1

Web and Database Security

Jiping Xiong, Lifeng Xuan, Jian Zhao and Tao Huang
Zhejiang Normal University,
China

1. Introduction

In recent years, with the frequent occurrence of security incidents, enterprises and organizations have now realized the importance of designing a safety information system. Today, information systems are heavily relied on web and database technologies, thus the risks and threats those technologies faced will also affect the security of information systems. Web and database security technologies can ensure the confidentiality, integrity and usability of data in information system, and can effectively protect the security and reliability of information system. Therefore, in order to better secure the information systems, we need to learn Web and database security-related knowledge. This chapter covers extensively practical and useful knowledge of web and database security.

This chapter can be divided into three parts: advanced security threats, the principles of safety design and safety audit; Advanced security threats section contains cross-site scripting (XSS) attacks, AJAX and SQL injection attacks and other security threats, which will be presented in detail; the principles of safe design section describe the general safety design principles to help design information systems security; last section describes the manual and automatically audit methods, and general security audit framework to help readers to understand more clearly.

2. Advanced security threats

2.1 Web security threats

2.1.1 AJAX security

As Web applications become increasingly complex, it is required for the performance of Web services is also increasing. AJAX (Asynchronous JavaScript and XML) (Garrett, 2005) technology is mainstream technology of Web2.0 that enables the browser to provide users with more natural browsing experience. With asynchronous communication, user can submit, wait and refresh mode freely, update partial page dynamically. So it allows users to have a smooth experience similar in desktop applications.

However, a variety of Web applications has brought us countless convenience, produced a series of security problems. When the introduction of AJAX technology, because of its inability to solve the security problems, the traditional Web security problems still exist, along with elements of the composition and structure of AJAX features, will lead to new

security threats. In recent years, adding AJAX elements in sites has become a very popular trend, and most websites are typical AJAX-based applications. As most of the website builders just enjoy the conveniences of AJAX technology, little is known about its security threat, resulting in most of the AJAX application sites have different levels of security risks. Here, we summarize and analysis the AJAX security threats.

1. Security Threats of AJAX Technology

a. The Deficit of JavaScript Language

JavaScript is a widely client-side scripting language, originally designed and implemented by Netscape, and it has been widely used to reduce the burden on the server. JavaScript scripting language features determine its presence in all kinds of security risks:

- JavaScript is an interpreted language. In the interpretation process, every error is a runtime error. Run-time error can only be found during runtime. If somewhere in the code the programmer has left a Bug, but the logic of the code at run time is not running to the area, then the bug will not be found, which leaving significant risks to the application. To detect, locate the error position of interpreted language is quite difficult.
- JavaScript is a weak typing language. Weak typing languages do not need to declare variables at the time the programmer declare the variable. This flexibility often easily leads to many problems.
- JavaScript code has dynamic nature. It can be dynamically generated code, and used the eval-function dynamic execution; or you can directly modify the existing function. Once the attacker can gain control of the JavaScript code, he can overwrite the other user-defined methods and even the browser built-in method, thus cause many serious malicious behaviours.

b. Problems of Asynchronous

Asynchronous communication is the highlights and core idea of AJAX technology. But asynchronous will also introduce a series competition problems.

2. Issues of AJAX Framework

a. Explosion of Client-Side Logic

Programming client-side logic using JavaScript will bring the client-side logic to public. Users can easily through the browser's View Source feature to see the client code.

b. Incomplete Server

Most AJAX programmers validate user input at client-side, though it reduces the burden of server, it lefts room for security risks.

3. Traditional Web Security Threats of AJAX

AJAX framework gives users a good experience in desktop's application, users no longer have such a long wait for the server to response and refresh the page. However, this feature also poses a problem: the user does not know what the current request was sent, did not even know the current request was sent. This feature allows many of the traditional Web attacks in a more intimate manner. Main traditional Web security threats are (Razvan & Maria, 2010):

- AJAX framework of SQL injection;
- AJAX framework of XPath injection;
- AJAX framework for cross-site scripting attacks (XSS);
- AJAX framework for cross-site request forgery attacks (CSRF);
- AJAX framework of denial of service attack (DOS).

4. Security Threats Introduced by AJAX

The introduction of AJAX, initially to solve the user to submit a request in the browser when the server response is required after a long wait, refresh the entire page to the next step of the problem. But AJAX technology to bring convenience, but also introduces some security threats.

a. JSON Injection and JSON Hijacking

JSON (JavaScript Object Notation) (Crockford, 2006) is widely used lightweight data transmission and exchange format in AJAX. JSON is based on a subset of JavaScript and developed from JavaScript Array and Object, and the adopted text format is completely independent with language. The data of JSON and can be transmitted cross-platform. Therefore, JSON Injection and JSON Hijacking are current two aspects of security threats.

