Research on Technologies of Vulnerability Mining and Penetration Testing for Satellite Communication Network

Kun Dong¹, Haixia Zhang²*, Yanmei Liu¹, Yang Li¹ and Yuanyuan Peng²
¹. (China Satellite Communications Co. Ltd., Beijing 100190). 2. (Institute of Software, Chinese Academy of Sciences, Beijing 100190)
Email: zhanghx@tca.iscas.ac.cn*

Abstract. According to the specific characteristics of software, hardware and network protocols, the cyber security problems of satellite communication network have gradually attracted the attention of the industry in recent years. This paper proposes a technical framework including information collection and detection, vulnerability mining and penetration testing. It introduces mining methods such as taint analysis, symbol execution and fuzzy testing, and combines with machine learning algorithms to improve the efficiency and accuracy of vulnerability mining. It uses buffer overflow, SQL injection, cross-site attack and Trojan horse penetration to test the security of satellite communication network. It is helpful to improve the ability of proactive defense and security guarantee of satellite communication network.

1. Introduction
As a new type of information communication mode, satellite communication does not rely on the traditional ground communication network facilities, and has the ability of comprehensive coverage for special areas (such as ocean, mountain area, airspace, etc.), and has achieved rapid development in technology progress and application promotion in recent years. Several high-throughput broadband communication satellites have been launched in Europe and the United States. Some companies have completed the global layout of high-throughput satellite network. Because the bandwidth of military communication satellites in various countries is in a short period of time, renting commercial communication satellites has become a normal condition. Western military powers, including the United States, hire high-throughput satellites to satellite operators for military purposes.

In recent years, the security problem of satellite communication network has attracted more and more attention at home and abroad. In April 2014, the United States released a wake-up call for Satcom security [1]. The report points out that some equipment, including the U.S. military satellite network, has security risks. Through the security analysis of satellite communication terminal, several potential threats are found, including hard coded certificate, non-public protocol, insecure protocol and backdoor program, which can be used by attackers to intercept, tamper or block network communication, and even remotely control communication equipment.

In China, satellite communication system is also facing serious security threats, such as using software and hardware vulnerabilities to achieve intrusion, illegal access to system permissions, stealing user information and network information, illegal insertion of satellite relay content, and so on. In history, there have been actual attack cases, which have attracted the attention of relevant departments and operation units.
Because satellite communication system adopts special firmware equipment and software system, its networking mode and bearing application are significantly different from those of ground network. The implementation of intrusion infiltration work is more difficult, and it depends on the exploitation and utilization ability of zero day vulnerability of special system. Therefore, it is necessary to carry out vulnerability mining and penetration analysis for satellite communication network communication, and master the vulnerability of relevant firmware, application software and network protocol, so as to provide support for the security risk investigation, active defense and network attack and defense of satellite network.

The second chapter focuses on the technical status of vulnerability mining and penetration testing, and proposes the technical framework for related work. The third chapter introduces the information collection and detection scanning methods for satellite communication network. The fourth and fifth chapters respectively describe the technical methods of security vulnerability mining and penetration testing for satellite communication network. Finally, the full text is summarized.

2. Technical Framework

Vulnerability mining refers to the use of technical means to analyze the security vulnerabilities of software and hardware equipment, and detect, find and locate the vulnerability of software and hardware equipment in the process of design, development, operation and maintenance that can be exploited by attackers or lead to equipment failure. The existing vulnerability mining techniques can be divided into static analysis technology and dynamic analysis technology according to whether the target program is executed.

Static analysis technology is the use of source code scanning tools, through control flow analysis, lexical analysis, syntax analysis and other analysis techniques to find the security vulnerabilities in the program, which is the basic technology of high-level programming language and program detection. Common static analysis techniques include: source code scanning [2], static Taint Analysis [3], static symbol execution [4], etc.

