving rules are used to return the obtained data to the client. In order to include other server information in the returned information, it is necessary to connect the string transmission rules [10]. Therefore, we can use the static analysis model to specifically describe the security vulnerability rules of mobile social networks.

According to the above description, the correspondence between the rules in static analysis and the mobile social network application in formula (2) can be formally defined:

$$P \rightarrow SS \cup DS \cup JS \cup RE = M \tag{3}$$

Where, SS Indicates the source rule of abnormal data; DS Indicates the transfer rules of abnormal data; JS Indicates the receiving rules of abnormal data; RE Represents the purification rule of abnormal data, M Represents the correspondence between mobile social network applications and exception data transmission rules [11]. The extracted exception data is statically analyzed according to the above process, and the corresponding relationship of the exception data rules in the mobile social network can be obtained.

2.4 Vulnerability Adaptive Detection

Use the above extracted correspondence to identify mobile social network security vulnerabilities, and the detection process is shown in the following figure.

As shown in Fig. 4, the vulnerability detection process reads the correspondence from the source file and parses it into automatic control rules. Match the scanned source code with the source code pattern in the correspondence. After successful matching, the pattern constraint will be checked [12]. When both pattern matching and pattern constraint are successful, trigger the pattern matching variable to bind the variable automatically to realize automatic state transfer. This process needs to analyze the environmental assessment indicators. Even in the same vulnerability, at the same time, in different environments, the vulnerability degree is different. Therefore, environmental assessment indicators must be analyzed during the transfer of bound variables. According to the environmental assessment index set, the basic assessment impact factors are calculated as follows:

$$Z = \min\{(M \times XR)(M \times YR)(M \times ZR)\} \tag{4}$$

Where, Z Indicates the security degree of mobile social network environment; XR Indicates confidentiality requirements; YR Represent integrity requirements; ZR Indicates availability requirements [13]. The basic detection results of mobile social network security vulnerabilities can be obtained by substituting formula (4) into formula (5):

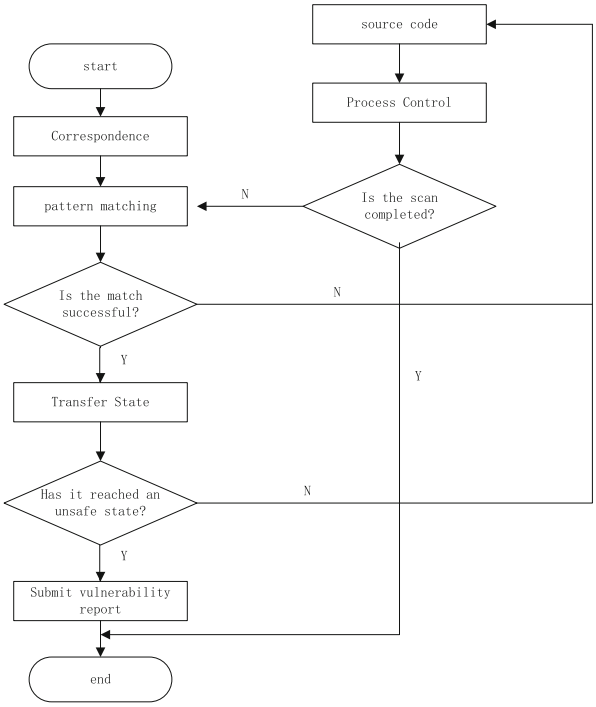

Fig. 4. Vulnerability Detection Flow Chart

$$H = (0.6Z + 0.4L) \times f \tag{5}$$

Where, H Represents the basic detection results of security vulnerabilities in mobile social networks; L Represents the basic detection utilization factor; f Represents the constant associated with the basic assessment impact factor. Basic detection utilization factor in the above formula L Is an unknown number, and its calculation formula is:

$$L = EV \times EC \times eu \tag{6}$$

Where, EV Indicates the propagation path of abnormal data; EC Indicates the complexity of abnormal data; eu Indicates the authentication strength of abnormal data. Substitute formula (5) into formula (7) to get the final detection results of mobile social network security vulnerabilities:

$$A = (H + H \times CDP) \times TD \tag{7}$$

Where, A Indicates the score of mobile social network security vulnerabilities; CDP Indicates measuring the potential impact of vulnerabilities; TD It indicates that vulnerability indicators exist in the potential harm of mobile social networks to the network [14]. Set the detection threshold according to the actual situation. If the calculated value of formula (7) is greater than the threshold, the output detection result is that the mobile social network has vulnerabilities; If the calculated value of formula (7) is less than

the threshold value, the output detection result is that there is no vulnerability in the mobile social network. According to the comparison between formula (7) and the detection threshold value, a vulnerability adaptive detection report is generated. When the self motivation reaches the unsafe state, the vulnerability report is submitted to the user [15]. If it does not reach the unsafe state, it will continue to scan the subsequent source code until the scanning is completed, so as to complete the design of adaptive detection algorithm for mobile social network security vulnerabilities based on static analysis.

