2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS) | 979-8-3503-0093-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/MICCIS58901.2023.00036

Research on Security Protection of Satellite Resource Scheduling System Based on WEB

1st Hong Li
The 54th Research Institute of CETC
Shijiazhuang, Hebei Province, 050081, China
1144422888@qq.com

2nd Yuhao Zhao*
Northwestern Polytechnical University
Xi'an, Shanxi Province, 710072, China
jioyli@126.com

3rd Huixun Li
Space City of China
Beijing 100094, China
429873969@qq.com

***Abstract*—In order to bring users more appropriate, more intuitive and better quality resource services and improve the automation level and resource utilization of the satellite system. The system is built on WEB-based external information dissemination platform, providing services such as free resource viewing, plan application and secure downloading of data to active certified users. This paper combines the WEB application requirements of the satellite resource scheduling system, analyses the security requirements brought by the application of WEB technology to the computer information system, designs a WEB-based security protection system for the satellite resource scheduling system, and explains the implementation techniques and basic assessment of the security protection system.**

Keywords-web ,security protect,satellite resource schedule

I. INTRODUCTION

The existing satellite resource scheduling model is text-to-electronic interaction model based on the C/S framework. With the continuous development of the system, it has increasingly failed to meet the needs of users. Firstly, it requires users to customize and develop corresponding client software to complete satellite resource applications and data downloads, which is difficult to develop and has a long lead time. Secondly, the satellite resource usage and idle window cannot be updated dynamically, and users lack understanding of the satellite system resource situation, and back-to-back application methods are used between user centres, resulting in serious conflicts with resource plans and data download applications but the system resource usage rate is not high. Thirdly, the data retransmission service requires users to submit requests and manual intervention is carried out according to normal business processes, which encroaches on system resources and results in wasted manpower. In order to solve the bottleneck problem in demand, resource scheduling can be based on the external information service mode of WEB to provide users with services such as free resource view, plan application and data downloading, to improve the system service capacity as well as user operation convenience. The construction of WEB sites brings a lot of convenience to users and system usage. At the same time, the increasing number of users and the high risk of WEB technology will all bring pressure and new risks to computer information systems. By analysing the technical characteristics of WEB sites, comparing them with the requirements of information system security level protection, and finding out the security risks brought by WEB sites to computer information systems, protection measures for computer information system are proposed to improve the information security protection capability of computer information systems.

II. ANALYSIS OF WEB-BASED RESOURCE SCHEDULING MODELS

A. Development of WEB technology

WEB is a web-based information service system for publishing, browsing and querying information, consisting of many WEB servers located in different geographical areas [1]. WEB sites are rich in content and easy to use, which are important reasons why WEB is widely used. WEB is able to bring together information such as graphics, audio and video in one place, and also has graphical and easy to navigate features that help to save time and increase efficiency.

The WEB site has good interactive features. Firstly, it has the ability to be super-connected, so that the order of browsing and the sites visited are entirely up to the user. Secondly, dynamic information can be obtained from the server in the form of a FORM. The user can submit a request to the server by filling in FORM and the server can return the appropriate information based on the user's request. The WEB client is easy to use. Users do not need to develop separate client software and can access and interact with the server using a common browser.

B. WEB-based resource scheduling model

It is on the basis of the advantages of the WEB that the resource scheduling system proposes subsequent system planning and provides users with application planning, submission and data download services via the website.

WEB site function: Users access the external information release website through a web browser (typically Internet Explorer) and are guided through the website pages to complete a search for available satellite resources and fill in and submit a satellite use application plan through the visual website pages.

Data download function: For website based download applications, the data is pushed to a specified directory on the website server through the data download server and the user completes the data download by visiting the specified directory.

By analysing the application requirements of the system, one main system service is added, namely the addition of a web server. In addition. There are two other

979-8-3503-0093-2/23/$31.00 ©2023 IEEE
DOI 10.1109/MICCIS58901.2023.00036

application services, one is the opening of WEB site, which updates the existing C/S framework business system to B/S. The other is the opening of FTP download service, which allows users to access specified directories to complete data downloads via the FTP protocol. The B/S business system is based on a common browser and WEB server, using common protocols and common ports for data communication, and its access users are complex and uncontrollable.