Dynamic analysis technology includes fuzzy test [5], dynamic symbol execution [4], dynamic stain analysis [6]. With the continuous progress of machine learning technology, there are also some vulnerability mining technologies based on machine learning, including machine learning method, symbol execution, fuzzy testing and other technologies to improve the efficiency and accuracy of vulnerability mining.

Penetration test can directly find some security risks of the tested target, such as the vulnerability of various hardware and software equipment and management mechanism and the possibility of exploiting the vulnerability. It can also find the password vulnerability of various devices, the vulnerability of network equipment, and the defects of firewall device strategy, so as to evaluate the security of the tested network technical risk.

According to the target system of penetration testing, penetration testing technology can be divided into host operating system penetration, database system penetration, application system penetration, middleware penetration, network equipment penetration, network protocol penetration, etc. It can be divided into white box test and black box test according to the test personnel's mastery of the target system environment related information.

Black box testing is a penetration test of the target system without knowing any information about the system under test. All information about the target system needs to be collected and analyzed by testers themselves. Black box testing is mainly to simulate the behavior of foreign attackers attacking the system under test. Common methods include buffer overflow, password cracking, session hijacking, etc.

White box test is a penetration test on the target after the tester knows some relevant information of the tested system in advance (including network address segment, network protocol used, network topology, application system type, system version and configuration information, and even internal personnel information, etc.). White box test is mainly to simulate the operation behavior of attackers (including system insiders) who are familiar with the target system environment to attack the system under test.
The goal of vulnerability mining is to find known or unknown vulnerabilities in the system, while penetration testing is to use the vulnerabilities to achieve successful intrusion or control. Therefore, there is a close relationship between vulnerability mining and penetration testing. The former provides the basis for the latter to carry out the penetration work, while the latter provides the verification results of vulnerability availability for the former. At present, association technology can be divided into two categories: rule-based Association Technology [7] [8] and graph theory based association technology. Among them, the method based on graph theory can well display the relationship between the security elements, the path of successful penetration and the corresponding vulnerability information by analyzing the security status and behavior of the target network. The commonly used analysis models are attack tree model [9], privilege graph model [10], attack graph model [11].

According to the current domestic and international technology status in this field, this paper proposes a technical framework for satellite communication network vulnerability mining and penetration testing, as shown in Figure 1. The framework includes three levels of network information collection and detection, vulnerability mining and penetration testing, aiming at typical security protection objects in satellite communication networks such as basic network, satellite terminal, baseband equipment, customer service system, business operation support system, shipboard application system and airborne application system. The key technologies used in the three levels are described below.

3. Satellite Communication Network Acquisition and Detection Technology
The common means of network attack is to use the existing weak links such as security loopholes and configuration defects through information collection and vulnerability analysis of attack objects, so as to achieve the access and promotion of the target system permissions, obtain the required key data or destroy them, and realize long-term latent and control behaviors through Trojan horse and backdoor.
retention. Before attacking the target network, it is necessary to collect and summarize all kinds of information related to the target system to form the necessary outline knowledge of the target network and prepare for the implementation of the attack. The collection scope of information collection stage includes unit information, personnel information, network topology, equipment type, operating system, database, middleware, etc.

Satellite communication network acquisition and detection technology includes network detection, passive acquisition, vulnerability scanning and social engineering.

1) Network detection refers to exploring network assets and topology information through active remote way, including IP address, domain name, type, application service, configuration, network connection status, etc. Network detection has the advantages of large amount of information and accurate results, but it is easy to be detected by detection system due to sending a large number of exploratory data packets.

2) Passive Collection refers to the collection of network traffic to extract all kinds of information related to network security, including IP address, port, network connection, application protocol and domain name resolution records of traffic data. Compared with network detection, passive acquisition has strong concealment because it does not send data packets to the detection target, but the amount of information acquired by passive acquisition is often less than that of network detection.

