Research on Database Security of E-Commerce Based on Hybrid Encryption

Jinbiao Hou
Department of Computer Science and Technology, Dezhou University, Dezhou, China
Email: houjinb@126.com

Abstract—Data in a database of e-commerce are very important. We must assure their security completely. Through the analysis on the process of users’ registration and retrieving password, the security problems existing in databases of traditional e-commerce are explained. Then it points out that it is difficult to ensure the security of the e-commerce system by using a single encryption technology. On the basis the technologies of symmetrical encryption and asymmetrical encryption are introduced. And then the hybrid encryption thoughts of combining the both are put forward. By using the method to improve the e-commerce process, the security of databases of e-commerce is enhanced.

Index Terms—e-commerce; database security; hybrid encryption; symmetric encryption; asymmetric encryption

I. INTRODUCTION

Security issues are an important topic in e-commerce. How to protect the security of an e-commerce system and data is its core research area [1]. There are many sensitive financial data and asset data in e-commerce databases, such as transaction records, commercial transactions, user account, market scheme and so on. The data are very important to the parties involved in e-commerce, so we must assure their security completely. At present the security technologies used in e-commerce databases are Web access control, user authentication, authorization control, safety audit, backup and recovery, data encryption and so on. These technologies can assure general database security, but it is difficult to assure their security for important databases. Encryption technology is one of the most effective technology of database security. However a simple encryption technology, such as symmetrical encryption or asymmetrical encryption, is very difficult to guarantee the security of network databases. We must combine the both and through hybrid encryption we can create a safe, efficient e-commerce database system.

II. SECURITY ISSUES IN E-COMMERCE DATABASES

An e-commerce system is a trading platform which sets up in a more open network environment. The transaction process is broadly divided into user registration, user login, purchasing merchandise, online payment and so on. When user information is transmitted in the web it may be stolen by hackers or other people with ulterior motives and will result in property loss. Therefore ensuring the security and integrity of basic information of users is the basis for the smooth conduct of e-commerce.

Next we take the most common mode of B2C e-commerce as an example and analyze security vulnerabilities in e-commerce databases that may exist. Figure 1 is the flow chart of user registration in a common B2C e-commerce system. Figure 2 is a common flow chart of a user to recover a password.

From Figure 1 we can see that, in the process that users submit it to the database server after they complete the information, password is encrypted and that it may be safe. However the question and the answer used to recover the password are not encrypted. If other people have stolen password hint questions and answers they will be able to obtain the password information of users in accordance with the flow in Figure 2 and also can change the password. It may result in loss of users and also can bring security problems to the system.

Through analysis we can discover that illegally stealing user information mainly occurs in the process that users enter complete information and submit it to a server. The main reason is that passwords can not be
reversed after they are encrypted by hash functions. They can be retrieved only with the password hint questions and answers which are filled in when users register. This link is not encrypted and others can easily eavesdrop the information from the Internet. This will lead to insecurity of database systems. In order to solve the problem this paper uses hybrid encryption technology, uses symmetric keys to encrypt user passwords, uses asymmetric key mechanism to transmit symmetric keys again, so that unauthorized users can not access users’ password information and it can enhance system security.

III. HYBRID ENCRYPTION TECHNOLOGY

A. Symmetric Encryption Technology

Figure 3 is a schematic diagram of symmetric encryption. When sending information, it will be encrypted through certain algorithms and keys and the original information will be changed into ciphertext. When receiving information, it will be decrypted with the same algorithms and keys and ciphertext will be restored.

At present the most widely used symmetric encryption algorithm is DES (Data Encryption Standard) algorithm proposed by the IBM company [2,3]. DES is a binary data encryption algorithms. Data packet length is 64 bits. Key length is also 64 bits. Eight bits in them are used for parity and effective key length is 56 bits. The basic process is as follows.

1) Initial permutation: Replace the location of ciphertext of 64 bits and get an out-of-order explicit group of 64 bits. It is divided into two paragraphs of 32 bits. L0 and R0 are respectively used to express.

2) Execute the following iterative transformation to L0 and R0:

\[ L_i = R_{i-1} \]

\[ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad i=1,2,\ldots,16 \]

3) Two parts output after the 16th transform exchange order, do inverse initial permutation and then ciphertext will result.

The advantages of symmetric encryption are fast speed, high efficiency. It is widely used in encryption of large amount of data. The disadvantages are that keys are easily intercepted when they are transmitted on the network. That will pose a threat to information security. Therefore when using symmetric encryption the security of key transmission need be guaranteed.

