The Research and Application of Network Security Technology in the University Network

Ling Jia
The Chinese People‘s Armed Police Force Academy, Lang Fang,China
jialing123321@163.com

Abstract—**The rapid development of computer network technology and information technology, brings greatly facilitate and enrich people's lives for information transfer and fast access, improves work efficiency. At the same time, the network information security is followed. How to ensure the network information is transferred security, which is the problem that various network information systems must face, and also a difficult and hot issue to be researched. In this paper, a variety of effective network security technologies are studied and corresponding implementations are provided for the information network system in the university.**

Keywords-network security, information transmission, encryption, user authentication

I. NETWORK SECURITY INTRODUCTION

With the wide spread and rapid development of the computer network technology and information technology, network security issues of information systems become increasingly complex and important. Security technology is an important aspect of network applications, and also the current difficulties and research focus in information security disciplines.

Computer network security as a very complex field, it references to technology, products and management and so on, is a comprehensive cross-disciplinary, involving computer science, network technology, cryptography, information security technology, applied mathematics, number theory and information theory and other disciplines. It has very broad range of applications, including network equipment security, operating system security, application services security, data security and information management security. With the deepening process of information system and the rapid development of network technology, network security areas are more and more abundant, and develop multi-level three-dimensional network security architecture.

In this paper, how to increase system's security by software is deeply studied for the information network in the university, data transmission in the network will not be exchanged, removed, tampered, disclosure or destruction is researched, which will enhance system reliability and controllability.

II. DESIGN PRINCIPLES OF NETWORK SECURITY IN THE UNIVERSITY

In the university, it usually contains multiple information systems to manage resources, teaching information, multimedia, etc., in order to realize informational and automatic office. Various information systems often use different implementation because of creation time, technology and applications, which constitutes multiple heterogeneous data sources. Using multiple heterogeneous data sources and each data system with different design is to achieve an effective information security strategy. Meanwhile, it is also very important to share information between heterogeneous data sources. The following will examine the network architecture and security principles in the university.

A. The network architecture in the university

Information system in the university usually has multiple independent application systems, such as student information system, instructional management system, library management system. Information between these systems is related, therefore, it needs to eliminate information silos, which requires a data exchange center system, to achieve sharing information between information systems. Figure 1 is the network architecture diagram in the university.

Each information system constitutes an independent system, saves different information of the university. Information systems achieve interaction with each other through data exchange center system, complete effective information retrieval and management.

B. The principle of university security

Based on the above university network architecture, in this paper, following areas of network information security in the university network is researched.

In the data exchange center system, the information of a registered user is authenticated; the encrypted XML document is used to achieve an effective interaction of information between the data exchange center system and various business systems, encryption and decryption module of each business system uses different approaches to achieve; each business system uses different implementation techniques, forms independent heterogeneous data sources, after the invasion of a system is not into other business systems in the same way. Figure 2 is a schematic diagram of university network security.

Published by Atlantis Press, Paris, France.
© the authors, 2013

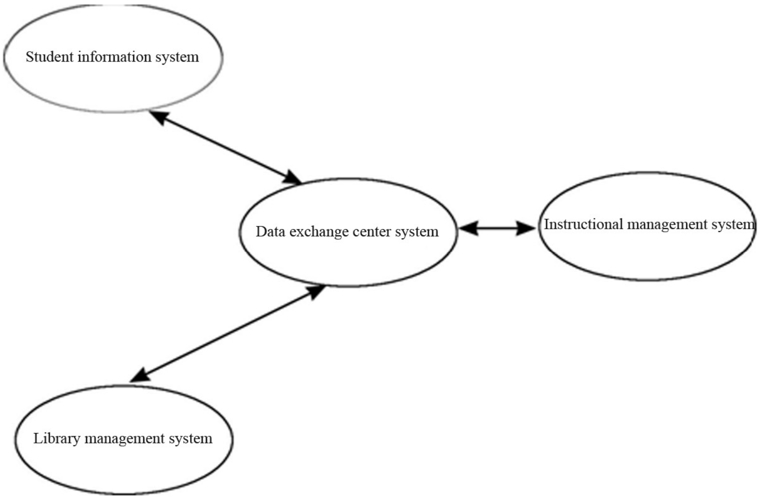
Student information system
Data exchange center system
Instructional management system
Library management system