3) Vulnerability scanning is the security related detection of computer system or other network equipment, in order to find out the security risks and vulnerabilities that can be used. Vulnerability scanning usually adopts information matching and exhaustive methods. Most vulnerability scanning adopts information matching technology, while a few vulnerabilities such as directory traversal vulnerability and information disclosure adopt exhaustive testing method. Based on the information matching of vulnerability database, the port opened by the target host and the network service on the port are obtained after the port scanning, and the relevant information is matched with the vulnerability database provided by the network vulnerability scanning system to check whether there are vulnerabilities that meet the matching conditions. Vulnerability scanning aims at network protocol, operating system, database, application system and other objects, including CGI vulnerability scanning, POP3 vulnerability scanning, FTP vulnerability scanning, SSH vulnerability scanning, HTTP vulnerability scanning, etc., and background address scanning is also performed to facilitate password cracking. In the vulnerability scanning stage, the scanning tool needs to collect the type, version and other information of the system under test, which can make full use of the results of the information collection stage.

4) Social engineering refers to the acquisition of sensitive information related to the target system, such as units, personnel, network access, system configuration and other non-technical means, including the name, address, mailbox and other public information of the unit, as well as system information such as network topology, access mode, application service, operating system type, and even collecting the identity information, telephone number, home of the system administrator Personal privacy data such as court address, birthday, etc. These data may help the attacker guess the system password or carry out the next attack.

Table 1 shows the collection capabilities of the above four methods for different types of information. For satellite communication network, network detection and vulnerability scanning are more effective in obtaining system security information. Social engineering helps to collect information of organization and personnel, while passive collection is more as a supplementary way to collect system data on the premise of ensuring concealment.
| Information type               | Network detection | Passive acquisition | Vulnerability scanning | Social engineering |
|-------------------------------|-------------------|--------------------|-----------------------|-------------------|
| Domain info                   | Strong            | Middle             | Weak                  | Middle            |
| Routing info                  | Strong            | Weak               | Middle                | Weak              |
| Boundary filtering rules      | Strong            | Weak               | Middle                | Weak              |
| Open port info               | Strong            | Middle            | Strong                | Weak              |
| Application service info      | Strong            | Middle            | Strong                | Middle            |
| System configuration info     | Strong            | Weak               | Strong                | Middle            |
| Organization info            | Weak              | Weak               | Weak                  | Strong            |
| Personnel info               | Weak              | Weak               | Weak                  | Strong            |
| Vulnerability info           | Weak              | Weak               | Strong                | Middle            |

4. Satellite Communication Network Vulnerability Mining Technology

The particularity of satellite communication network vulnerability mining is that the tester cannot directly access the firmware code of satellite network equipment when mining some typical broadband satellite network equipment. Therefore, we divide the vulnerability mining work of satellite communication network into two parts.

1) For the part that can obtain the source code, the symbolic execution technology is adopted. Considering the possible path explosion problem in symbolic execution, the static stain analysis of the source code is selected to realize pruning, discard the redundant path, and then perform the compliance execution analysis.

2) For the firmware that cannot get the source code, fuzzy testing method is used. In order to improve the effectiveness of test cases generated by fuzzy test, machine learning method is used. At the same time, in order to improve the code coverage, disassembly technology is used to guide the generation of test cases by combining the technology of instrumentation and taint analysis.

The communication boundary of satellite network mainly includes user interaction boundary, satellite channel boundary, and system boundary which has interaction relationship with other forms of network, such as satellite terminal equipment used by users, network application services for users, etc. Therefore, for the satellite communication network vulnerability mining, firstly, according to the satellite application program source code and satellite equipment firmware, we use Taint Analysis [6], symbol execution [4], and instrumentation technology [12] to conduct deep code audit and vulnerability mining, and use network protocol fuzzy test method to analyze satellite communication network protocol, so as to detect possible security All the loopholes and configuration defects can improve the overall anti boundary penetration attack capability of satellite communication system.

This paper introduces the key technologies and methods used in vulnerability mining of satellite communication network.