B. Asymmetric Encryption Technology

Figure 4 is a schematic diagram of asymmetric encryption. From it we can see that in the asymmetric encryption technology key is decomposed into a pair (private key and public key). Thereinto private key belongs to the owner of key pair and others do not know. Public key is open and everyone can know. Information encrypted by public key can be decrypted only by the corresponding private key. Information encrypted by private key can be decrypted only by the corresponding public key.

Typical asymmetric encryption algorithm is the RSA algorithm [4]. The algorithm is proposed by R. Rivest, A. Shamir and L. Adleman from the Massachusetts Institute of Technology. It builds on the basis of the theories of decomposition of large numbers and detection of prime numbers. The following is the description of the algorithm.

1) Select confidential large numbers p and q.

2) Calculate \( n = p \times q \), \( \phi(n) = (p-1) \times (q-1) \). Thereinto \( \phi(n) \) is Euler function value of n.

Figure 4. The schematic diagram of asymmetric encryption
3) Select an integer \( e \), satisfy \( 1 < e < \phi(n) \) and \( e \) and \( \phi(n) \) are coprime.

4) Solve equation \( d \cdot e = 1 \mod \phi(n) \) and calculate \( d \).

Based on the above steps, obtain public key \( \{e, n\} \) and private key \( \{d, n\} \). Thereinto \( e \) is encryption index and \( d \) is decryption index.

**Group every text, value is \( m \). Require \( m \) less than \( n \).** Encryption and decryption operations are as follows.

**Encryption:** \( c = m^e \mod n \)

**Decryption:** \( m = c^d \mod n \)

The advantage of asymmetric encryption technology is ease of key management. Disadvantages are the complexity of encryption algorithm and slow encryption.

It does not apply to the encryption environment of large amount of data. Therefore in data transmission using symmetric encryption technology to encrypt data can be considered first and using asymmetric encryption technology to transmit symmetric encryption key second. Thus both strengths of each other can be exerted.

**C. Hybrid Encryption Technology**

Through fully considering the strengths and weaknesses of symmetric encryption and asymmetric encryption we can combine the two and realize hybrid encryption [5]. Figure 5 is a schematic diagram of an asymmetric encryption.

**A:** Use symmetric encryption algorithm to encrypt text. In order to guarantee transmission security of symmetric key use public key of \( B \) to encrypt symmetric key. This can ensure that only \( B \) correctly knows symmetric key. Even if others have get key ciphertext they can not decrypt.

**B:** First of all use its own private key to decrypt key ciphertext and get symmetric key which encrypts documents. Using the symmetric key can unite ciphertext. Finally get the original information.

We can see that hybrid encryption technology overcomes not only the difficulties that symmetric encryption transmits keys but also the disadvantage that asymmetric encryption does not apply to large amount of data. The advantages of both can be fully integrated.

![Figure 5. The schematic diagram of hybrid encryption](image)

![Figure 6. The improved user registration flow chart](image)

![Figure 7. The improved flow chart of a user to recover a password](image)
IV. THE APPLICATION OF HYBRID ENCRYPTION IN E-COMMERCE DATABASE SECURITY

For security issues existing in Figure 1 and Figure 2, hybrid encryption technology is used to improve. The improved user registration flow chart and the improved flow chart of a user to recover a password are respectively shown in Figure 6 and Figure 7.

From Figure 6 we can see that in the improved user registration flow the password hint question and answer need not be filled out but submit the password encrypted by the symmetric key $K_1$ to the server. And the symmetric key $K_1$ is encrypted by the recipient’s public key $K_2$. In this way even if others have stolen the encrypted symmetric key they can not decrypt (because the private key is known only by the recipient). This makes the users’ password transmission become safe.

After the registration flow is improved user login steps become: (1) Users enter a website, fill out the username, password and the symmetric key $K_1$; (2) The client uses $K_1$ to encrypt the password; (3) Submit the password encrypted by $K_1$ to the server; (4) Based on the username the server queries the password encrypted by $K_1$ when users register; (5) Judge whether the two encrypted passwords are same. If they are same users successfully log on, otherwise they exit.

By Figure 7 we can see that after being improved the rules of users to retrieve passwords are as follows: Judge whether the public key $K_2$ submitted by clients and the passwords encrypted by $K_1$ are the same with the database; If they are same encrypted passwords will be sent back to the client; Users decrypt with the symmetric key $K_1$ and will get initial registered passwords.

V. CONCLUSION

Using hybrid encryption technology can give full play to the respective advantages of two kinds of encryption algorithm and provides more reliable and efficient security for e-commerce systems. The hybrid encryption technology used in the paper can also be used to enhance the security of other network databases.

REFERENCES