Research on Mimic Defense Technology and Security Test Method of Electric Power Web Service System

Research on Mimic Defense Technology and Security Test Method of Electric Power Web Service System

Xin Sun[1], Qinyuan Li[1], and Sheng Zhou[1], Changhua Sun[1]

[1]State grid zhejiang electric power research institute, Hangzhou, Zhejiang, ZIP code, China.

Abstract. In this paper, aiming at the demand of active defense against attacks in the environment of "poisonous bacteria" in electric power web service system, the mimic defense technology of electric power web service system based on dynamic transformation of resources and heterogeneous redundant executors is proposed. The dynamic environment is realized through active changes of software and hardware elements at different levels, thus destroying the deterministic and persistent dependency conditions of the attack chain on the operating environment, blocking the network attack chain, solving the problem of unknown attack defense using unknown vulnerabilities and unknown backdoors, and effectively enhancing the network security of key Web application systems in the power industry. On this basis, in order to verify the security of mimic defense technology in electric power web service system, a security test method is given to verify the feasibility and effectiveness of mimic defense technology on web.

1. Introduction

Great changes have taken place in the Internet environment in recent years. According to the 2016 Internet Security Report of CNCERT/CC National Internet Emergency Center[1], only one vulnerability in the Web system accounts for 16.8% of all vulnerabilities. In 2016, CNCERT/CC monitoring found about 178,000 fake pages targeting websites in China, and about 40,000 IP addresses planted backdoors to more than 80,000 websites in China, up 9.3% from 2015.

With the popularization of power information system and continuous accumulation of data, power production, dispatching and marketing rely more and more on information system. More and more Web application systems based on B/S architecture are continuously built and put into use. Accompanying this is the explosive growth trend of attack methods and continuous renovation, which brings serious hidden dangers to the security of business systems. At present, the network security defense system, which is widely used or deployed in firewall, security gateway, intrusion detection system, virus detection and killing, user authentication, access control and other technologies or equipment of power enterprises to improve system security. Its essentially a passive security protection system based on prior knowledge (including known attacker's characteristics, behaviors, fingerprints, etc.). There are genetic defects in its response to uncertain threats. It only has "acquired immunity" and can only "constantly find vulnerabilities and patch them up". It cannot defend against unknown vulnerabilities and unknown attacks by unknown backdoors. In this situation, there is a serious asymmetry between attack and defense in power enterprises, which makes it difficult to effectively deal with all kinds of increasingly complex and intelligent infiltration network intrusions, resulting in the ultimate difficulty in ensuring the security of key Web business systems of power enterprises.

According to the characteristics of the grid Web system of State Grid Corporation of China, this paper analyzes the security risks it faces, combines the characteristics of network attacks, introduces the core technology of mimic defense, designs a mimic defense gateway architecture for grid Web applications[2], and conceives a hierarchical and dynamic heterogeneous redundant defense framework. Effective protection is implemented in multiple attack phases to expand the defense area, thus providing security protection capability for power grid Web applications. On this basis, this paper will focus on the security testing methods of mimic defense technology applied in power grid web.

2. Mimic Defense Technology of Power Grid web Service System

The mimic defense technology for power web system designed in this paper mainly includes two key technologies, namely, mimic defense technology based on dynamic jump of network resource address and mimic defense technology based on heterogeneous redundant executors.

Based on the mimic defense technology of dynamic jump of network resource address, starting from the web resource address, the mimic defense is realized through web resource address detection and dynamic replacement of web resource address. This technology is mainly aimed at the problem that static URL will expose the Web application directory structure and become an attack portal. Combined with the dynamic thought of mimic defense, it makes the URL of the power grid Web service system in a constantly changing state, realizes the hiding of the Web application directory structure and the dynamic change of potential attack portals, blocks attacks and ensures the security of web applications.