b. Trust Crisis of AJAX Proxy

For security reasons, JavaScript code is limited to running in a sandbox, JavaScript also prohibit access to third-party domain. But sometimes you need to call in the AJAX third-party services, such as components Mashuop procedures. Solution to this is to build an AJAX proxy that the Web server to create a Web service, only forwarding calls to third-party Web service request. AJAX proxy allows the client calls the Web service as a third party may also have to provide AJAX proxy servers and third-party server, a crisis of confidence. First, the attacker can access through the AJAX proxy direct access to many previously unavailable resources. Meanwhile, the attacker via AJAX proxy attack on third-party Web server, you can also hide the source of the attack, showing up as if from the AJAX proxy attack (Anley, 2002).

c. Disclosure of User Data

AJAX technology gives users a better browsing experience, but some AJAX-based application inadvertently brought the disclosure of user data. AJXA technology is widely used in such situations: a user registers a mailbox, enter the account he wants to use, after he moves to the next input section, the browser prompts the user name input box: the account that you are applying has been applied, please re-apply. This design reflects good human-based design rule, the user does not have all the information before being prompted to fill out and submit the account has been to apply for. But in this way the user data will be leaked in the unconscious. False malicious attacker by entering any letters, numbers, combined to form the account, you can immediately know whether the mailbox has been registered. If you know the mailbox already exists, there may occur spam, or send e-mail containing the malicious XSS code may be so. Enumeration by simple repetition, the attacker can even know the mail server name of all existing accounts, which will undoubtedly bring great threats.

2.1.2 Cross site scripting

Cross-site Scripting (also known as XSS or CSS) occurs when dynamically generated Web pages display input that is not properly validated. In XSS, malicious attackers acted as normal visitors upload Malicious Script as JavaScript codes etc. to Web server by utilizing the bugs of utility programs or codes in the Web server. Attackers also send URL links including malicious script to objective users. When Web users visit the pages containing malicious script or open the received URL links codes in the Web sites, users' browsers will auto-load and execute the malicious script codes. This attacking procedure indicates that XSS is actually a simple attack technology. In most cases, malicious attackers attack users indirectly by utilizing Web server, and direct attack occurs merely.

XSS is a passive attack. First of all, by utilizing the XSS bugs in the Web programs, malicious attackers construct a trap page and the malicious script can be saved in the page content or URL. The URL of this page is then announced in the BBS after embedding to e-mails or disguising attractive titles. If the users visit ULR, the JavaScript will be executed by attackers' browser. The procedure of XSS attack is shown in fig. 1.

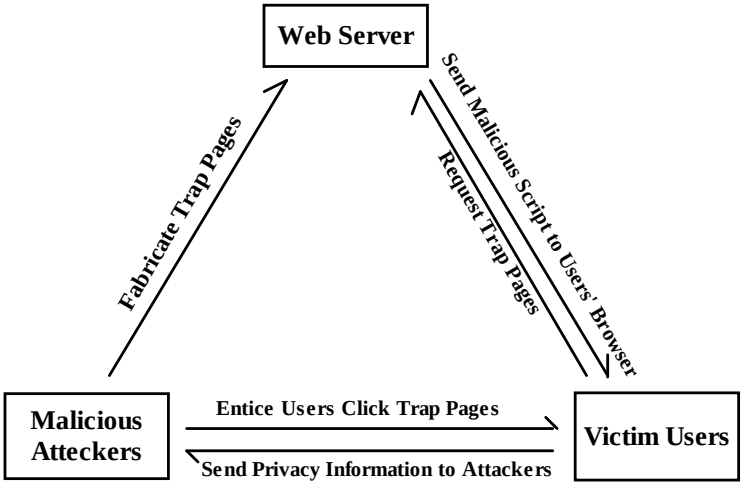


Fig. 1. The Process of Cross Site Scripting Attack

2.2 Database security threats

Database security relates to two parts: data visiting and data recovery. The first part can be realized by using a suitable authorization to make sure that the legal users can get their right data and reject all exceeding authority at the same time. The latter part means that database can recover the data securely and completely.

Recently, database is facing the problem of security hole e.g. privilege elevation, SQL inject, XSS, data leakage and improper error processing.

2.2.1 SQL inject

1. SQL Inject Principle

SQL Inject refers that the attackers deceive database server to execute unauthorized wilful inquire and illegal operation through adding extra SQL statement element to the end of predefined inquire statement in application programs. The essence of SQL Inject is utilizing the bugs caused by the programmers who did not detect or incomplete detect the database inquiry request, submitting malicious SQL statement and cheating server executes malicious inquiry. At last, the attackers can get the sensitive data or control the whole website.

The main reason for SQL injection attack to succeed is that when dynamically generating SQL statement commands, websites only directly using the subscribers inputted data without any verification.

2. Process and Methods of SQL Attack

In SQL attack process, the attackers firstly trial the SQL inject bugs in application programs by design inputs. The executive SQL statements are then imported to control implement programs. After obtaining the database information, the attackers acquire the administration authority of server system.

a. Discovery of SQL Inject Bugs

Discovery of SQL inject bugs brings necessary information to further attack. Before SQL attack, the attackers need to identify the aim database platform and decide what SQL attack statements or methods should utilize (Halfond et al., 2006).

