The Network Security Analysis System Design Based on B/S Structure: An Approach Research

Julan YI[1, a]

[1]XINYU UNIVERSITY, Xin Yu 338004,China

[a]julanyi@126.com

Keyword: B/S architecture; Network Security; Network Monitoring

Abstract. Based on the B / S network architecture is very widespread, and the distance between the browser and the application server is usually more distant, and therefore ensure that the information transmitted over the remote line is particularly important. Many domestic and foreign academic institutions, enterprises and standardization organizations have recognized some of the research in this area began to build a meaning and importance based on the variety of network and security infrastructure of unified security management system, and. However, due to security reasons, openness and safety management system and other aspects, the research work safety management system is still in the exploratory stage. Through systematic research study found that the direction of research relevant literature and conduct adequate research and analysis of the existing network security detection systems cannot efficiently detect unknown intrusion defects, we propose a detection and analysis of network security architecture uses mode, design mode network security monitoring and analysis system architecture based architecture.

Introduction

With the development of computer networks wide and pan-popular Internet, information has become the core of modern social life. Faced with emerging network security issues and the limitations of a single network security products, many institutions and departments have purchased a variety of network security products such as firewalls, intrusion detection systems, vulnerability scanners, real-time monitor, VPN gateways, network anti- virus software. With these security products for network management security, so that these products are at different sides protected network [1-2]. However, the use of a large number of security products after the emergence of new problems, most of the features of these products scattered, fighting each other, formed a mutual no associated isolation "safe island", there is no effective between each other a variety of security products unified management scheduling mechanism cannot support each other, work together, so that application performance security products cannot be fully exploited, which brought great inconvenience to security management. To solve these problems, many domestic and foreign academic institutions, enterprises and standardization organizations have recognized some of the research in this area began to build a meaning and importance based on the variety of network and security infrastructure of unified security management system, and. However, due to security reasons, openness and safety management system and other aspects, the research work safety management system is still in the exploratory stage [3].

Network communication security is directly related to the ability to avoid or reduce risks and losses communications, increase user confidence, thus further promote the application of information and communication technologies and networks. Information related to the communications and network security technology, laws and regulations and worldwide cooperation. Network security is placed in front of web workers is an important issue. Currently, based on BS / network architecture is very widespread, and the distance between the browser and the application server is usually more distant, and therefore ensure that the information transmitted over the remote line is particularly important, based on BS / architecture security application system came into being.

System diagram based on B/S structure

In the design of network security management system, the main object-oriented design methods, the use of J2EE technology for J2EE multi-layer B/S structure based on. Before Internet is widely used, the traditional two-tier C/S (Client / Server) architecture is a common architecture, the structure in a certain period of time has achieved considerable success, the only service but, in many cases, provided by the server [4-5]. It is the database service. In this solution, the client is responsible for data access, business logic, display the results with the appropriate style, pop the default user interface to accept user input and so on. C/S structure is usually the first deployment is relatively easy, but difficult to upgrade or improve, and often based on a proprietary protocol (usually some sort of database protocol). It allows reuse of business logic and interface logic is very difficult. More importantly, in the Web era, the story does not reflect the application of generally good scalability, making it difficult to adapt to the requirements of the internet. The multi-layer B/S (browser/server) architecture is the business logic of the traditional two-tier C/S structure separated from the task of the client, the user makes a request to a number of servers distributed across a network through a browser The server for the browser's request is processed, the required information returns the user to the browser. The rest, such as data request processing results are returned and dynamic page generation, execution of work on the database access and application are all done by the intermediate layer. B/S structure to reduce the load on the client, reducing the performance requirements of the client, but also a more centralized management system, and fully apply to the network environment, the mainstream construction business systems currently used [6]. Figure 1 shows the architecture of B/S.

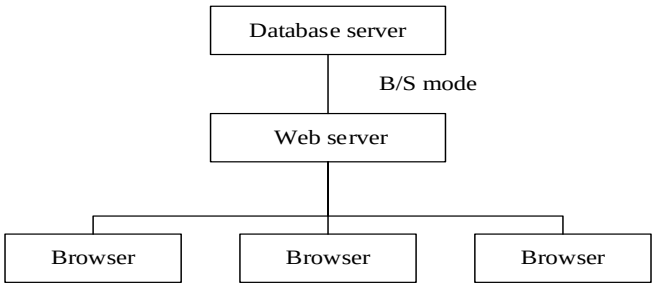

Figure 1. System structure of B/S

Web layer contains J2EE web components, including JSP and Servlet. This layer is mainly used to deal with customer requests, call the appropriate logic modules, and the results in the form of dynamic web pages returned to the client. This layer generates web pages and web page dynamic content, dynamic content that is typically obtained from a database, and presentation layer can be put in a request sent by the client's web page contains a package. To build this layer using the Struts framework. The Struts Action Servlet framework describes how to handle HTTP requests, how to generate the response, you can use them in the system to deliver dynamic content. Data layer is responsible for data management, data acquisition, the system uses 0RACLE 9i database, data in the database include: asset data information, vulnerability information data, the threat of information and data, risk information and data, event information data, work order information data, security knowledge of policy data and system support information. Data collection layer will be the management of resources (hardware, software, etc.) in safety-related information preprocessing (such as filtering, standardization, association, etc.) according to a certain format, while required to follow standard communication protocols output or accessed.