Based on the mimic defense technology of heterogeneous redundant executors[3], starting from the Web application execution environment and execution process, the heterogeneity of Web application executors and the redundancy of Web application executors are studied to realize mimic defense based on heterogeneous redundancy. Heterogeneous redundant executor is the core of mimic defense implementation in this technology. Therefore, it is necessary to study the heterogeneous redundant executor construction technology of grid Web service system composition attributes, with emphasis on operating system, Web service software, Web application writing language and other levels. At present, the main implementation methods of heterogeneous redundant executors mainly include diversified compilation of instruction codes and diversified transformation of intermediate languages. Based on heterogeneous redundant executor technology, this paper designs and proposes a prototype architecture for verifying the principle of mimic defense gateway of power grid web service system. It is mainly composed of access request balanced distribution module, non-similar Web executor pool, dynamic heterogeneous redundant executor scheduler, response redundancy voter, etc. The system structure is shown in Figure 1, where the ontology is the Web server to be protected.

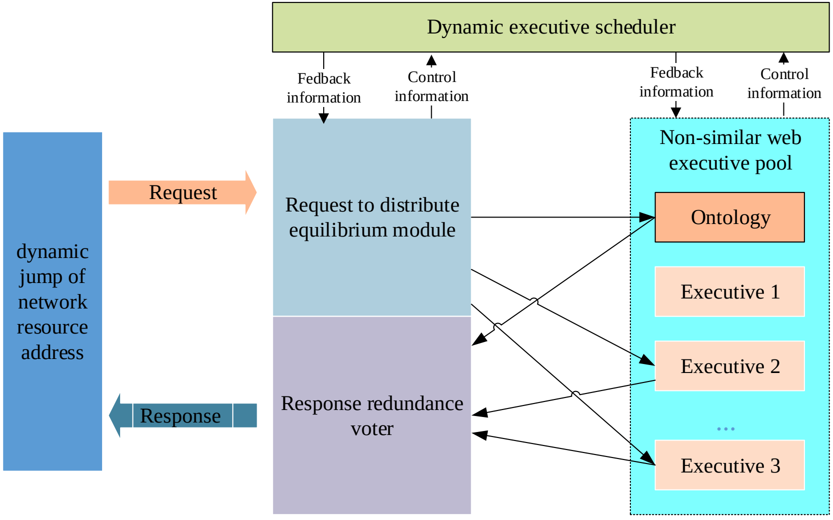
Dynamic executive scheduler
Fedback information
Control information
Fedback information
Control information
Non-similar web executive pool
Ontology
Executive 1
Executive 2
...
Executive 3
Request
Request to distribute equilibrium module
Response redundance voter
Response
dynamic jump of network resource address

Figure 1 mimic defense gateway system architecture

3. Test on Mimic Defense Capability of Power Grid web Service System

In order to verify the effectiveness of the proposed theories, models, algorithms and strategies related to mimic defense of the web system, based on the requirements of relevant national product safety standards, this chapter constructs a mimic defense safety testing environment in combination with the deployment framework of power grid web application systems, and proposes a scenario and scheme for the evaluation of mimicry-security gateways of power Web systems. Since the Web service system is composed of software middleware at all levels, and the mimic defense gateway applies the mimic security defense mechanism to the application level of Web services[4], the defense scope of the mimic defense gateway prototype is to block vulnerabilities or backdoor attacks in the operating system of the real Web service provider and illegal tampering of Web service files, which is the security boundary. Levels or modules that have not been protected by mimic defense mechanisms do not fall within the scope of this security assessment.

In order to test the mimic defense security of power grid Web service system, it is first necessary to build a set of network attack[5] and defense test range based on open source cloud computing platform, deploy the power grid web service test system with mimic defense gateway in the virtualized range environment and preset security vulnerabilities, and deploy two groups of control systems with different protection levels, and adopt gray box test method to conduct mimic function test, performance comparison test and security comparison test. In the second step, according to the characteristics of the information network and Web application system of the power grid company, a pilot application scheme of the mimic defense gateway in the information external network of the power grid company is formulated, and the mimic defense gateway is deployed at the boundary of the external network to carry out mimic defense on some Web applications. The third step is to conduct a double-blind penetration attack and defense experiment on the power grid company's extranet Web application without informing the details of the experiment, and to verify the defense effect of the mimic defense gateway by comparing the test results with and without mimic protection.

3.1. Environment Setting of Attack and Defense Test Range

The network attack and defense target test field is divided into three test groups, the test group comprises a Web server and a database server, and the network isolation is carried out through a strong isolation device to simulate the internal and external information network of electric power. The front end of test group 1 deploys the mimic defense gateway of the project results for protection, the front end of test group 2 deploys WAF for protection, and test group 3 has no boundary protection equipment. Through the penetration tests of the three groups of networks by the test clients, the mimic-protection effect is transversely verified. See Figure 2 for the topology diagram of the network attack and defense test range.