The common methods for SQL inject bugs are as follows:

- Add single quotes etc. characters to the end of submitted inquiry. So that attackers judge if the inject bugs exist depending on estimating database type of prompt message return from the server.
- Push `and 1=1` and `and 1=2` to the end of submitted inquiry. Bugs exist when `and 1=1` stay regular and `and 1=2` go wrong, and then illegal inquiry and other malicious behavior occur. It means that illegal inquire statements can be added after inquiring and assaultable bugs existed.
- A regular method to find bugs is to judge database style by the build-in variable and function of database.

b. SQL Inject Bugs Utilization

After finding out the bugs, attacks including illegal inquire database, obtaining secret information and users data, controlling database and server system occur.

- Speculating table name and field name. Attackers take advantage of SQL statement, such as `and (select count(*) from TestDB.dbo.tablename)>0;` to guess table name. If the table name have existed, the webpage returns to regular.
- Obtaining field value. After getting table name and column name, field value is generated by utilizing ASCII word-by-word decoding.

After these two steps, the attackers can get data, user name, password and information in database.

- Further attack. From definition and principle of SQL inject, we know that attackers are interested in administrators authorizations rather than their account numbers. The administrator authorizations will bring further attack and acqire higher authorization for attackers to add Trojan to webpages.

3. Security design principle

3.1 Web security design principle

We should obey the following principle when designing and deploying computer network security.

1. Balance Analysis Principle of Demand, Risk and Cost

According to the existing technology, there is hardly a perfect Safety network. We should do some qualitative and quantitative analyse to threaten and possible risk network faced. The standards and measures are then made to confirm security policy of system.

2. Principle of Comprehensiveness and Integrity

We can analyse security issues of network and formulate specific measures by using views and methods of system engineering. Multi-methods make a prefer security measure. A computer network including links of human being, device, software and data take an important role in network security, and only analyse and treat in whole view can they obtain valid and executive measures.

3. Consistency Principle

Consistency Principle means that network security issues should concurrent exist with the whole network operating cycle, and security architecture should keep in line with network security. Actually, network security strategies should taken into consideration in the beginning of network construction rather than at the end of this procedure with characters of facility and low cost.

4. Principle of Security and Reliability

Guarantee of system security is very important. In procedure of design and implement, specify measures are adopted to ensure security of information secure product and technology proposal. By strict technology administration and redundancy configuration of device, quality of product and reliability of system can be guaranteed.

5. Principle of Advanced Technology

Advanced technology system and standard technology are required in security design.

6. Principle of Easy-operation

Security measures are manually completed. Complexed measures can always lead to high requirement for administrators, and low security. Otherwise, the measures should be friendly to operation of system.

7. Principle of Adaptability and Flexibility

Security measures must change with the developing of network performance. Characters of easily to adapt and modify are required.

8. Multiple-protection Principle

Perfect security protection methods merely existed, so that a multiple-protection system is constructed to protect each layer. When one layer is broken, any other layers can still protect information.

Methods as installing fire wall, setting up isolation region for protected resource, encrypting the sensitive information being stored and transmitted, providing identity authentication and building secret passage, providing digital signature for audit and tracking to software without any security guarantee are adopted to ensure Web service security.

1. Install Fire Wall

The most popular security method is providing an isolation region to LAN or website. Fire wall of LAN is a function module inside computer or network equipments between innernet and Internet. Its purpose is to provide security protection to an innernet or host and control access objects, so it can also called access control technology. There are two operation mechanisms for fire wall e.g. packet filtering and agency. Packet filtering aims at the service provided by host of special IP address. Its basic principle is to intercept and capture IP packet of IP layer in network transmission, then find out resource address and destination address, source port and destination port of IP packet. Whether to transmit IP packet is based on fixed filtering principle.

Agent is achieved in the application layer, the basic principle is to construct an independent agent program for Web services, and client program and the server can only exchange information by their own agent programs rather than allow them to interact directly with each other.

2. Encryption for Confidential Information

This method is particularly effective to protect confidential information, which can prevent wiretapping and hacking. Transmission encryption in Web services is in general achieved in the application layer. When WWW server sends confidential information, firstly, it selects keys to encrypt the information, based on the receiver's IP address or other identification; After browser receives the encrypted data, it decrypts the encrypted data according to source address or other identification of the information in IP packet to get the required data. In addition, transmission, encryption and decryption of information at the IP layer also can be achieved by encrypting and decrypting the whole message to ensure information security at the network layer.

3. Provide Identity Authentication for the Client / Server Communication and Establish A Secure Channel

Currently some network security protocols e.g. SSL and PCT have appeared, which are based on the existing network protocol. These two protocols are mainly used for not only protecting confidential information but also preventing other unauthorized users to invade their own host.