III. Analysis of Risks

The increasing number of users and the increasingly complex nature of user units will bring great pressure to the computer information system. the application of WEB technology brings new risks to the computer information system. The WEB-based satellite resource dispatching system website has changed the traditional text-to-electronic application model and C/S framework, bringing a lot of convenience to users and improving resource utilisation and work efficiency. At the same time, WEB technology itself has a lot of security loopholes, and WEB-based network attacks are more likely to cause data leakage, web page tampering and website unavailability.

A. Risks of WEB attacks

1) SQL Injection Attack. In WEB applications, users access backend databases with SQL commands by submitting CGI parameter data. If these data are not strictly filtered, malicious SQL codes may be inserted to manipulate the backend database without authorisation, leading to leakage of sensitive information, damage to the database content and structure, and even control of the server operating system using the database's own extensions. The main hazards of SQL injection attack include reckless manipulation of data in the database, malicious tampering with web content, reckless addition/deletion of system accounts, malicious web page hangings, chain theft operations, etc.

2) Cross Site Script Attack (XSS). The XSS vulnerability is a dynamic web page WEB application that does not adequately check and filter the request parameters submitted by the user, allowing the user to enter HTML syntax in the submitted data. The code submitted by the malicious attacker will be accepted, interpreted and executed by the victim's browser. The attacker uses the vulnerable WEB site to attack users of other related web pages, thereby stealing sensitive information such as usernames and passwords from the user's session, and at the same time executing a Trojan horse attack on the user by inserting Trojan horse code.

3) Web Cookie Poisoning. Web Cookie is information that is temporarily stored on the local computer by the web application server based on system settings, client settings, etc., so that the server can use it to identify the visitor's computer and display a different page. When a user visits the same website again, the WEB server will first check the information stored in the local Cookie and if local information exists, the server will judge and display a different page based on the contents of the Cookie. Therefore, the content of the cookie is extremely important to the WEB application. Based on the intercepted Cookie, an illegal user can impersonate a real user and communicate with the server.

B. Risks of WEB leakage

The reason for information leakage is the lack of effective protection of "encrypted data", or even the lack of classification of confidential and non-confidential data, which allows illegal users or WEB users to access some confidential information through WEB applications.

C. Availability risks of WEB

The main purpose of a DDoS (Distributed Denial of Service) attack is to prevent a specified target from providing normal services. HTTP Flood is an attack launched against a WEB service at the Layer 7 protocol and is extremely harmful in three ways: it is easy to launch, difficult to filter and has far-reaching effects. An HTTP Flood attack uses a port scanner to find anonymous HTTP proxies or SOCKS proxies to launch HTTP requests to the target of the attack. HTTP Flood attacks can cause serious knock-on effects, not only slowing the response of the attacked WEB front-end, but also indirectly attacking the back-end business logic and database services, and even affecting the entire network.

IV. Design and Implementation of Security Protection Systems

The security protection of WEB site is a systematic and all-rounded architecture that includes functions from the deployment location of the site and boundary protection to server operating system security, website code writing, as well as intrusion detection, security auditing and vulnerability scanning. In this paper, the design and implementation of the security protection system is carried out in accordance with the requirements of hierarchical protection, combined with computer information systems.

A. External service website deployment

The entire network is first divided into security domains for hierarchical management, and border security protection equipment is added between the different zones. After configuring the WEB web server, the computer information system can be divided into internal core area, external interconnection area and external service area. The internal core area mainly includes the internal LAN and the internal users of the system, whose access users are the internal network and the internal users of the system. The external interconnection area mainly refers to the external networking platform, including the external private network A user networking platform and the external private network B user networking platform, whose interconnection users belong to the untrustworthy third party. The external service area mainly includes the WEB web server and its subnet, with which the hosts for data interaction are both the core area of the internal network and external users.

According to the service objects of the external website, it can be divided into three directions: internal network, external private network A and external private network B. According to the different service objects, three external service areas are built respectively, and the

WEB website is built in the external service area to interact with the internal network database through database synchronization. The website database of each direction only synchronizes the data table of this direction, and there is no data interaction between the directions.