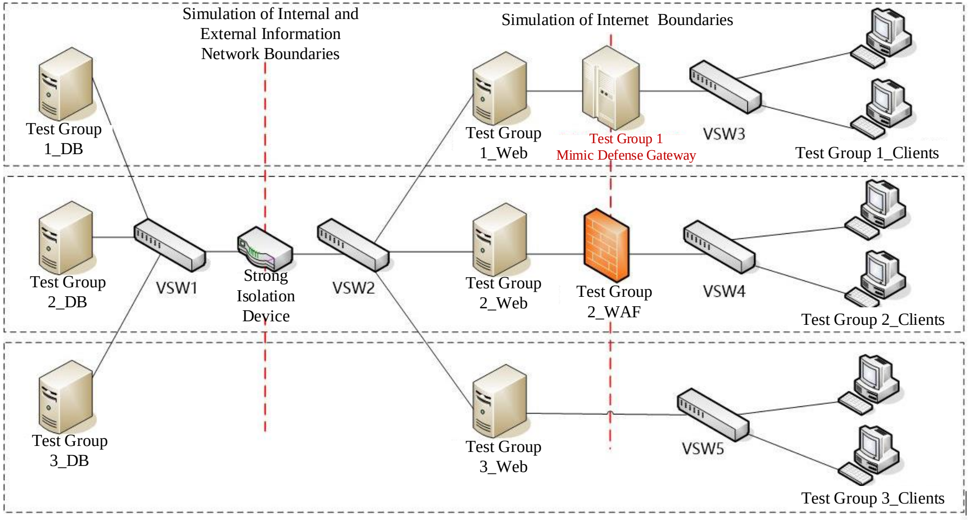

Figure 2 Topology Diagram of Virtualized Network Attack and Defense Range

In order to ensure the effectiveness of lateral testing, the software environment of the three test groups should be completely consistent. Operating systems, middleware and databases are installed in application and database servers. Typical external network Web application systems are selected and deployed to servers. Test data are imported and high-risk security vulnerabilities are preset. Security vulnerabilities are set in combination with vulnerability hazards, attack methods and other factors, and the following types are considered: information disclosure, SQL injection, upload vulnerabilities, WebShell presetting, remote command execution, etc. The test client should install all kinds of tools needed for attack and defense penetration, including protocol grabbing, Web vulnerability exploitation, trojan horse remote control, etc.

3.2. Verify test content

1. Function test of mimic defense

In order to better carry out quantitative evaluation, it is proposed to refer to the evaluation methods in "GB/T20984-2007 Information Security Technology Information Security Risk Assessment Specification", "GB/T30279-2013 Information Security Technology Security Vulnerability Ranking Guide" and "General Vulnerability Scoring Standard" for system security scoring. The specific items and contents of the mimic defense function test are as follows:

Table 1. Specific items and contents of the mimic defense function test.

No.	*Projects*	*Content*
1	Basic function	Can provide normal Web services
2	Main function	Verify the current mainstream operating system-level attacks to ensure the normal operation of Web services
3	Heterogeneity	Verify Heterogeneous Composition of Gateway Information
4	Dynamics	Verify that the gateway presents different system attributes in different time periods
5	Self cleaning	Verify that the gateway is always healthy

2. Performance comparison test

Using Loadrunner and other tools to test the performance and stress of the three groups of test application systems respectively, test the average page response time under specific business scenarios and visits, as well as the maximum concurrent visits and throughput under extremely high-intensity visits. By comparing the performance test results of the three groups, it is verified that the processing capability and time delay of the mimic defense gateway are within an acceptable range, and the performance status of the mimic defense gateway and the traditional Web Application Firewall (WAF) are compared to provide a feasible basis for further pilot application.