SSL protocol is a private communication and includes technology of authentication, signature, encryption for the server, which can not only provide authentication for the server but also provide authentication for the client according to the options of the server.

SSL protocol can run on any kind of reliable communication protocols, e.g. TCP, and can also run in application protocols e.g. HTTP, FTP, Telnet etc. SSL protocol uses X.509 V3 certification standards, RSA, Diffie-Hellman and the Fortezza-KEA as its public key algorithm and uses the RC4-128, RC-128, DES, 3-layer DWS or IDEA as its data encryption algorithm. The authentication scheme and encryption algorithm provided by PCT are more abundant than SSL, and it makes improvements in some details of the agreement.

IPSec protocol is used to provide end to end encryption and authentication services for public and private networks. It specifies all kinds of optional network security services, and the organizations can integrate and match these services according to their own security policy, and they can build security solution on the framework of the IPSec. The protocol provides three basic elements to protect network communications, the basic elements are "Authentication Header", "Encapsulating Security Payload" and "Internet Key Management Protocol".

HTTPS protocol (Secure Hypertext Transfer Protocol), which is built on its browser for compressing and decompressing the data, and returns the result which is back to the network.

4. Digital Signatures for the Software

Many large companies use digital signature technology for their software, and claim that they are responsible for the security of their software, especially e.g. Java applets, ActiveX controls, which will bring risks to Web services. Digital signatures are based on public key algorithms, using their private key to sign its own released software, and are authenticated by using the public key. Microsoft's Authenticode technology is used to identify a software publisher and prove that it has not been damaged. Authenticode is software for client, which monitors the ActiveX control, Cab files, Java applets, or download of executable file, and look for the digital certificate to verify in these files, and then show warning words, the certificate organization's name and other information to the user for possible security problems. Digital signature can protect the integrity of the software, and it is sensitive to illegal change of the software in the transfer process.

3.2 Database design principles

Users enter into the database system through the database application program when users firstly access the database, database applications deliver the username and password which is submitted by the user to the database management system for certificating, after determining their legal status, users are allowed to enter. They also must pass the authentication when operate objects, tables, views, triggers, stored procedures etc. in the database. How can users operate in application and database is depended on rights allocation and constraints of accessing control.

1. Secure Database System Model

Criteria based on security database, you can create a simple security database system model which is divided into four layers: system layer, including data access, encryption and decryption algorithm; function layer is the key to the whole system, including key distribution mechanism, fast indexing mechanism and derive control; interface layer is directly user-oriented, which includes the function of user authentication, authorization

management, database maintenance and query management; At application layer, users can manage database through not only interactive ways but also command mode.

2. Management Strategy of Database

a. Access Control

Access control is the rights control of user access to all kinds of resources of the database, which is divided into two stages: one is security account identification, the other is the access permission identification. In the security account authentication phase, the user logins for the authentication, if it's successful, he can connect to the SQL Server, otherwise it will reject the connecting requirement. Access license verification refers to that after the user connect to SQL Server, the system determine whether they have license to access to the database according to the user account stored in the database and correspond to server login identification. Access control can prevent the illegal users.

b. Database License

After the legal users access to the server and database, the database access mechanism will control the legal users to operate the data objects. First of all, statements in the database license will limit the database user to carry out some SQL statements. Secondly, objects in the database license will limit the database user to carry out some tasks of the database objects.

c. Establish Data Security by Using System Stored Procedures

As the database administrator, if you want a user to have a select right rather than the delete right, at this time you can achieve the goal by establishing stored procedures, thus protecting the safety of the data.

d. Establish Data Security by Using the View

If the administrators give users the permission to access the database tables and form a too large user access area, it will cause threats brought by users to data security of the database. To avoid this situation, you can achieve data security view through the way of establishing data view.

e. Establish Data Security by Using the Database Role

This role is used for setting license at a time that number of database users can access to the database, if permission is not deployed properly, it will threat data in the database directly. As an administrator, you should be very careful when you give permission to the public role.

f. Data Backup

Data backup is principal work in the course of daily management of the database. When the server or database system breaks down, the original data is difficult to recover without a backup strategy. Therefore, the database should be installed in security zone of their intranet, and can not be connected to the Internet directly. In addition, different computers should implement backup strategies to protect data security when people deal with abnormal failure.

g. Database Encryption

Database encryption requires that database cryptography changes plaintext into cipher-text, and cipher-text data stored in the database. Cipher-text is decrypted to get clear information when queries, so data will not be leaked even if the hardware store is stolen, thus the database system security is greatly improved, of course, the cost also increases. Response to attacks from the network level, the database mainly uses many ways e.g. installing a firewall, doing intrusion detection etc. to improve its safety performance. Firewall resists the incredible connections from outside. Intrusion detection systems are generally deployed in firewall, and detect abnormalities on the network and the host through Network packet interception analysis or Analysis of log.

h. Audit Trail and Attack Detection

The audit function records all database's operation in the audit log automatically when the system works, attack detection system analyses and detects attempt of internal and external attackers according to the audit data, and reproduces events which leads to the status of the system, find vulnerabilities of the system by analyzing, and then trace the relevant responsible person.