3 Experimental Analysis

3.1 Experiment Preparation

In order to verify the reliability and feasibility of the mobile social mobile social network security vulnerability adaptive detection algorithm designed in this paper based on static analysis, the experimental analysis is carried out as shown below. The operating platform used in the experiment is the 32-bit Win7 flagship version, the experiment uses C # language, and the programming experimental platform is the VS2010 flagship version. The experimental data uses the test page provided in the Wavsep program. With a mobile social mobile social network as the experimental environment, the advantages of the research method in vulnerability detection rate are verified by automatically expanding the simulation attack mode. The construction of simulation attack set mainly depends on the identification and judgment of attack types by security experts. Each attack is a separate individual for research. The artificially expanded simulation attack process is shown in the following figure (Fig. 5).

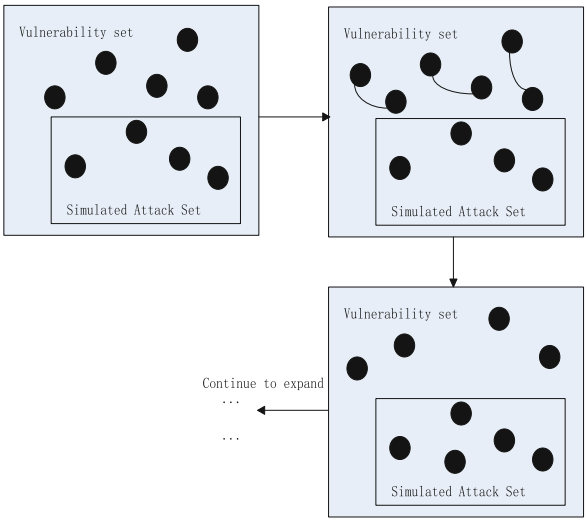

Fig. 5. Simulation attack process of manual expansion

As shown in the above figure, if the user enters a string when attacking the mobile social mobile social network, the final execution result will be obtained in the browser.

The process is as follows: enter the URL address in the browser address bar, add the refined string suffix, and the new page jump request in the string will be sent to the site business processor for processing. Send analysis request, and formulate jump strategy according to the analysis results. However, because the server does not deploy the corresponding security mechanism, the submitted URL string does not belong to the traditional jump request type. If there is a security vulnerability in the mobile social mobile social network application, the server will usually send a response, thus exposing sensitive information. By analyzing the response results returned to the client browser vulnerability, determine whether there is a corresponding vulnerability problem on the server side of the mobile social networking site. If the user constructs a string as the result of the jump request, when the customer browses the mobile social networking target website, the string in the browser address bar will be input and sent to the server, that is, an error query will be launched to the database, and the related information will be returned to the vulnerability injected by the external user through the browser.

In order to achieve the purpose of injection attack, the attacker must first find the vulnerability of the server side security mechanism. In terms of technical methods and formal rules of security scanning, their security verification mechanisms are similar, and they are all aimed at limited code, that is, the vulnerabilities covered by the simulation attack set used in security scanning are limited. The generation of different use cases is realized by deformation, so as to find the smallest set of simulated attacks. By studying the interrelationship between attack modes, a series of transformations and settings are carried out on the test case code to realize the vulnerability extension simulation process. In the experiment, the vulnerability data file of mobile social mobile social network includes 6 types of security vulnerabilities, namely NVD1.zip, Secunia2.zip, SecurityFocus3.zip, Cnvd4.zip, CNND5.zip, NSFocus6.zip. After the above design is completed, the initial parameters of the experiment are designed, and the specific parameters are shown in the table below.

Table 2. Table of Experimental Parameters

S/N	name	parameter
1	Vulnerability data load unit parameters	256
2	Initial value of vulnerability information sample mixing coefficient	1.25
3	Minimum carry value of vulnerability information	2
4	Number of security vulnerability types	6
5	Number of security vulnerabilities	90

During the experiment, the total transmission amount of vulnerability data annotation index in unit time is greater than or equal to 1, and the transmission order of vulnerability data does not change when the SQL annotation statement is executed, and the position of the encoding vector can only move from the first annotation node to the last annotation node.