3. Permeability comparison test

Covering the main attack paths and attack means of hacker attacks, penetration security tests of the same strength are respectively carried out on three groups of Web application systems. As the Web code, host middleware and database configuration, test data, preset vulnerabilities and other aspects of the Web application systems of the three test groups are exactly the same, but the border protection technologies are different, group 1 adopts mimic defense technology, group 2 adopts Web firewall technology and group 3 has no protection measures. Through comparative tests, the characteristics of mimic security defense technology in Web security protection compared with traditional similar protection technologies are verified, and the defense effect of mimic gateway prototype is verified. At the same time, the following tests are required to verify the mimicry of the mimicry gateway.

(1) Scanning and detecting mimic defense test scenes of attack types

The network resource address dynamic jump and request distribution equalization module is adopted in the network web service system mimic defense gateway to realize mimic transformation and request distribution of the web service system access portal. Their main function is to dynamically transform the access entry and fragment the request data to transit to the server cluster via random paths. Heterogeneous redundant executors only open the ports and transit channels when they are selected. Therefore, a detection and scanning test scheme for the power grid web service system is constructed according to this function. When the attack host scans through the public network IP host each time, the reasonable penetration test feedback should be that the attack host obtains completely different host information to prove the effectiveness of the mimic defense technology.

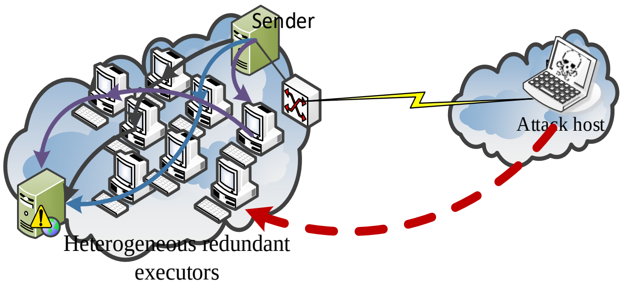

Figure 3 Dynamic Traffic Distribution Module Test Scenarios

(2) Penetration and Utilization of Mimic Defense Test Scenarios of Attack

The core purpose of mimic defense technology is to resist network attacks caused by vulnerabilities and the use of back doors. The non-similar heterogeneous redundant web execution technology module designed in this paper is mainly used to randomly select a server to process and return the results when the Web access request passes through the virtual machine pool. For this function of mimic defense, attack test cases such as system breakthrough, preset back door and system damage should be constructed. Aiming at the web service executor with known specific vulnerabilities, a system breakthrough attack is carried out during its online operation to test whether the web service executor service can automatically switch off the line before the attack is completed. Similarly, if the back door is embedded in the web service executor and attempts to infiltrate and utilize it during its online period, it is also expected that the mimic defense gateway should be able to identify the back door utilization and dynamically switch the service executor to resist infiltration attacks.

4. Conclusion

Mimic Defense in web is a security strategy for the serious asymmetry of attack cost and defense cost in web, as well as the severe lag of core technology and industrial foundation in China's information field in the current conditions in national security requirements. In this paper, the dynamic transformation of the structure and dynamic diversification of the operating environment of the power grid web service system are proposed to block or disturb the static, similarity and certainty on which the attack chain depends, thus achieving the requirement of controllable system security risks. On this basis, this paper presents a security testing scheme for the mimic defense gateway of the web service system under the power information network environment, designs the security testing requirements in terms of function and performance, and puts emphasis on the security testing scenarios and testing requirements, which provides a solution for the feasibility and effectiveness verification of the mimic defense technology of the power web system.

Acknowledgments

Supported by the science and technology project of State Grid Corporation of China: "Research and application of Mimic Defense Gateway applied to web application for power grid" (Grand No. 52110118001F)

References

[1] China Internet Network Security Report 2016. http://www.cac.gov.cn/2017-06/23/c_1121197293.htm..

[2] Wu J.X.(2016). Research on Cyber Mimic Defense. Journal of Cyber Security, 1(4):1-10..

[3] Tong Q. Zhang Z. Zhang W.H, Wu J.X.(2017). Design and Implementation of Mimic Defense Web Server, Journal of Software. 28(4):883-897.

[4] Hu H.C. Chen F.C. Wang Z.P. (2016) Performance Evaluations on DHR for Cyberspace Mimic Defense. Journal of Cyber Security., 1(4): 40-51.

[5] Zhang Z. Ma B.L. Wu J.X. (2017) The Test and Analysis of Prototype of Mimic Defense in Web Servers. Journal of Cyber Security., 2(1): 13-28.