B. *Internal core area protection*

Network isolation system is deployed between the internal core and the external networking platform, with strict control policies in place to ensure that only application data is exchanged between the internal and external networks, and that protocol analysis and protocol stripping of the physical, link, network and protocol layers is completed before data is exchanged. Private transmission information and transmission protocols (or no protocols) are used between the internal and external network units of the isolation system. The security isolation system shields the internal network topology and the operating system vulnerabilities of the internal hosts from external users and completely protects against attacks based on network protocols, i.e. attack packets from the network layer cannot reach the network to be protected. The system significantly enhances the security of the core network by performing protocol analysis, completing the extraction of application layer data and then exchanging it, keeping network attack packets such as Tear Drop, Land, Smurf and SYN Flood completely out of the trusted network[2].

The network isolation system is generally divided into three parts: the intranet processing unit, the extranet processing unit and the isolated data exchange subsystem, which completes the secure and controlled data exchange between the two networksintranet processing unit is connected to the high-security network (intranet) and the extranet proces [3]. The sing unit is connected to the low-security network (extranet platform). The data exchange subsystem includes a data exchange card and a special data exchange protocol, which is the only physical channel between the intranet processing unit and the extranet processing unit and connects the intranet processing unit and the extranet processing unit through a physical switch. The internal isolation system consists of two separate network processing systems: the intranet server and the extranet server. The intranet server is used to process internal network data and the extranet server is used to process external network data. A proprietary communication protocol is used for pure data exchange between the intranet server and the extranet server, which uses dedicated hardware rather than network hardware and software for the pathway, thus ensuring that the data exchange between the internal and external networks is independent and that there is no network pathway. Two completely isolated data channels are established between the intranet processing unit and the extranet processing unit: one transmits only data from the intranet to the extranet and the other transmits only data from the extranet to the intranet. A proprietary communication protocol (Secure Isolated Exchange Protocol) ensures that only pure data is transmitted between the intranet and the extranet and that no network information, control information or other security risks are transmitted, ensuring that the information exchanged between the intranet and the extranet is pure, secure and reliable.

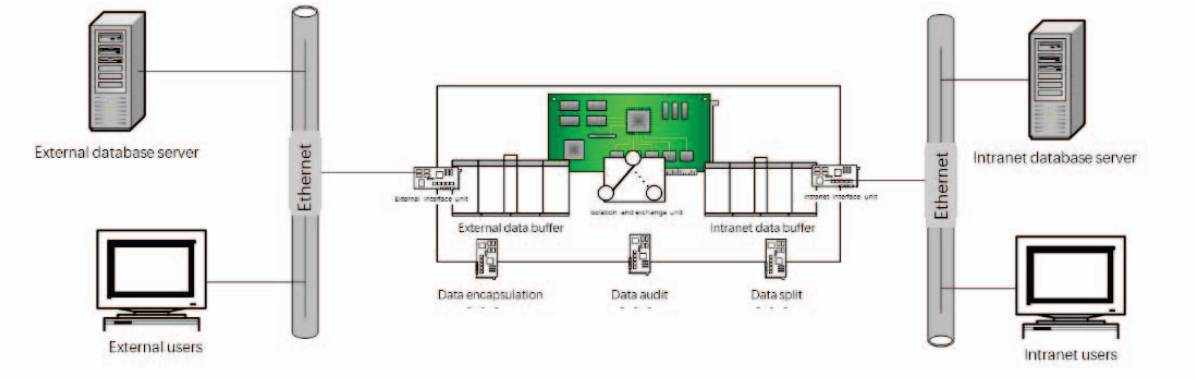

Figure 1. Components of the network isolation system

C. *Network security protection for WEB service area*

As the WEB site is located in the external service area, this security area is located between the core intranet and the external interconnection area, as shown in Figure 3. By deploying firewalls, intrusion detection, WEB application firewalls, combined with a complete security audit system, a multi-layer defence fortification is constructed for the WEB site to enhance the security of the WEB site.

