**MENMORANDUM**

DATA: June 7, 2015

To: Staff worked in BUPT and all the students who are going to have this class

FROM: The teacher of Product Development

SUBJECT: The arrangement about Product Development

**INTRODUCTION SUMMARY：**

The electronic commerce information security problems. Due to the openness of the system itself, make the electronic commerce system is facing all kinds of security threats. Hidden trouble in security at present, the electronic commerce mainly have the following several aspects.

**The problem of identity pretend to be attacker**

Piggybacking on legitimate user identity information through illegal means, counterfeit legal user's identity to trade with others, information fraud and corruption, in order to gain illegal benefits. Main performance: pretend to be others identity; Pretend to be others consumption, plant; Pretend to be legitimate host spoofing and legitimate users, etc.

**The network information security problems**

Mainly on the transmission channel of the attacker in the network, by means of a physical or logical, information interception, tampering, delete, insert. Intercepted, the attacker may through the analysis of the various characteristics of network physical line transmission, intercepted confidential information or useful information, such as consumer account, password, etc. Tampered with, that is, change the order of the flow of information, the content of the changes to the information; Delete, delete some information or some part of namely; Insert, insert some information in the information, make the transmitter read don't understand or accept wrong information.

**The problem of denial of service**

The attacker make legitimate access to information, business, or other resources .Main show is the spread of false information, disturb the normal channels of information. Including: falsely making out site and shop, send emails to users, collect orders; Forged a large number of users, E-mail, end business resources, make the legal users can't normal access to network resources, make a strict time requirements of service can not be answered in a timely manner.

**The problem of denial**

Some users may to malicious denial of their message, to shirk their responsibilities. Such as: the publisher later denied ever send certain information or content; Recipient later denied once received certain information or content; Buyers purchase order not admit; Merchants sell goods of poor quality but not admit that the original transaction. In the network world who as a trade dispute between the two sides for notarization and arbitration.

**The problem of computer system security.**

Computer systems for electronic commerce is the basic equipment, if you don't pay attention to safety problems, it will threaten the information security of electronic commerce. Computer equipment itself exists physical damage, loss of data, information and other issues. Computer systems are also often suffer the illegal invasion and destruction of the computer virus attack. At the same time, the problems of personnel management computer system, if the responsibility is not clear, competence unknown will also affect the safety of the computer system.

E-commerce security technology including backup technology, password technology, authentication and access control technology, etc.1. Backup technology. The so-called database backup and recovery plan, the purpose is in the database system failure and in a short period of time is difficult to restore, the database with data stored in the backup media restore to backup state. Data backup according to different types of database management system, there are multiple backup implementation plan. For used, for example, a database backup, the transaction log backup, incremental backup and file and file group backup. Electronic commerce information system database management system must be established in the backup and recovery strategy in detail. Can put the e-commerce database failures or obstacle is divided into the following three categories: system failure, transaction failure and media failure. When some type of failure, in order to reduce the enterprise's losses to a minimum, must be in the shortest possible time to restore data, therefore, according to the actual situation of enterprises and data types and features, set a reasonable and economic backup and recovery strategy is necessary.

**Authentication technology**

Authentication technology can prevent has system authorized users illegally destroy sensitive confidential data, a database management system to prevent all kinds of counterfeit attack security policy. Password identification is a method of database management system for identity authentication, each specific user is allocated a fixed system user name and password, many data of e-commerce system has the characteristics of openness, therefore must access to each user's identity authentication system. When the user access to sensitive key data, must be conducted between the client and the database management system authentication.

**Access control technology**

There are three kinds of access control scheme, named independent access control (DAC), mandatory access control (MAC) and role-based access control (RBAC).When a user to access the database, the system will be based on user level and authority to determine whether the operation is allowed or forbidden, so as to protect sensitive data from leaking or tampered with purpose. In a database management system, different users have different permissions. So must ensure that a user can only access or appropriate data access with their permission scope. Users have access includes two aspects of content: one is what kind of data objects, the user can access the database is the user can be what kind of operation of the data object.4. Audit technology. This effective mechanism can be in the largest extent, guarantee the information security of the database management system. There are two kinds of audit mode: the user audit and audit system. Users to enable auditing will record each user action in the data dictionary database of all details, including the user name, operation type and so on; And system audit is conducted by the DBA. Audit technology is a database management system to monitor all of the user's operation process related to a security scheme, the security scheme in audit logging is the specific method for each user actions on the database, including user modify, delete and query operations.

**Encryption technology**

Database management system of encryption in fields as the smallest unit, encryption and decryption is usually through symmetric encryption mechanism is the key to implementation. Data encryption, database management system to clear data after converting key cipher text data, the data in the database are cipher text data storage state, in the permission of the user query, then remove and decrypting cipher text data, to restore clear data. A further boost to the security of the database .E-commerce system of ordinary users is not allowed in some commercial confidential data on random access. Encryption scheme is the purpose of controlling these confidential data can only be accessed by a specific people get corresponding authorized and access.

**Encryption technology**

Encryption to protect sensitive information transmission, to ensure the confidentiality of information. In an encryption system, information encrypted using encryption key, get the cipher text to transmitter and receiver use the decryption key to decrypt the cipher text to get the original. At present there are mainly two kinds of encryption methods: secret key encryption and public key encryption.

**Digital envelope**

Digital envelopes technology is combined with the advantages of secret key encryption and public key encryption technology of a kind of encryption, it overcomes the secret key distribution of difficulties in the secret key encryption and public key encryption in the encryption time problem, using two layers of encryption to gain the flexibility of technology of public key and secret key technology of high efficiency.2.3 the digital signature .Digital signature is used to ensure the information transmission in the process of information complete and provide the sender's identity certification. Use of public key algorithm is the main technology to realize digital signature, in addition, the double digital signature is to make sure the three parties in the process of electronic trading safely transmission technology.

**Authentication technology**

Authentication technology is one of the important safety technology in electronic commerce. Certification is divided into entity authentication and information authentication. The entity here refers to the individual, the client program or service such as communicating entities. Entity authentication refers to those involved in communications of an entity authentication. Authentication information refers to information authentication, to determine the legality of the information. Authentication information in the recipient receives the information, used the related technology information authentication, who is to confirm the sender information, whether the information in the process of transmission is modified, replacement, etc.

**E-commerce security SET protocol**

lSET (Secure Electronic Transaction) is in an open network (Internet or public multimedia network) to use the payment card (credit card, debit card and debit card, etc.) to pay the safety of the Transaction agreement. The agreement is led by two Visa and MasterCard credit card organization, united the GET, IBM, Microsoft, RSA and VeriS - ign big company development together. Realization of the SET protocol does not need to pay network for existing bank big reform. With the rapid development of Internet and World Wide Web, online e-commerce is growing rapidly .In real life, electronic money (credit card, debit card and debit card, etc.) the use of more and more popular, many Banks plans on the Internet to provide direct payment card certification .These factors contributed to the generation of the SET. The purpose of the SET is to safely use the payment card transactions on the Internet. So SET made the confidentiality of sensitive information, the integrity of the payment, the merchants and cardholders and the identity authentication of recipient bank safety technical requirements.