4.1. Stain Analysis Technology

Stain analysis technology is a kind of technology to track and analyze the flow of taint information in the program. The main principle is to mark the data from the network, file and other untrusted channels as "contaminated", and then a series of arithmetic and logic operations will act on the data, and the newly generated data will inherit the "polluted" attribute of the source data. By analyzing these properties, some characteristics of the program are obtained.

For the software of satellite communication network, it is abstracted as a triple (sources, sinks, In the form of sanitizers, source refers to the direct introduction of untrusted data or confidential data into the satellite network; sink refers to the taint gathering point, which directly generates security sensitive operations or divulges private data to the outside of the satellite network; sanitizer refers to harmless treatment, which means that data transmission is no longer soft to the satellite network by means of data encryption or removal of harmful operations The safety of the parts is harmful.

By analyzing the software program in satellite communication network, if the data introduced by the tainted source is not harmlessly processed, it can be directly transmitted to the pollution gathering
point, which indicates that the software has security loopholes such as privacy data leakage or dangerous data operation. Otherwise, the software is safe in the dimension of information flow.

4.2. Symbol Execution Technology
The basic principle of symbolic execution technology is to symbolize the input data of software program, that is to use symbolic variables instead of actual values to explore and analyze programs. In order to represent the possible execution flow, the control flow graph (CFG) of the program can be drawn to analyze all the paths traversed during the execution. You can also create a symbolic execution tree that references CFG to record the symbolic expressions associated with the program input variables generated by each path.

For the software of satellite communication network, traditional symbol execution, dynamic symbol execution and selective symbol execution are comprehensively used to analyze the possible security defects. Traditional symbolic execution is a kind of static symbolic execution, whose input variable is the symbol of simulated execution rather than the actual execution of software program; dynamic symbolic execution is the combination of symbolic execution and specific execution, inheriting the advantages of both; selective symbolic execution can execute symbolic execution in some areas of software program, especially improving the analysis of target software by symbolic execution Particle size.

Through symbol execution technology, the execution space of software program in satellite communication network is effectively covered, and the program execution path under various conditions is defined. For each program execution path, the specific input set can be generated, and the existence of various software errors, including assertion violations, uncapped exceptions, memory damage, etc., can be used as the basis for judging whether the software has vulnerabilities.

4.3. Code Piling Technology
The purpose of instrumentation technology is to insert the corresponding function code in the specific position (logical space) of the target software, so as to control the program execution process, realize the condition trigger, path selection and data extraction.

For satellite communication network, the use of code instrumentation technology, in essence, is to modify the code space of software programs. Therefore, it is necessary to ensure that the target program after instrumentation has the same logic integrity function as before. Then, the inserted program is run. According to the inserted function code, various data of the program execution are collected in real time to realize the instrumentation detection.

Software programs in satellite communication network usually need to go through four stages from writing to running, that is, source code writing stage, source code preprocessing stage, source code compiling stage, code base connecting and running stage. Each stage can realize the software code instrumentation. The first three stages belong to static level instrumentation because they do not need to start the program, and the last stage of running program belongs to dynamic level instrumentation.

The technology of inserting piles can effectively control the flow direction of the software program and extract the required execution data at the designated location. Therefore, it is more effective for discovering the loopholes in the operation of satellite communication network software programs, and can effectively make up for the defect that static scanning cannot cover the program execution path.

4.4. Fuzzy Test Technology
By inputting a large number of semi random data into the target system to be tested, fuzzy testing monitors the operation of the target system, records and analyzes the anomalies of the system, so as to find potential vulnerabilities.

For the software of satellite communication network, semi random data refers to the important data format and most of the data are valid and legal. The other parts are illegal data that do not meet the input data format specification of the target program. For example, for the web application software in satellite communication network, especially the software that provides interactive input query function, it can input a large number of normal data In order to test whether the target software has typical...
security vulnerabilities such as overflow and injection, some abnormal data, such as super long input string or input string containing special characters, are mixed in.