1) First protection barrier: Firewall system. The firewall is deployed at the unique connection of information between different networks or network security domains. According to the security policy formulated by the organization's business characteristics, industry background and management system, it uses technologies such as packet filtering, proxy gateway, NAT conversion and IP+MAC address binding to achieve comprehensive control (allow pass, deny pass, process monitoring) of information flow in and out of the network, with control categories including IP addresses, TCP/UDP ports, protocols, services, connection status and other aspects of network information.

For the WEB service area, through the firewall, isolation can be formed at the external exit of its area and

access to the WEB service area from external terminals can be restricted by implementing strict access control means. Access control factors include source address, destination address, protocol, port number, user, time, etc., thus effectively restricting illegal access and forming the first barrier of protection for the WEB service area.

2) Second protection barrier: Intrusion detection and firewalls working in tandem. Firewall technology is carefully configured and usually provides secure network protection between internal and external networks, reducing network security risks. However, an intruder can look for a 'back door' to the firewall, or the intruder may be inside the firewall.

The network intrusion detection system is deployed on the backbone of the extranet. It is capable of listening to network data streams in real time to look for network violation patterns and unauthorised network access attempts. When network violations and unauthorised network access are detected, the network monitoring system is able to react according to system security policies, including real-time alarms, event logging, or the implementation of user-defined security policies. Intrusion detection and firewalls work in tandem to form the second barrier of protection for the WEB service area.

3) Third protection barrier: deployment of a WEB application firewall on the front end of the WEB server. Traditional firewall systems are based on the detection of IP messages and exist as access control devices, working mainly at layers 3 and 4 as defined by the OSI model. If a malicious attacking application encapsulates itself as a legitimate hypertext transfer protocol (http) and passes through the firewall detection from an open port of the firewall, for example port 80 (http) or 443 (https), thus evading the firewall system rules detection for attack and intrusion purposes.

The Web Application Firewall (WAF) works at the application layer, monitoring and isolating the communication flow at the application layer in real time, detecting and verifying the content of all kinds of requests from the client of the web application, ensuring the security and legality of the requests, and blocking illegal requests in real time to achieve the purpose of effective protection of the web site. The WEB application firewall uses active security technology to achieve content inspection and security defence at the application level, creating 'White Lists' to describe the legality of behaviour and access. The WEB firewall defends against unknown attacks and blocks attacks against WEB applications.

The WAF provides comprehensive protection against WEB service areas, checks HTTP and HTTPS traffic at the application layer, looks for attackers while legitimate applications are running, and is able to detect and defend against all types of common WEB application attacks such as worms, illegal attacks, cross-site scripting, web piracy links, etc.

The WAF provides in-depth inspection of WEB application data and can detect and defend against common denial-of-service attacks such as SYN Flood, UDP Flood, ICMP Flood and HTTP Get Flood at a fine-grained level.The WAF's comprehensive protection of the WEB service area becomes the third barrier of protection for the WEB service area.

4) Powerful assistance: a fine-grained security audit system. For WEB service areas, the access they receive should also be effectively recorded and made available to the system administrators of the information system for post-event analysis. The security audit system is based on trace detection, protocol reduction technology development and is capable of monitoring and reviewing online information. The security audit system intercepts and restores data such as access packets and transmission information to and from the WEB service area in a bypassed, transparent manner and at high speed in real time. It can also audit communication content according to user requirements, providing high-speed sensitive keyword retrieval and tagging functions to prevent leakage of sensitive information on the internal network and the spread of illegal information. It can completely record the origin address and user of various information, providing first-hand information for investigation and evidence collection.

The security audit system provides effective assistance for the management of the WEB service area. Through in-depth analysis of the audit records, the system administrator of the information system can grasp the activity status of the network, and can also use the analysis to deeply explore the possible deep-seated security risks of the system, providing powerful assistance for the continuous reinforcement of the WEB service area.

