

# Briefly Talking about the Present Situation, Elements and Countermeasures of E-commerce Safety in China

Guopei Pan

Jiangxi Institute of Fashion Technology  
Nanchang, Jiangxi, China

**Abstract**—By analyzing current situation, causes of E-commerce safety problems and E-commercial demands on safe environment, the paper puts forward the safe and preventive countermeasures of E-commerce, makes further statements and analysis on the main problem solutions of E-commerce safety and provides technical references, so as to establish and complete E-commerce safety system.

**Keywords**—E-commerce Present Situation Element Safety Technology; Safety Agreement

## I. INTRODUCTION

The development of E-commerce has pushed business enterprises across the world into the spring tides of commercial revolution, in which safety is the key. E-commerce system is a sort of comprehensive transaction system involved in information, funds and materials deal on the Internet, whose safe structure is an open complicated system closely coupled with social system in which people frequently do businesses. It is made of commercial organization on its own (including marketing system, paying system and distributing system and the like) combined with information & technology system. The system's safety target and scheme depends on the characteristics and demands of the organization.

## II. THE PRESENT SITUATION OF E-COMMERCE SAFETY

### A. The Emergence of E-commerce Safety Issue

1) *The safety issues brought forth by the virtualization of on-line dealer*: Under the environment of E-commerce, any people can send or receive network information by a computer network without registration, and conclude the transaction with others through a certain program. The existence of virtual dealers makes E-commerce transaction safety severely threatened.

2) *The safety issues brought forth by the release of false messages*: The sellers and buyers can both release false the messages concerned with supply and demand, or pretend to be nowadays messages with overdue messages so as to gain by cheating others' money or goods, when users enter the system with legal identity.

3) *The safety issues brought forth by too low credit degree*:

a) *The safety issues brought forth by the buyers with low credit degree*: The buyers with too low credit degree may probably overdraw spitefully or use forged credit cards to gain

by cheating the sellers' goods, or delay payment, so the sellers need to take a risk for this.

b) *The safety issues brought forth by the sellers with low credit degree*: Sellers can't deliver the goods purchased by consumers on time by quality and quantity, or fully fulfill their engagements signed with group buyers so as to cause the buyers' risks.

c) *Both the buyers and sellers with low credit degree have phenomena of disavowal*.

d) *The safety issues brought forth by the existence of network cheating*: Frequently cheating users is often used by network swindlers in electric transaction activities. Applying E-commerce to cheating has become a new type of crime activity. Nowadays, such network cheating has also become an international difficult problem to solve.

e) *The safety issues brought forth by the process of replacing paper contracts with electric contracts*: Under the condition of on-line transaction, all the messages of two parties' transaction are stored in computer hard disks or other electric media in an electric form. These records can not only be erased, deleted, copied, and lost easily, but also be impossible to exist independently as evidence when separated from recording tools (computers), from which safety issues related to many respects can arise.

f) *The safety issues brought forth by on-line electric payment*: On-line payment of E-commerce is completed by a credit card or electric fund transference on a virtual bank. The realization of such a process is involved in the agreement of between Internet bank and Internet customer, cooperative agreement of between Internet bank and Internet web and other issues about safety guarantee.

g) *The safety issues brought forth by the process of products' delivery*: Some special problems of visible goods caused in logistics dispatching link during on-line transaction and some safety issues brought forth by the transference of right, return of goods and the fulfillment of payment in the process of the payment of invisible information products.

h) *The safety issues brought forth by protection of rights of net consumers*: The virtualization and openness of on-line market and the convenience of net purchases make the protection of consumers become an obvious issue on quality, return, and complaint and repair and so on.

i) *The safety issues brought forth by the act of sabotage conducted by vicious net attackers:* It includes system penetration, the breach of authorization principles, implanting, monitoring communications, interfering communications, interruption, refusing services, denying and so on.

j) *Fishing web site:* Nowadays it mainly registered as fake bank web site, ticket booking web site which cheat users not to use the third platform to directly transfer money to result in the users' loss.

#### B. E-commercial Demands on Safety Environment

1) *Ensure the safety demands of information including validity, confidentiality, completeness, dependability, undeniableness and differentiation and so on.*

2) *Ensure the validity of authorization.*

3) *Ensure the certainty of dealers' identity.*

4) *Ensure the tightness of internal web site.*

### III. THE ELEMENTS OF E-COMMERCE SAFETY

#### A. The Security of Information

It refers to that information cannot be stolen in the process of transmission or storage.