4 Security audit

4.1 Definition of security audit

Security audit is based on certain security policy, improving system's performance and safety by recording and analyzing historical events and data. Security audit includes all actions and instruments, e.g. testing, assessing and analyzing all of the weak links in the network information system to find the best ways to let the business run normally, based on the maximum guarantee of safety. It is to ensure the safe operation of network systems and prevent confidentiality integrity and availability of the data from being damaged, prevent intentional or unintentional human error and detect criminal activity on the network. The network status and processes can be targeted to recorded, tracked and reviewed by using the audit mechanism, and find safety problems. In addition, the audit can provide the basis of making filtering rules for online information, if the harmful information is found in the website, it will be added into the list of route filtering, to reject all information of IP addresses on the filtering list through information filtering mechanism. Fig.2 gives a brief overview flowchart of security audit.

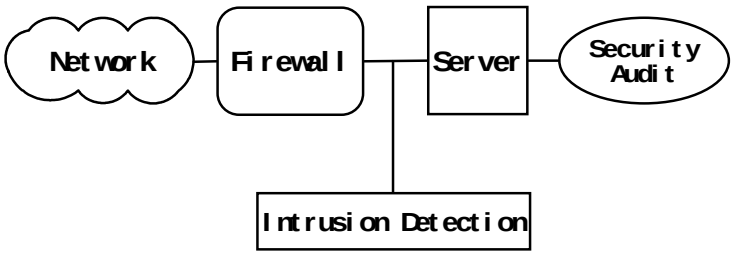


Fig. 2. Situation of Security Audit System in Network

Security audit techniques use one or several security testing tools (generally referred to as scanner), first of all, it will scan loopholes and inspects security vulnerabilities of the system, then achieve the inspection report about the weak link of system, at last it will take security protection and emergency measures according to the response strategies.

Traditional security audit has the function of "old records", pay attention to the audit afterwards and emphasize the deterrent of the audit and verification of security incidents. With the change of United States national information security policy, doing the so-called "defense in depth strategy information" in the information infrastructure is put forward by Information Assurance Technical Framework (IATF), this strategy requires security audit system to participate in the active protection and response. In modern time, network security audit is an all-round, distributed, and multiple-level strong audit concept, which breaks the previous concept of "log" and other shallow level security audit, and it's consistent with the requirements of protecting, detecting, replying and recovering (PDRR) dynamic process, which is put forward by IATF. It can protect and response to the information actively on the basis of improving the breadth and depth of audit.

1. Based on the objects of audit, security audit is divided into:
- Operating system of audit;
- Application system of audit;
- Equipment of audit;
- Network application of audit;
2. Based on the ways of audit, security audit is divided into:
- Distributed audit: audit information is stored in the server and security equipment, and system security administrator will review it. Distributed audit is applied to enterprise information system which demands less with information security protection.
- Centralized audit: audit information in the server and security equipment is collected, collated, analyzed and compiled into the audit report. Centralized audit is applied to enterprise information system which demands more with information security protection.
3. Based on control mechanism of audit, security audit is divided into:
- Host based audit. Host based control mechanism can control the specified host system, its control ability is in detail;
- Network based audit. Network based control mechanism can real-time monitor network security risks, to realize the comprehensive protection of intranet resources;
- Combination of host and network based audit. It can not only monitor host but also the network.
4. The emphasis of the information system security audit are mainly the following types:
- Network communication system: It mainly includes analysis, recognition judgment and record of the typical protocol in the flow of network, intrusion detection of Telnet, HTTP, Email, FTP, online chat, file sharing etc, as well as for traffic monitoring, recognition and alarm of anomaly traffic and network equipment operation monitoring.
- Important server host operating system: It mainly includes audit of the startup of system, running situation, the administrator login, operation situation, system configuration changes (e.g. the registry, the configuration file, the user system) as well as a worm or virus infection, the resource consumption; audit of hard disk, CPU, memory, network load, processes, operating system security log, system events, access to the important document.

- Main server host application platform software: It mainly includes the audit of the running of the important application platform processes, Web Server, Mail Server, Lotus, middleware system, health status (response time) etc.
- Main database operation audit: It mainly includes the audit of the database process operation conditions, violated access behaviour to operate the database directly by passing the application software, the database configuration changes, data backup operations and other operations of maintenance and management, to access and change important data, and data integrity.
- Main application system audit: It mainly includes the audit of office automation system, document flow and operation, webpage integrity, interrelated service systems etc. The relevant business system includes normal operation of business system, important operations of setting up or stopping the user, authorized change operation, data submission , processing, access and publishing operation, business process etc.
- Main regional network client: It mainly includes audit of virus infection situation, file sharing operation through the network, operation of copying or printing file, the situation of unauthorized connect to Internet through the Modem, installation and operation of non business abnormal software.