The network security prevention analysis

The network security prevention process is shown in Figure 2. Network security monitoring system architecture can be divided into a centralized system architecture and distributed system architecture two kinds. Centralized system architecture structure is relatively simple, the system is only one main service area is responsible for analyzing data sets uploaded other sub-control nodes, mainly used in small-scale network. Structure is more complex distributed system architecture, the

system is divided into multi-level security detection server, a distributed architecture, the local server is only responsible for managing the security of the region controlled host, while the analysis of the structure uploaded to a higher node, the system architecture mainly used in large-scale network. For a large number of data transmission network in the network, the system architecture enables cost-sharing central node, host resolution to increase the advantages of availability. The disadvantage is the cost of maintaining large, complex analysis mode.

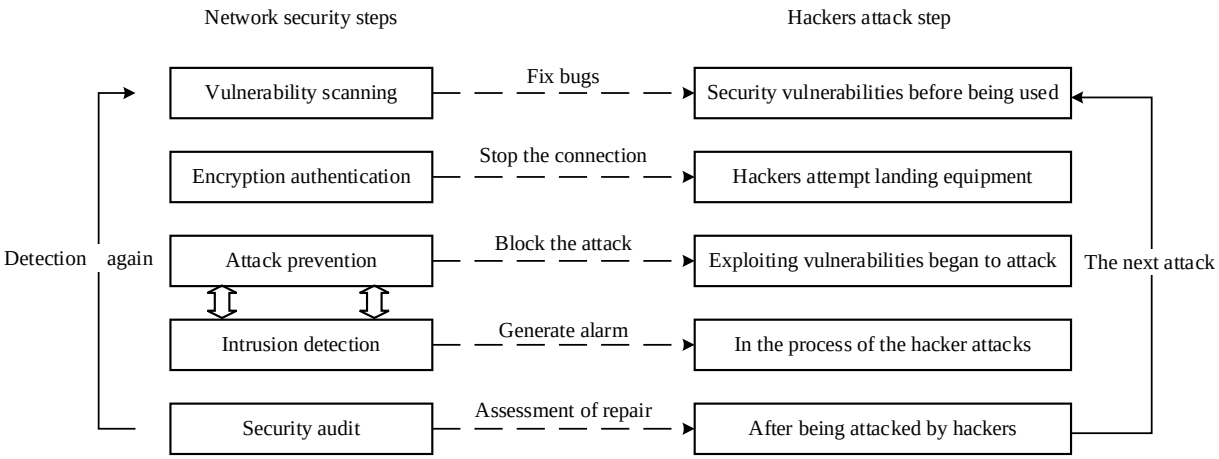

Figure 2.The network security prevention steps and hacker attacks

Centralized system architecture, the host can be divided into two types: the accused and safety testing server host, was charged with the host mainly responsible for collecting this node listens to packets uploaded to the central node; safety testing server is located in a central node, for the analysis of child nodes uploaded data packets, detect intrusions. Detect proxy process to deploy the accused after the host platform, the process for recording data on the system and related software and hardware information such as user privileges according to the detection mode used in the program, such as user application software usage, system hardware, and other related information, agent process through real-time monitoring port to transfer data packets to obtain data, and then upload the data to the central node, the server is responsible for safety testing save the analysis. Central node has child nodes receive real-time data upload, and data standardization and analysis, after the results of the analysis to detect whether the host accused risky behavior, and dangerous behavior warning.

With the gradual expansion of the size of the application environment, and centralized security system central node data analysis to detect pressure, a single point of failure and other shortcomings become increasingly apparent. In this regard, especially in large networks or large amount of data transmission network, now more commonly used system architecture for distributed architecture, the system architecture to set up multiple security detection server in the network, step by step information on the network is detected ñ?? Local safety testing server is responsible for managing the server Area accused host and sends the test results to the higher of the host server. This method will handle the data spread across different servers to achieve decentralized management overhead, reduce system load and speed up the system detects the speed of purpose.

B/S architecture of network security analysis system

Based on BS / architecture network security analysis system includes security agent client (SAC), the secure proxy server (SPS), with three components Server (CAS), in between the traditional CTP / IP protocol and the HTTP protocol by extending SSL the formation of a safe passage agreement to form a complete, tight security system. Overall structure as shown below Figure 3.