#### B. The Integrity of Information

Its mistakes of information about trading probably arise owing to the unexpected errors of data input or the act of cheating.

#### C. The Validity of Information

Since E-commerce replaces paper files with electric files, how to ensure the validity of trade information in electric form is the prerequisite of conducting E-commerce activities.

#### D. The Undeniableness of Information

It demands that the individuals, enterprises or countries participating in deals should supply reliable logos in the process of transmitting dealing information so that sending data for senders or receiving data for receivers are undeniable.

#### E. The Realness of deal Identity

It refers to the two parties of trading are indeed existent, not fake.

#### F. The Reliability of System

E-commerce system is equal to computer system, whose reliability means that the safety and reliability of system operation must be guaranteed through preventing computers from failure, program errors, transmission mistakes, hardware breakdown, system software making errors, computer viruses, natural damages and other hidden threats

### IV. SAFETY AND PREVENTION SCHEMES OF E-COMMERCE

Safety and Prevention Schemes of E-commerce have developed into integrity, usability, controllability, and undeniability of business information, and further into the basic theory and operation technology concerned with many respects such as "attack, defense, measurement, control, domination, evaluation and so on" from the earliest confidentiality of business information through decade's exploration. Nowadays,

in the field of E-commerce safety there have been 9 great key technologies such as coding technology, identity check technology, visit control technology, firewall technology, safety kernel technology, network anti-virus technology, information disclosure prevention technology, network safety leak scanning technology, and invasion check technology.

#### A. Main Safety Technology of E-commerce

1) *Coding technology:* Coding technology solved the problem of information-sending confidentiality, which includes symmetrical coding and asymmetrical coding. Symmetrical coding is a traditional method of identifying information. Two sides of exchanging information commonly agree on a password or a great of secret code to establish a key to the secret code them can share. Communication Side A will send the messages coded in a private key to Side B, meanwhile Side B will get the messages sent by Side A after decoding with the same private key with Side A. Symmetrical coding mainly adopts such coding algorithm standards as DES data coding standard, three multiple DES, IDEA and AES (high-level coding algorithm) and so on. Its maximum advantages are to rapidly code or decode, suitable for coding a great number of data, but the key to code is difficult to control. Asymmetrical coding is also called coding with open key to code. It uses an open released key to code and a private key to code controlled by the trader who made the key to separately conduct coding and decoding operation. For instance, Trader A makes a pair of key to code and gives one of them to the other trader as an open code key. And Trader B, after getting the open key, sends information coded by the key to Trader A. Trader A again uses another private code key to decode messages. Coding technology with an open code key is the core of coding technology, which mainly adopts RSA algorithm, DSS/DSA algorithm and ECC algorithm, whose advantages are to operate conveniently, but coding and decoding are slow.

2) *Digital signature:* Digital signature solved the problem of preventing others from breaking sent documents and how to identify the sender's identity. Digital signature has the same effect with written signature on document, which stands for the features of document. If documents change, the value of digital signature also changes with it. Different documents will get different digital signature. Digital signature uses the double coding method to join in workflow:

- The sent document is coded with SHA code to form a digital abstract of 128 bit.
- The sender again codes the abstract with a private code key to form digital signature.
- Original document and the coded abstract are simultaneously sent to counterpart.
- The counterpart decodes the abstract with the sender's open code key and simultaneously codes the received document with SHA code to form another abstract.
- The decoded abstract is compared with the formed one through recoding by the receiver after receiving

documents. Finally, anti-fakery and anti-denial ability are realized.

3) *Digital time stamp*: Digital time stamp service, supplied by a special organism, provides safety and protection of electric files. Digital time stamp is a credential file formed by coding, including three parts such as the document abstract which need to be add a time stamp, the date and time when DTS receives the document, digital signature of DTS. The forming workflow of time stamp is as follows:

- The user code the document to be added a time stamp with HASH code to form an abstract, and then send the abstract to DTS.
- DTS, after receiving the messages about the date and time of the document abstract, code the document (digital signature), and then return it to the user. Digital time stamp is added to by certification unit DTS, based on the time when DTS receive the document.

4) *Digital certificate*: Digital certificate is issued by CA authentication center, a voucher of verifying an user's identity and visit right to network resources in an electric form. CA authentication center is a service organization, which can take on the service of safe on-line electric deal authentication, issue digital certificate and very users' identity. Digital certificate provided authentic, reliably confirmed public service, solved the problem about the identity, credit confirmation, maintaining the safety of deal activities of deal participants concerned in the E-commerce activity, guaranteed the smooth operation of E-commerce deal activity fundamentally. In on-line electric deal, the two sides can carry out safely deal operation with their own shown digital certificates.