If there are such loopholes in the software program of satellite communication network, errors may occur when processing these data, which may lead to application crash or trigger corresponding security vulnerabilities. Traditional fuzzy testing is based on black box testing. In this method, the generation of test cases is lack of pertinence, which leads to many paths can not be covered and the test efficiency is low. The combination of fuzzy testing and symbolic execution technology forms a white box test method, which can automatically generate test cases with high path coverage, and then find potential vulnerabilities in the target program.

4.5. Vulnerability Mining Based on Machine Learning

The essence of applying machine learning to vulnerability mining is to regard vulnerability mining as a software classification or clustering problem, to distinguish software programs containing vulnerabilities from normal programs or to aggregate programs containing vulnerabilities. Vulnerability mining models can be divided into vulnerability mining models based on software metrics [13] and vulnerability mining models based on syntactic semantic features [14].

Software measurement is a continuous and quantitative process of data definition, collection and analysis of software development projects, processes and products in satellite communication network. The purpose is to understand, predict, evaluate, control and improve software development projects. Software metrics is a quantitative representation of software specific entity attributes, which can provide various information of software, and can be obtained through software tools. Software metrics include complexity measurement, code change measurement, coupling degree, cohesion and other metrics. To some extent, it can reflect which files may contain vulnerabilities. It is one of the basic methods for software vulnerability mining in satellite communication networks.

Semantic based vulnerability mining mainly uses text mining technology to obtain semantic information in software source code. First of all, through the analysis of software development documents or program notes and mining the possible vulnerabilities; secondly, the text mining of the source code, extracting the effective information of the source code to mine the vulnerability. We use ast representation program syntax to mine software vulnerability of satellite communication network. Based on this graph, the structure of the source code can be represented automatically by traversing the tree structure of the source code.

On the other hand, for the software programs in satellite communication network, in order to improve the efficiency and accuracy of vulnerability mining, we apply machine learning to the above work. Because static taint analysis technology often needs large space cost and high false alarm rate, machine learning can quickly process a large number of samples, thus reducing the false alarm rate; one of the key problems of symbol execution is the space explosion of path execution. The suspicious function set is determined by machine learning, and the symbol execution is guided by the suspicious function set, which can effectively reduce the number of paths. In order to improve the performance of symbol execution, fuzzy testing needs to generate more effective test samples to effectively trigger vulnerabilities. Combining machine learning to generate test cases can improve the effect of fuzzy testing.

5. Penetration Testing Technology of Satellite Communication Network

The penetration test analysis of satellite communication network mainly focuses on the test of business application system, network equipment and user terminal, including buffer overflow, SQL injection, cross site attack and Trojan horse penetration to try to obtain the control authority of the target system or equipment.

For the boundary penetration of satellite communication network, the difficulty lies in the strong closeness of all kinds of satellite components and application systems, the firmware code is closed, and there are basically no open security vulnerabilities. Therefore, it is difficult to directly use the existing vulnerabilities for penetration attacks. It is necessary to combine the results of unknown vulnerability mining and verify the specific security and risk.
According to the security loopholes and detection tools that have been mastered, simulate hacker's attack method, and conduct non-destructive attack test on satellite network under the premise of authorization and supervision. Penetration analysis mainly focuses on vulnerability mining and utilization analysis of satellite communication system application components, bearing facilities, satellite communication equipment and communication protocol. The following testing techniques are mainly used:

5.1. Buffer Overflow Attack
Buffer overflow is one of the most common and harmful security vulnerabilities in the field of computer software. It exists widely in various operating systems, databases and application software, as well as in the software system of satellite communication network.

Buffer overflow attack is a kind of attack which takes advantage of the buffer overflow vulnerability. It generally refers to that when the computer fills the buffer with data, it exceeds the capacity of the buffer itself, and the overflow data is covered on the legitimate data. Usually, the correct return address of the function in the program will be covered, and the program will jump to the location designated by the attacker and execute malicious code.