Fig. 1. The network architecture diagram in the university

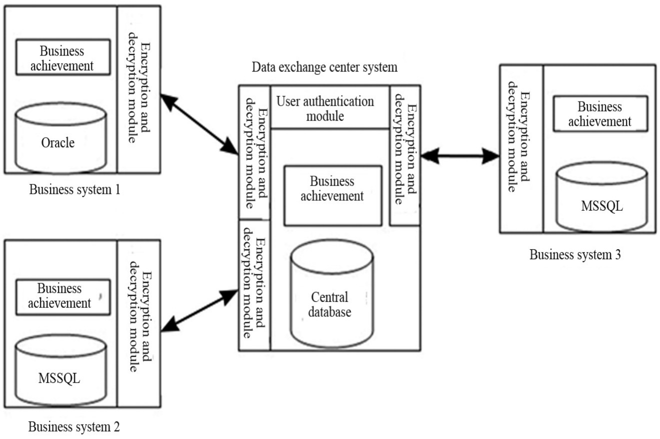
Business achievement
Oracle
Encryption and decryption module
Business system 1
Data exchange center system
User authentication module
Encryption and decryption module
Business achievement
Encryption and decryption module
Encryption and decryption module
Central database
Business achievement
MSSQL
Encryption and decryption module
Business system 2
Encryption and decryption module
Business achievement
MSSQL
Business system 3

Fig. 2. A schematic diagram of university network security

III. RESEARCH AND IMPLEMENTATION OF USER AUTHENTICATION

User authentication process is that the user submits a user name and password in login window, the information will be transferred to user authentication module in the data exchange center system across the network, the incoming information will be compared with the information stored in the database based on the encryption and decryption algorithms in this module, according to the compared result to decide whether to allow the user to enter the system.

User authentication information is stored in a central database in the data exchange center system. Data tables associated with user authentication in the database are: user authentication table, current user table and user information table. User authentication table contains four fields: user ID, encryption seed, summary of key information, last login time. Current user table holds the current online users, including user ID and login time. The user information table saves some basic information of the user, such as user name, age, gender, email, registration time. The table structure is as follows.

Table 1. User authentication table

Column	Data format	Length
UID	Int	8
PwdSeed	char	16
Hash	char	64
LastTime	Date	16

Table 2. Current user table

Column	Data format	Length
UID	Int	8
LoginTime	Date	16

Table 3. User information table

Column	Data format	Length
UID	Int	8

Published by Atlantis Press, Paris, France.
© the authors, 2013

Name	Char	64
Age	Int	4
Sex	Char	2
Email	Char	64
Time	Date	16

If the user's password is directly stored in the database, when the user information in authentication table is leaked, the intruder can easily access all users' login password, so it is needed for password encryption.

When the user is first register, the user will pass the user name and password to the user registration module, user ID will first be checked to determine whether there is duplication. If there is duplicate user ID, then corresponding information is returned to the user, the registration is failed, user should be re-register; if not repeated, the registration module calls random algorithm to generate a random encryption seed string, then assembles the user's password and encryption seeds into a new string, uses the MD5 algorithm to encrypt this string and generate summary of key information. Then, the user ID, encryption seeds and summary of key information are stored in the database.

Meanwhile, some basic information is required to fill out for users, the information will be stored in the user information table to find some information of registered users, when information related to users is changed in the information system, you can e-mail to notify the user and realize real-time and efficient office.

MD5 algorithm is widely used in the computer field, which is a hash encryption algorithm to provide information security and integrity protection. Through the MD5 encryption algorithm, the system could determine the legitimacy of user identity without known the user's origin password. This prevents the user's password known by the administrator and other special rights of people. MD5 could covert string of arbitrary length into a 128-byte integer, and by the 128-byte integer is very difficult to launch the original string. From the mathematical principle that is because the original string has an infinite number, this is a bit like there is no inverse function of mathematical functions.