4.2 Execution of security audit

4.2.1 Process of security audit

Process of Security audit can be divided into two modules, including the collection of information and the security audit, the structure is shown in the following fig.3.

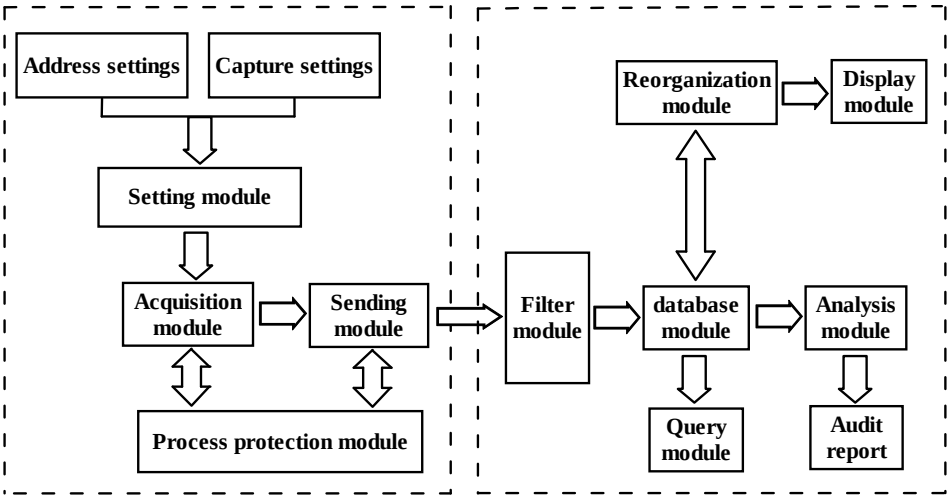


Fig. 3. Architecture of Security Audit System

Information gathering side runs on the system server. Information collecting side transmits information to the security audit terminal through a special security channel, security audit client runs on a stand-alone computer separately. To ensure the safety of audit side, the computer which operates safety audit module is not access to the server's LAN. To ensure

the communication between audit module and information collection module, we do a dual-channel design, the user can set any ways to communicate, and the system can automatically switch to another way when one way can not work normally.

Information collection module collects the data which needs to be audited, including network packet, process information, port information, file access information, and modify the registry information, as well as a variety of server logs, such as WWW logs and security logs. In order to process conveniently later, all data is stored in the audit module of the database.

4.2.2 Key technologies of network security audit system

1. Analysis of Data Source of Network Security Audit System

For security audit system, selection of incoming data is the key problem to be solved, data source of the security audit can be divided into three categories: Based on the host, based on network and other channels. In order to select the appropriate data sources, it analyzes each class of data source respectively as follows.

a. Data Source Based on the Host

Data sources of the network security audit based on the host , including audit records of the operating system, system log, log information of application system and information based on the target.

b. Data Source Based on the Network

Network data is the most common source of information in the current network security audit system and commercial intrusion detection system. The basic principle is that when the network data stream transmitting in the network, using a special data acquisition technology to collect the data transmitted in network as the data source of security audit system.

c. Other Data Source

Data source from other safe products mainly refers to log files produced by safe products e.g. firewall, authentication system which are operated independent in the target system. These data sources also should be considered by security audit system.

Data source from network device e.g. a network management system, using information provided by SNMP (Simple Network Management Protocol) as data source. Out-of-band data source refers to data information provided by the artificial way, which is contrived and non-systematic, e.g. recording what happened in system environment manually, including hardware error information, system configuration information, system crash, other kinds of natural hazard events etc. Out-of-band data source may play an important role for later analysis.

In general, it will improve the performance of security audit system if active log of the network and its safe device are used as audit data source.

2. Functions of Network Security Audit System
a. Data Acquisition and Storage Capability

Data collection captures data-packets based on the data link layer. It filters out the packets without audit and saves selectively according to the defined policies and system analysis requirements. Data acquisition and data files are generated to provide data source the network security audit system. It is the key link of the network security audit system, and is the basis of data analysis and processing. Because the system only access the external computer and the user network audit, it is not necessary to collect or store intenal network data.

b. Log Data Management Capabilities

The log data with sustainable growth are very large, even a small network produces over 3 G network logs per day. Integrated mechanism of backups, recovery and processing is constructed for management of network security logs rather than simply delete.

c. Feature of Automatical Analysis and Statistical Reports Generation

The network will generate a lot of daily log information, and it is difficult for administrators to process these huge amount of work. A visualized analysis and statistical reports automatically generated mechanisms need to be provided to ensure that administrators can find a variety of network anomalies and security events effectively.

d. Data Analysis and Processing Functions

System access to external networks, achieve the user's computer and the contents of the audit network behavior via processing and analyzing to the data collected and preserved. The core is protocol analysis. Web content audit system includes web audit, mail audit, FTP audit and user log etc. The function data play a decisive role in audit results.

e. Function of Real-time Network Status Monitoring

Real-time monitoring function mainly includes analysis, identification, judgement and record of typical protocol in network traffic, intrusion detection for Telnet, HTTP, Email, FTP, Internet chat, file sharing etc. flow monitoring, and identification and alarming of unusual flow.

f. Network Service Control Function

Network service control function achieves control of host and service for user access to network services, to be able to support the operations of user authorization, settings of white list host and user access rules.