5) *Firewall technology*: As the first safe barrier shield to outer network from inner network, network firewall technology is foremost paid much attention to. It can prevent from illegally visiting information resources, can also prevent patent information from illegally outputting from enterprise's network by using firewall, which is the most suitable for a single and comparatively independent network that has limit channels to outer network and centralized network service kinds. Firewall has two basic principles: one is that not be allowed is prohibited; another is that not to be prohibited is allowed. Based on the principles, firewall should transmit all the information flow, and then item by item shield probably harmful service. By this method was formed a more convenient application environment and can be provided more services for users.

#### B. Safety Agreement Technology of E-commerce

1) *Safety agreement technology of E-commerce is mainly composed of SSL agreement and SET agreement as well as PCT which only a little reformed SSL*: SSL agreement, including "SSL recording agreement" and "SSL hands shaking agreement", provides the application program based on TCP/IP client/server with secure measures concerned with confirmation, data integrity and information confidentiality of client/server. The agreement implements the investigation into

secure features concerned through exchanging SSL initial hands-shaking agreement before the application program carrying out data exchange. In SSL hands-shaking information are adopted DES, MDS and so on coding technology to realize confidentiality and data completeness, and the digital certificate of X 509 to conduct verification. SSL agreement has been widely used as a de facto standard. The mode of "SSL+sheet signature" is also adopted to make SSL further improve the secure guarantee of E-commerce on the basis of ensuring authenticity, integrity and confidentiality of information in the process of application of E-commerce.

2) *SET agreement is a type of secure electronic payment agreement based on credit card and jointly developed by Mastercard company and Visa company, which is applicable in the Internet environmen*: It can authenticate all parties of the transaction, prevent traders from cheating, and make transaction safe. It gave a set of standard electronic deal process which is at present publicly regarded as an international standard of on-line credit transaction.

3) *Constructing a frame of E-commerce secure control and formulating criterion, law and regulation on E-commerce*: It is helpful for solving security and reliability of E-commerce through secure control and execution of E-commerce criterion. It is immeasurable that E-commerce bring interests to enterprises, consumers and society. Especially, E-commerce will definitely become a newly emerging business operation mode, push ahead the rapid development of global economy by its high efficiency and low cost. However, the security of commercial information is all the time the key of E-commerce, which has become the most serious problem of hindering the wide application of E-commerce. The problem can be solved through synthetically applying all types of E-commerce safety technology to make them increasingly improve and perfect, establishing and perfecting the secure mechanism and relevant regulations of E-commerce, and implementing international criterion of E-commerce.

4) *Enhancing self-awareness of safeguard and strengthening standard administration*: With the growth of economy, increasing development of information, information capacity can also continuously increase, which certainly including lots of fake and cheating messages. For this reason, it is demanded that people keep on enhancing self-awareness, ask more, compare more, understand more, and try to use the third party's platform when repaying is necessary. When shopping on line, one should have a good look at the credit information and deal records of company and individuals concerned, and try to avoid the occurring direct on-line payment. Meanwhile, our country should energetically take advantage of self-superiority, actively follow oversea advanced technology, set up a good environment supporting E-commerce, construct a complete set of matched facilities of E-commerce, and make an all-out attempt to propel enterprise information march ahead.

## V. CONCLUSION

It is necessary that we establish the awareness of safely prevention of E-commerce, be fully aware of the security problems brought by the development of E-commerce, and maintain the security environment of E-commerce. Further more, we also should attach importance to establishing a reliable commercial system and making safely and preventable measures of E-commerce, especially applying security technology to E-commerce.

## REFERENCES

- [1] *E-commerce New Angle of View of Administration* ( 2<sup>nd</sup> edition) [ M ].Compiled by (U.S.) Efreim Tebasdavid Kim Jim; Translated by Wang Liping and Zhang Xiaofeng. Electronic Industry Publishing House . 9, 2005
- [2] Yang Jianzheng Compilation: *E-commerce Basis and Application (the 5<sup>th</sup> edition)* [ M ]. Publishing House of Xian Electronic University of Science & Technology, 7, 2007
- [3] Gan Yue. *Briefly Discussing about the Construction of E-commerce Security System* [J]. *Northwestern Adult Education Journal*, 2007 (2).