When a registered user next logs system, the system will first search user ID in the user authentication table, find the appropriate user ID, get the encryption seed to generate the original string with the user information together. The string will be encrypted by the MD5 algorithm to get the user password, then compared with the string in the user authentication table, If consistent, then that is a legitimate user, allows users to log in; and if not, the user has passed the wrong password, requires users to log in again.

When a user successfully logs into the system, it will update the user authentication table LastTime, which is the last successful login time, if in a short time, one user often tries to login, you can judge that someone maliciously breaks the user's password, and refuse to sign in again. After a user successfully logs into the system, the user will be filled in the current user table and the current online users is calculated, when reached the large number of online users, you can deny other users continue to log in, to reduce the operation burden of the system.

IV. THE RESEARCH AND IMPLEMENTATION OF TRANSMISSION INFORMATION SECURITY

Between the data exchange center system and business systems, it is necessary to encrypt transmission XML messages to prevent information from being intercepted and stolen. Figure 3 is the encryption process of information transmission.

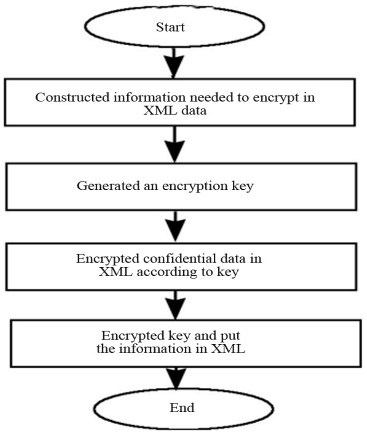
Start
Constructed information needed to encrypt in XML data
Generated an encryption key
Encrypted confidential data in XML according to key
Encrypted key and put the information in XML
End

Fig. 3. The encryption process of information transmission

First, the important information in XML is determined, and then a key is generated, such information is encrypted, the data is encrypted and re-construct to XML messages, and then the message is sent to the message receiver. Key generation uses a randomly generated way to ensure that each encryption and decryption keys are different, in order to increase the difficulty of cracking information.

The following is an unencrypted XML message that is the student's payment information. It includes student's name, payment amount, payment currency, payment bank card account, bank, payment date, non-payment of the amount of money.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
  <PaymentInfo>
  <element1>
    <Name>Chen Ming</Name>
    <CreditCard Value="2000" Curreney="RMB">
          <CardID>3895793250559083503</CardID>
          <Bank>ABCBank</Bank>
          <ExPiration>01/12/2011</ExPiration>
          <Remain>26539</Remain>
    </CreditCard>
  </element1>
  </PaymentInfo>
```

The CreditCard element is encrypted, only the user name is displayed, and some other sensitive information is encrypted, the XML data as follows is generated:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
  <PaymentInfo>
  <element1>
    <Name>Chen Ming</Name>
    <CiPherData>
```

© the authors, 2013

```
<CiPherValue>sdjflsdfkdsjgflkgj348574936549rijgo4943u
9gjr04tj04t

r459c65u868uxudr44tgriuretjfggfgrer4359rt94u</CiPherVa
lue>
      </CiPherData>
    </element1>
    </PaymentInfo>
```

When this XML information is transmitted to the other side, it will extract the decryption key, the decryption key and the encrypted message together is passed to the appropriate decryption algorithm to restore the original XML message, then the valid XML information is extracted.

V. CONCLUSION

With the development of networks, information systems must ensure transmission security for all important information. Network security technology has become difficult and hot to research in information system. In this paper, network information system for colleges and universities is studied, several possible security technologies are focused on, and are demonstrated feasibility in the university information system, a specific implementation is made. It has some theoretical significance and practical value for information security.

REFERENCES

[1] Richards K. Network based intrusion detection: a review of technologies .Computer &Security, 1999,188, 18(8): 671-682

[2] Schneier B. Managed Security Monitoring: Network Security for the 21st Century .Computer & Security, 2001,206, 20(6) :491-503 .

[3] James Goodwill. Mastering Jakarta Struts. Willey Publishing，2002

[4] W. Timothy Coombs. Ongoing Crisis Communication Planning, Managing and Responding London: Sage Publieations Ine. ,1999.

[5] Liu Dongping, Chen Li,ChenRui, JinJie. Design and Implementation of technology Data sharing platform with Web services [J]. ISBIM 2010(451).