3. Network Security Audit System Architecture

Network security audit system mainly consists of three modules.

a. Data Collection Module

Data collection module acquires network packet of users' operation by monitoring and core filtering technology depending on imaging feature of switchers and user-defined strategies. The key to realize this module is to acquire accurate and complete packet. Data integrity of data acquisition modules is determined by the exactness and completeness of audit results.

b. Packet Processing Module

Protocol analysis is a key step in the data packet processing. Main job of packet processing module is to capture the data packets and determine the protocols e.g. TELNET, FTP and

other protocols it belongs based on their header information. According to the formats, transmission mode and message content, it make the user's operation to restructure, restore, and finally it restore user data and submit to the audit module.

c. Data Audit Module

According to the rules defined format, the achieved user information e.g. TELNET and FTP commands, SQL statements, manipulate objects, operating keywords will match with the user-defined strategy in rule base. Responses are made according to the matching results, and the audited data are recorded into audit logs. The rule base is generated based on the visit strategy deployed by authorized administrator. The authorized administrators formulate or modify the strategy, and issue it to the next rule base. In process of utilizing audit system, administrators gather experience and add novel strategies constantly according to the issues in system usage making the rule base more and more abundant.

4.2.3 Security audit approach

1. Methods Based on Rule Base

Rulebase based security audit method is the process below. Administrators extract feature of attack behaviors, and then push them into rulebase after represent by script language. When executing security audit, network attack behaviors are detected after the comparison and matching operations e.g. keywords, regular expression, fuzzy approximation degree between the above rule base and network data. But these rules are only fit for certain specific types of attacks or attack software, and failures of rule base are generated when new attack or upgraded software turns up.

2. Mathematical Statistics Based Method

Method of mathematical statistics is to create a statistic description for object firstly e.g. average value or variance of network traffic. And then value of characteristic quantity under normal circumstances is calculated to compare with actual network packet. If actual value is far different with regular value, the attacks is then occurred. However, the biggest problem of mathematical statistics is how to set the thresholds of statistics i.e. cut-off point between the normal and abnormal value, which often depends on the administrator's experience that inevitably prone to false and omission.

3. New Method Based on Network Security Audit System : Learning Data Mining

The biggest drawback of the above two methods is that the known intrusion patterns are hand-coded inevitably, and can not applicable to any unknown intrusion patterns. So people start to pay attention to the the data mining method owning the learning ability. Data mining is the process of analyzing mass data completely including data preparation, data preprocessing, establishment of mining model, model evaluation and interpretation. It is an iterative processing and can get a better model by continuously adjust methods and parameters. The main idea of the network security audit system is to find *normal* network communication patterns from *normal* network communication data and then achieve the purose of detecting web accack behaviors by relewance analysis with the regular attack rule base.

Firstly, the system collects data from collection points, and put the data into database after processing. Invasion evens are detected by executing engine of security audit to read in rulebase. The invasion is then recorded into invasion time database as well as the regular network visiting data are recorded in regular network database, and regular visiting patten can be abstracted by data mining. Latest rulebase is acquired from old rulebase, invasion events and regular visiting patterns. The above procedure is repeated and self-learning constantly until achieving a stable rule base. Data mining technology extracts the regular visiting mode semi-automatically from the mass of the normal data, which can reduce the human perception and experience participation which declining the possibility of misinformation.

4.2.4 How do security audit

1. Establish Audit System

An audit system which leads to excellent audit should to be developed to ensure that auditors do their work on a regular basis. In the audit system, auditors should clearly know what the audit objects are. The main focus is the enterprise's information protection e.g. the server, backbone switches, routers and security devices.

2. Focus on Safety Auditors fostering

Safety audit involves massive products and wide content. The basic information of the audit come from operating system, network systems, security devices, applications system etc. Security auditors are not only necessary to understand the operating system knowledge, but also should be familiar with network protocols, database, virus infection mechanism. Moreover, auditor should understand the basic situation of application systems as well as master the work principles of servers, switches and security devices, especially the understanding a variety of security policies of information systems deeply. Thus, in the audit processing, the analysis of massive information can be developed and the observing and thinking ability can be cultivated.

However most of the enterprise information system security audit work is just begin without any own professionals. Although security audit can be conducted by professional security company or buying excellent audit software, it is still harmful in term of the safety and long-term development. The audit process involves a number of important enterprise information especially the system security weaknesses. Serious threaten will occur when criminals turn up or the workers are in low ability to analyze the weak links. From the above analysis, the security audit work should be accomplished by the professionals in the enterprises.