The harm of buffer overflow attack depends on the privilege of the overflowed program itself. If the operating system components and drivers encounter overflow, it means that the attacker can execute malicious code with the root user rights of these programs, thus causing serious damage to the system.

Buffer overflow is an important part of penetration testing. For satellite communication network, the objects of buffer overflow test should cover network equipment, server operating system, database, middleware, application service, client and so on, in order to fully test its security.

5.2. SQL Injection Attack
SQL injection enables attackers to bypass the authentication mechanism and take full control of the database on the remote server. At present, most web applications use SQL database to store application data. Like most languages, SQL syntax allows database commands to be mixed with user data. If web application developers are not aware of security, user data may be interpreted as commands, so that remote users can not only input data in the web application, but also execute arbitrary commands on the background database.

Satellite communication network contains a large number of service software relying on Web applications. For this kind of service software, special SQL statements are written to interact with the background database, and the relevant information of the server and application can be obtained by viewing the returned results. The reason of SQL injection vulnerability is that developers do not check the validity of SQL statements when writing applications, so that illegal statements are executed without server verification. Through the SQL injection vulnerability, the intruder can add, delete, modify and query the user information in the database, and even export the important data such as account information and enhance the user access rights, so as to achieve the goal of fully mastering the target system.

Cross site attack

Cross site attacks include cross site scripting and cross site request forgery:

Cross site scripting refers to the use of website vulnerabilities, attackers through the insertion of malicious code in the link to steal user information. In order to increase the concealment of malicious code, the attacker usually encodes the malicious code to disguise it as a legitimate link, so that the user can click. Cross site script is also a kind of vulnerability of web application. Aiming at the web application service in satellite communication network, we should focus on the penetration test based on cross site script.

Cross Site Request Forgery is a kind of attack method to prevent end-users from performing unintended operations on currently logged in web applications. With a little bit of social engineering, such as links sent via email or chat software, attackers can force users of web applications to perform actions of their choice. Using cross site request forgery attack to attack network devices (such as routers) can control the user's network access or obtain the network device permissions. Cross Site Request Forgery may cause serious consequences. For example, when the user logs in to the satellite
communication application service normally, the attacker can forge the identity of the application server and make the user perform sensitive operations in unknown circumstances, such as transferring money and recharging to the attacker's account in the satellite communication account, thus causing the user's property loss.

5.3. Trojan Penetration Attack

Trojan horse penetration test is common in network penetration, which is a great threat to the information system. The main principle is to reverse the tunnel for remote control, that is to install the Trojan horse to the server through various ways. At this time, the remote connection can be established to the server on the client, that is, the intruder's computer, so as to achieve the effect of complete control.

Trojan horse penetration is one of the main security threats for satellite communication network, which has high security sensitivity. Because this kind of network usually sets strict input blocking rules at the boundary, it is difficult for attackers to directly invade the devices inside the network. However, Trojan programs are implanted into the internal host or terminal through e-mail and social software, and then the devices are isolated through the network through reverse connection, so as to achieve the purpose of remote control. Trojan horse program has the functions of stealing data, remote file management and opening unauthorized services, and has the characteristics of concealment, self starting and automatic recovery in the process of penetration. Therefore, using Trojan horse to conduct penetration test can greatly improve the automation level and efficiency of network penetration test.

On the other hand, because Trojan horse implantation is usually combined with social engineering techniques, penetration testing with Trojan horse can also help to find out the security omissions of network users, so as to achieve the purpose of comprehensive investigation of security risks and improve the safety awareness of all staff.