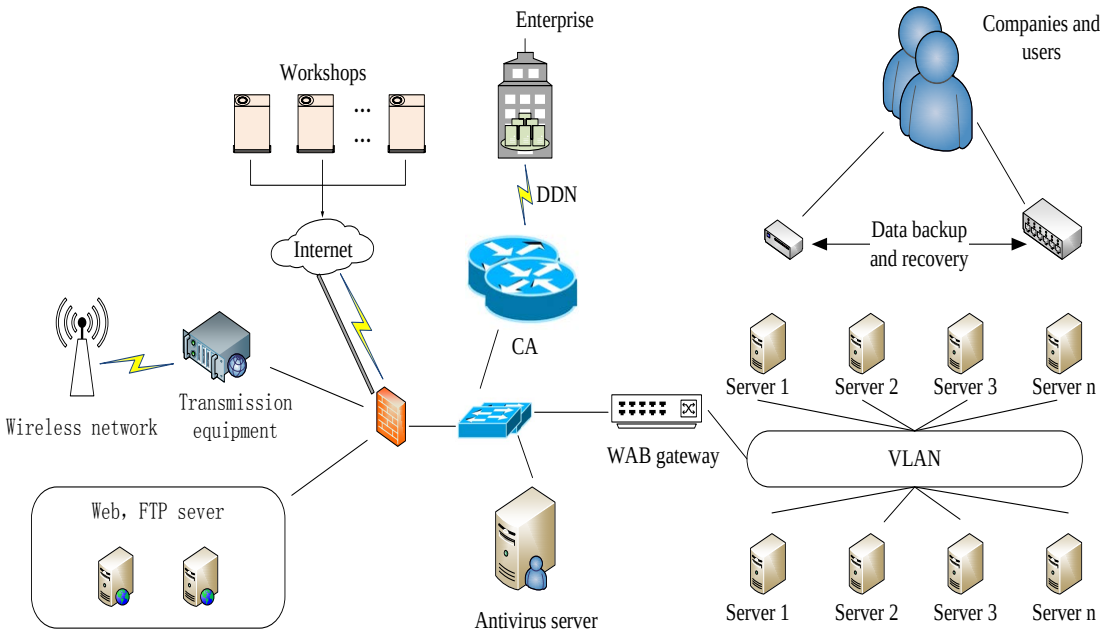

Figure 3. The Topology of network security system based on B/S

CA is a third-party organization. Typically the client and the server when exchanging identity information needs to be verified both at the same time believe that a third-party authority, since this way you can verify the authenticity of both identity. Transmitting information data in Internet or LAN environment risk of being tampered with, if there is no identification of the CA, the authenticity of the data is not reliable. Since it is a secure application platform for B / S application, the link is essential.

Security Agent client. Client browser must use a secure proxy client program that is running locally. It is mainly for storage in general proxy / forward function; users to use SSL to access secure sites, multi-level proxy functionality; access to encryption card, take to the user's private key, encryption algorithms and other information, in the form of a password to verify user identity, encrypt the information; important information submitted by users to digitally sign and send along with the request along to the secure proxy server; security agents operating parameters to configure the client.

Security proxy server. It is placed in the application server before a secure server, Web Server as a firewall to prevent clients direct access to Web Server. The main function of the SAC to establish secure SSL channel; access to encrypted machines, the main obtain encryption algorithm; access control; log includes log management, including the login log, access logs, exception log and digital signature server logs; communicate with CA server, authenticate users the authenticity and validity of the certificate; SAC sent the request to decrypt, restructuring, verify forwarded to the appropriate Web Server, and Web Server's response encryption, signature, restructuring forwarded to the SCA.

Encryption card and encryption machine used to provide authentication, data encryption and other hardware features. On the client, using the encryption card, each user has their own encryption card, the preservation of the user's private key encryption card, symmetric algorithms, asymmetric encryption algorithms (RS) A and data digest algorithm for data encryption, decryption, digital signature.

Conclusion

Network security is placed in front of web workers is an important issue, based B/S network architecture is very widespread, and the distance between the browser and the application server is usually more distant, and therefore ensure that the information transmitted over the remote line is particularly important. In this paper, the proposed analysis mode detection by security systems research findings direction of research related literature, and adequate research and analysis of the

existing network security detection systems cannot efficiently detect unknown intrusion defects, proposed a kind of an architectural pattern detection and analysis of network security, network security monitoring architecture design analysis model based on the system architecture. First introduced the idea of architecture as a basis for design ideas introduced distributed network security detection system, and one of the key design and implementation of the program. This paper integrates the existing network security detection technology to analyze the advantages and disadvantages of the current security detection technology to explore the limitations and significance of existing network security detection method proposed significance of this study.

References

[1] Shiravi H, Shiravi A, Ghorbani A. A survey of visualization systems for network security[J]. Visualization and Computer Graphics, IEEE Transactions on, 2012, 18(8): 1313-1329.

[2] Aydın M A, Zaim A H, Ceylan K G. A hybrid intrusion detection system design for computer network security[J]. Computers & Electrical Engineering, 2009, 35(3): 517-526.

[3] Cutillo L A, Molva R, Strufe T. Safebook: A privacy-preserving online social network leveraging on real-life trust[J]. Communications Magazine, IEEE, 2009, 47(12): 94-101.

[4] Al-Kuwaiti M, Kyriakopoulos N, Hussein S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability[J]. Communications Surveys & Tutorials, IEEE, 2009, 11(2): 106-124.

[5] Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, et al. Anomaly-based network intrusion detection: Techniques, systems and challenges[J]. computers & security, 2009, 28(1): 18-28.

[6] Shabtai A, Fledel Y, Kanonov U, et al. Google android: A comprehensive security assessment[J]. IEEE Security & Privacy, 2010 (2): 35-44.