From the angles of security audit requirement for auditors and situation enterprise internal personnels, the enterprise should lay emphasis on the foster of information system administrators, network administrators, security guards especial the safety audit personals. Because all security policy, security system and security measures are developed by human beings, personnels with high quality and ability are required in developing management standards of enterprise information system and ensuring enterprise information security.

3. Reasonable Structure of the Security Audit System

The premise of improving the safety audit is to build a security audit system in line with business needs. In building a security audit system, the follow issues should be considered:

a. The profundity and scope of audit. The audit profundity and scope determine the complexity of the audit system, which are also the basis of audit products selection.
b. Problems of data sources. An audit system operation is based on data from the system at all levels, and how to obtain the data sources of audit system is the most critical issue.
c. Relationship with the original systems. To ensure the normal operation of the original system go smoothly in the realization of the audit, and the least modification and the minimum impact on system performance make the audit perfect.
d. Eliminate of audit function ignore. If the audit system is easily bypassed, it would lead to serious problems.
e. Effective utilization of audit data. In establishing an audit system, the lack of deep utilization of audit data will lead to weak audit system effection.

Network security is accompanied with the production of computer, especially the present popular network, security problem is emphasized by at all levels of sectors and industries especially the area of intranet security. Network security is a huge and complex dynamic system, hardware equipments provide basic security for the network, but a system which continues to improve can find a kind of dynamic equilibrium only with the help of network security audit system by doing real-time audit and effective evaluation to the system which has been established and discovering the potential safety hazard in time. These problems will become hot spots for future security research in building a solid and reliable network security audit system.

Computer network security audit is a very complex and extensive research subject, as an indispensable part in integrity security framwork, it is a complement for a firewall system and a intrusion detection system. It involves a wide range of knowledge. With the complexity of computer operating system and network communication technology increasing, the complexity of network security audit is also increasing. How to improve network security audit system performance of various technologies and how to build a strong network security audit system need to further constantly explore and research.

5. Conclusion

Web and database technologies are in a rapid evolution roadmap, for example web3.0 and graph database (Angles, 2008) are getting more and more attention. At the same time, related security issues will appear, but the fundamental security rules will remain the same. In this chapter, we briefly overview the advanced web and database securities, the security design principles and security audit rules and methods. Due to the limitation of chapter length and variable programming languages, most contents in each section are general guide lines and rules. When deploying practical information systems, we need to map those rules to real implementation. Information systems can be more secured if we know and apply those technologies.

6. Acknowledgment

This work is partially supported by Zhejiang Provincial Youth Natural Science Foundation (Q12F020022) and Zhejiang Educational Foundation.

7. References

Jesse James Garrett (Feb 2005). Ajax: A New Approach to Web Applications. Available from http://adaptivepath.com/ideas/ajax-new-approach-web-applications

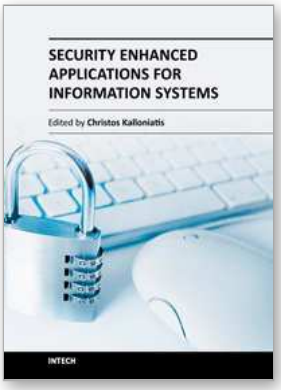
Raducanu Razvan & Moisuc Maria (2010). The security of Web 2.0 and digital economy. *Recent Advances in MATHEMATICS and COMPUTERS in BUSINESS, ECONOMICS, BIOLOGY & CHEMISTRY*. pp.168-170, ISSN: 1790-2769

D. Crockford (July 2006). The application/json Media Type for JavaScript Object Notation (JSON). *RFC 4627*, July 2006

Anley C. Advanced SQL Injection in SQL Server Applications. *Next Generation Security Software Ltd*. 2002.

Halfond W G ; Viegas J and Orso A (2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, Mar. 2006

Renzo Angles, Claudio Gutierrez. Survey of graph database models. *Journal ACM Computing Surveys*, Volume 40 Issue 1, February 2008



Security Enhanced Applications for Information Systems

Edited by Dr. Christos Kalloniatis

ISBN 978-953-51-0643-2
Hard cover, 224 pages
Publisher InTech
Published online 30, May, 2012
Published in print edition May, 2012

Every day, more users access services and electronically transmit information which is usually disseminated over insecure networks and processed by websites and databases, which lack proper security protection mechanisms and tools. This may have an impact on both the users' trust as well as the reputation of the system's stakeholders. Designing and implementing security enhanced systems is of vital importance. Therefore, this book aims to present a number of innovative security enhanced applications. It is titled "Security Enhanced Applications for Information Systems" and includes 11 chapters. This book is a quality guide for teaching purposes as well as for young researchers since it presents leading innovative contributions on security enhanced applications on various Information Systems. It involves cases based on the standalone, network and Cloud environments.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821