6. Summary

Satellite communication network is a kind of new communication network environment which develops rapidly in recent years. Due to the strong specialization of network protocol and software and hardware equipment, its security problem has not been paid enough attention. Aiming at the security protection of satellite communication network, this paper puts forward a technical framework including information collection and detection, vulnerability mining and penetration testing. Through the combination of general technology and special characteristics of satellite network, it provides reference for the security detection and active defense of satellite communication network. Based on the above technology and methods, the terminal equipment and application services in satellite communication network are analyzed and mined. A series of high-risk vulnerabilities including overflow, backdoor and injection are found. The security countermeasures against the vulnerabilities are proposed and the reinforcement work is completed.

Satellite communication network involves many types of network protocol, hardware and software equipment, middleware, application service and management mode. In the future, the scope of vulnerability mining and penetration testing will be gradually expanded to cover satellite network data center and various business application systems, satellite communication equipment and terminal station equipment, so as to comprehensively grasp the security status of satellite communication network. On the other hand, a complete response mechanism is established for the vulnerability risk of various products, equipment and systems in the satellite communication network, including how to detect and discover the vulnerability risk in the product, equipment and system, how to repair and reinforce the discovered vulnerability risk, how to use the situation awareness technology to realize the vulnerability risk in real time, and how to formulate the emergency plan for vulnerability risk So as to establish the dynamic defense and defense in depth capabilities to ensure the security of satellite communication network.
7. References

[1] Ruben Santamarta. A Wake-up Call for SATCOM Security. IOActive Technical White Paper[OL]. https://ioactive.com/wp-content/uploads/2018/05/IOActive_SATCOM_Security_WhitePaper.pdf 2014.

[2] Hongyu Sun, Yuan He, Wang Jice, Dong Ying, Zhu Lipeng, Wang He, Zhang Yuqing. Application of artificial intelligence technology in the field of security vulnerabilities [J]. Journal of communications, 2018,39 (08): 1-17 Caplar R and Kulisic P 1973 Proc. Int. Conf. on Nuclear Physics (Munich) vol 1 (Amsterdam: North-Holland/American Elsevier) p 517

[3] Niu Weina, Zhang Xiaosong, Du Xiaojiang, Zhao Lingyuan, Cao Rong, Guizani Mohsen. A deep learning based static taint analysis approach for IoT software vulnerability location[J]. Measurement, 2020, 152(C).

[4] Cadar C, Sen K. Symbolic execution for software testing: Three decades later[J]. Communications of the ACM, 2013, 56(2):82-90.

[5] Miller B P, Fredriksen L, So B. An empirical study of the reliability of UNIX utilities[J]. Communications of the ACM, 1990, 33(12):32-44.

[6] James Newsome. Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software [J]. Chinese Journal of Engineering Mathematics, 2005, 29(5):720-724.

[7] Baldwin, R. Kuang: rule based security checking[R]. MIT Lab for Computer Science,1994.

[8] Zerkle D, Levitt K. NetKuang: a multi-host configuration vulnerability checker[C]. In Proceedings of the 6th conference on USENIX Security Symposium, San Jose, CA, 1996, 12(24):21-29.

[9] Bruce Schneier. Attack trees: Modeling security threats [OL]. http://hackerproof.org/wwwb/data/hacker/attacktrees-ddj-ft.pdf, .1999.

[10] Dacier M, Deswarte Y. Privilege Graph: an Extension to the Typed Access Matrix Model[C]. In European Symposium on Computer Security-esories. DBLP, 1994.

[11] Phillips C, Swiler L. A graph-based system for network-vulnerability analysis[C]. In Proceedings of the New Security Paradigms Workshop, Charlottesville, VA, 1998: 71-79.

[12] Huang, J. C. Program Instrumentation and Software Testing[J]. Computer, 1978, 11(4):0-32.

[13] MCCABE T J. A complexity measure[J]. IEEE Transactions on software Engineering, 1976 (4): 308-320.

[14] HOVSEPYAN A, SCANDARIATO R, JOOSEN W, et al. Software vulnerability prediction using text analysis techniques[C]. The 4th International Workshop on Security Measurements and Metrics. 2012: 7-10.