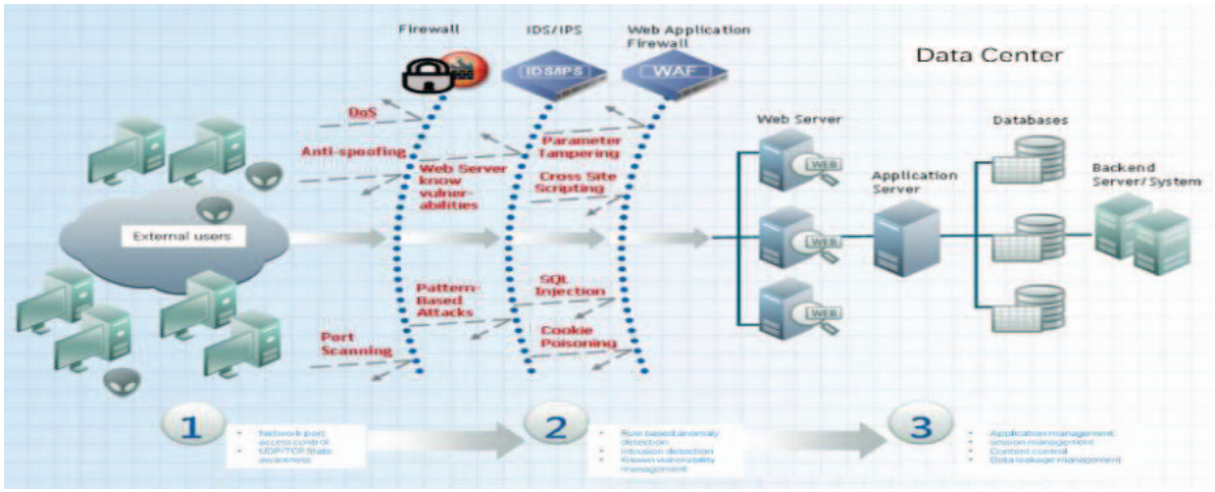

Figure 2. Security protection for WEB service areas

D. *Brief description of WEB application protection*

1) The foundation for securing applications: The security of the host platform. The security of the host platform mainly includes the security of the host system and the security of the WEB component system.

Firstly, the security of the host platform should be adapted to the requirements of independent and controllable. In terms of hardware technology, products developed and produced independently are used. In terms of software technology, a security operating system with China's independent intellectual property rights is used.

Secondly, the security of the host system is mainly based on strong identity authentication, peripheral control, access control, data security and administrator rights control in order to configure and tune the system security policy. The security of the WEB component system is mainly based on the reasonable setting of WEB sites and directories, file access rights settings, high security passwords and application isolation in order to carry out the security configuration and protection of the WEB component system. The installation of anti-virus software for real-time monitoring of the file system can prevent illegal persons from uploading files with viruses to the server through loopholes, and also ensure the safety of files uploaded by administrators.

2) Real safety: Security of WEB applications. WEB application security mainly refers to the security of WEB service software and business system code. WEB service software should be chosen to deploy a higher security system with fewer vulnerabilities, and a set of well thought out and detailed ideas should be designed in the development and writing of the code. It is also necessary to consider the use of a mandatory identity verification system, as well as the construction of an integrated WEB vulnerability scanning system to conduct security scans before and during the operation of the WEB service, so that security risks can be identified in a timely manner and targeted countermeasures can be taken in a timely manner to minimise security risks.

V. CONCLUSION

This paper analyses the security risks brought by WEB services to computer information systems from the demand of WEB applications in the application mode of satellite dispatching systems, and builds a security protection system for computer information systems by making use of the idea of managing and protecting security in separate areas, and reasonably configuring security protection measures and means, with emphasis on the security protection of WEB service areas. As the saying goes, "three points technology, seven points management" [4], through the computer information system security protection technology measures, combined with effective security operation system and management, will certainly be able to create a reasonable and effective computer information system protection system.

REFERENCES

[1] Xue H Deng J and Ye B 2012 Distributed Site Security Protection System, Computer Systems & Applications vol 21 chapter 03 pp 42-45

[2] Liu L 2012 Research on the application of isolation gateway technology in e-government construction, Network Security Technology & Application vol 2012 chapter 12 pp 28-29+27

[3] Zhang X 2012 Application of Physical Isolation between Intranet and Intranet in Enterprises, Public Communication of Science & Technology vol 4 chapter 24 pp 227+222

[4] Dou H Wu Y and Duan S 2012 Analysis and research on security risk of Web application, Journal of Xi'an University of Architecture & Technology(Natural Science Edition) vol 44 chapter 03 pp 446-451