3.2 Result Analysis

After the above experimental preparations are completed, the mobile social mobile social network security vulnerability adaptive detection experiment is carried out. The experimental execution process is as follows:

Step 1: Select the client PC: host as the experimental object, and connect it to the wireless LAN communication environment;
Step 2: Select the adaptive detection algorithm for security vulnerabilities of mobile social mobile social network based on static analysis as the application method of the experimental group;
Step 3: In order to make the experimental data and experimental results have a certain degree of explanation and reliability, two traditional algorithms are selected for comparison. The two traditional algorithms are the detection algorithm based on blockchain technology and the detection algorithm based on ant colony algorithm. The following are represented by traditional algorithm 1 and traditional algorithm 2 respectively, and the two traditional algorithms are used as the application methods of the control group;
Step 4: Design the experiment scenario, and the experiments are verified in this scenario.
Step 5: Explain the experimental equipment and parameters.
Step 6: Record the experimental values of the experimental group and the control group;
Step 7: Compare the experimental group and the control group to record the values and summarize the experimental rules. Next, set the evaluation indicators for this experimental test. In this experiment, the vulnerability detection rate is used as the evaluation index of three algorithms. In order to restore the vulnerability detection rate of mobile social mobile social network without security protection mechanism, no input URL filtering is added and no firewall is set, so as to test the vulnerability detection rate without security protection mechanism. Without adding any input URL filtering, the above three algorithms are used to analyze the vulnerability detection rate. The comparison results are shown in Table 2 (Table 3).

Table 3. Vulnerability detection rate of three algorithms without security mechanism (%)

Number of vulnerability samples	Design algorithm	Traditional algorithm 1	Traditional algorithm 2
10	98.8	65.4	68.4
20	97.6	62.5	64.2
30	96.8	58.4	60.2
40	96.3	56.3	55.6
50	96.4	55.1	52.4
60	95.2	51.4	50.3
70	95.1	48.5	47.5
80	94.3	45.3	44.4
90	94.1	42.7	41.2

From the data in the table above, we can see that the vulnerability detection rate of the algorithm designed in this paper is higher than that of the two traditional algorithms, and the number of detected vulnerabilities is basically consistent with the actual situation. The number of undetected vulnerability samples accounts for 6.9% of the total vulnerability samples, which is far lower than that of the two traditional algorithms. This is because the design algorithm utilizes plugin technology to scan mobile social networks and obtain network data. This technology can enhance the ability of vulnerability detection, enabling algorithms to better capture and identify vulnerabilities, and improve vulnerability detection rates. In contrast, traditional algorithms do not fully utilize plugin technology, resulting in a decrease in vulnerability detection rate.

In addition, in order to restore the vulnerability detection rate with security protection mechanism, it is necessary to use a dedicated line to connect the simulation software to the dedicated interface of the firewall to test the vulnerability detection rate of the three algorithms with security protection mechanism. Under the security protection mechanism, the above three algorithms are used to analyze the vulnerability detection rate. The comparison results are shown in the following figure (Fig. 6).

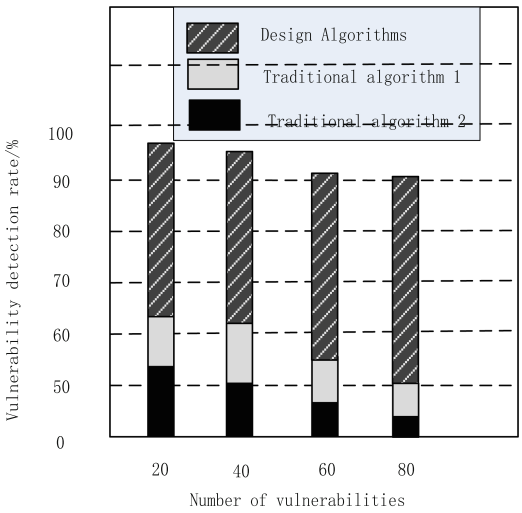

Fig. 6. Vulnerability detection rate of three algorithms with security protection mechanism

It can be seen from the above figure that under the security protection mechanism, for different vulnerability sample numbers, the comparison results of the vulnerability detection rate of the three algorithms are different. The vulnerability detection rate of the three algorithms decreases with the increase of the number of vulnerability samples, but the design algorithm is less affected by the number of vulnerability samples, and the vulnerability detection rate is always more than 90%, The vulnerability detection rate of both traditional algorithms decreases significantly with the increase of vulnerability samples. The vulnerability detection rate of traditional algorithm 1 can only be maintained at 50.3%–62.4%, and that of traditional algorithm 2 can only be maintained at 43.5%–54.6%.This is because the design algorithm in this paper adopts a static analysis

method, which can more comprehensively analyze and detect security vulnerabilities in mobile social networks by building abstract simulation of Web application and defining vulnerability corresponding rules. In contrast, traditional algorithms cannot fully utilize the advantages of static analysis.

From this, it can be seen from this that the vulnerability detection rate of the algorithm designed in this paper is high, which can comprehensively detect the security vulnerabilities of mobile social mobile social networks. The algorithm designed in this paper has good feasibility and reliability, and is more suitable for adaptive detection of security holes in mobile social mobile social networks than traditional algorithms.

4 Conclusion

With the continuous updating of modern Internet technology, the data volume of mobile social network is increasing, and the operational efficiency and security of mobile social network nodes are increasingly concerned. In depth research on this aspect, it is found that mobile social mobile social network will involve a large amount of data related to cloud computing when carrying or transmitting information. If the node data vulnerability is not detected in time, the security risks of mobile social mobile social network will not be found in time, thus causing the mobile social mobile social network to fail to operate normally. Therefore, how to effectively solve the security problems and reduce the risks in mobile social networks has become one of the important topics in the current scientific research field. For this reason, this article uses plugin technology to scan mobile social networks, obtain network data, and preprocess using anomaly data propagation rules to extract network anomaly data. Then, the extracted abnormal data is statically analyzed, and the corresponding rules of network security vulnerabilities are defined by constructing an abstract simulation of Web application, and the corresponding relationship between abnormal data and network security vulnerabilities is extracted. Finally, the final rating of network security vulnerabilities is calculated based on the basic evaluation utilization factor to identify and detect security vulnerabilities in mobile social networks. After the completion of the design, this method has proved through comparative experiments that it can achieve accurate detection of vulnerabilities in mobile social mobile social network nodes, and can be popularized in the subsequent mobile social mobile social network engineering field using this method instead of traditional methods. The research in this article is of great significance for addressing security issues, reducing risks, and promoting the development of mobile social networks. By proposing an adaptive detection algorithm for security vulnerabilities in mobile social networks based on static analysis, precise detection of node vulnerabilities in mobile social networks can be achieved, providing effective guarantees for the safe operation of mobile social networks.

References

1. Aslan, Ö., Aktuğ, S.S., OzkanOkay, M., Yilmaz, A.A., Akin, E.: A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics **12**(6) (2023)

2. Chen, G., Wang, H., Zhang, C.: Mobile cellular network security vulnerability detection using machine learning. Int. J. Inf. Commun. Technol. **22**(3) (2023)
3. Algarni, A., Thayananthan, V.: Autonomous vehicles: the cybersecurity vulnerabilities and countermeasures for big data communication. Symmetry **14**(12) (2022)
4. Jagannathan, J., Mohamed Parvees, M.Y.: Security breach prediction using artificial neural networks. Meas. Sens. **24** (2022)
5. Zheng, X.: Computer deep learning network security vulnerability detection based on virtual reality technology. Adv. Multimedia **2022 (**2022)
6. Xing, Y.: Design of a network security audit system based on log data mining. Wirel. Commun. Mob. Comput. **2022** (2022)
7. Guoyu, L., Luo, G.: Research on network security vulnerability detection method based on artificial intelligence. J. Phys. Conf. Ser. **1651**(1) (2020)
8. Shaaban, R., Faruque, S.: Cyber security vulnerabilities for outdoor vehicular visible light communication in secure platoon network: review, power distribution, and signal to noise ratio analysis. Phys. Commun. 40 (2020). (prepublish)
9. Telecommunications - Physical Layer Communications; Study Data from University of North Dakota Provide New Insights into Physical Layer Communications (Cyber security vulnerabilities for outdoor vehicular visible light communication in secure platoon network: Review, power distribution, and ...). Comput. Netw. Commun. (2020)
10. Saudi Arabian Oil Company: "Cybersecurity vulnerability classification and remediation based on network utilization" in patent application approval process (USPTO 20200162498). Technol. Bus. J. (2020)
11. Afreen, S.S.: Analytical study on network security Breach's. J. Trend Sci. Res. Dev. **4**(3) (2020)
12. Xing, W.: Research on computer network security vulnerabilities and preventive measures based on multi-platform. IOP Conf. Ser. Mater. Sci. Eng. **740** (2020)
13. Syed, R.: Cybersecurity vulnerability management: a conceptual ontology and cyber intelligence alert system. Inf. Manag. **57**(6) (2020)
14. FDA warns of urgent cybersecurity vulnerabilities with medical devices. Biomed. Saf. Stand. **50**(1) (2020)
15. Alvarez Valenzuela, D., Hevia Angulo, A.: Legal protection for the search and notification of cybersecurity vulnerabilities in Chile. Revista Chilena de Derecho y Tecnologia **9**(2) (2020)
16. Sun, H., Cui, L., Li, L., et al.: VDSimilar: vulnerability detection based on code similarity of vulnerabilities and patches. Comput. Secur. **110**(5–6), 102417 (2021)
17. Alaaraji, Z., Ahmad, S.S.S., Abdullah, R.S.: Propose vulnerability metrics to measure network secure using attack graph. Int. J. Adv. Comput. Sci. Appl. **12**(5), 2021 (2021)