A Critical Research on threats and security technology related to Payment System on E-commerce Network

Dhirendra Pandey
Dept of IT,
Babasaheb Bhimrao Ambedkar University

Dr. A.Rastogi
Department of CSIT
Guru Ghasi Das University

ABSTRACT

This paper is mainly concerned with the study in which how we can make our electronic transaction more safely and protective and also concerned with research of the security technology, key technology and current application protocol of payment transaction on network, and gives some useful suggestions and countermeasures for the development of protective payment transaction on network and safety E-business system. As we know network payment is a key button for understanding and perceptive of E-commerce, and safety electronic transaction is the base of bank's participating in E- commerce, so that this paper concentrates about safety analysis on payment system of e-commerce network

Keywords : Security Technology, E-Business, E-commerce.

1. INTRODUCTION

Electronic-commerce is also known as E-commerce, just as its name implies, the content of E-commerce contains two aspects, the first is by way of electronic, and the second is commercial activity. E-commerce means transaction on networks, such as on Internet or on public computer network, which offers a fast and effectively solution for realizing various kinds of business .E-commerce forms a high integrated new running method of business affairs like information query, substance transmit, financial balance and remote management by way of integrating application of computer inter linkage network and telecom facility. Payment on network is a critical important chain of whole E-commerce, for an intact business process always contains the payment activity. It is essential to ensure the safety of E-financing whether it is flowing on special usage network or on public Internet, it is applicable to reach this goal from point view of network technology by using the technology of safety control steps of transaction layer and application layer and the technology of firewall. Currently, though massive manpower and financing are injected into the research of ensuring the safety topic of payment on network and E-commerce, yet still many safety problems of financial transaction of E-commerce exist, which need to be improved by further research.

2. Safety difficulty of payment balance system of E-Commerce

A bank is a key component among the frame of EC system, and it is the prerequisite for EC to use the payment balance service of bank. As the largest customer of computer system, computer network and communication technology, the bank industry hopes to offer the E-finance service on network by way of actively utilizing the digital virtual information transaction technology. The public and open Internet provides a new and easy access for hackers to invade into the bank network system. It is even possible for network hackers to invade into the core business system of a bank, which may juggle or delete the important data and steal large amounts of bankroll, what is more serious is that the safety system of EC may be damaged intently, and the computer system of bank may be crashed. Thus problems concerning bank safety listed below remain to be solved:

(1) How to establish a safe and reliable computer network? The finance service of a bank is running without any break, the network compliant to payment system of EC network must be running 24 hours a day without any trouble. After the operational database system of bank is being connected to public network by way of WWW, it is essential for them to prevent themselves from being attacked maliciously.

(2) How to avoid the trading data of customer being wiretapped on its way of transmitting on Internet? When a customer trades on a network bank, some important data such as: cooperation account, payment code, individual credit card number, password, trade information may be wiretapped during the process of transmitting on network.

(3) How to prove the integrity of trading data. Bank must build a verification mechanism concerning trade data on network, to ensure the data received has not been falsified during transmitting.

(4) How to identify a legal customer? Banks need to construct a validating mechanism, which should provide a way to ensure the individual / enterprise who has made electrical orders or electrical cash transfer via Internet are valid, thus to prevent the behavior of forging and cronkness.

(5) Establish the standardized integrated E-payment system. It is essential for the electrical payment under public environment to have a standardized mode, which makes it possible to ensure the safety and keep interactive. Though some kinds of pen criterion of E-payments are under practice , such as the EMV96 (short for Europay Mondexcard and Visa) used in IC, SET in credit card, E-check in electric balance and Cyber cash Coin system in small quantum cash. But currently no uniform standard or protocol is established in public inter-linkage network aspect. Presently only one kind of protocol can be offered by most of the application systems, while the ability of various kinds of payment is still unreachable. It is necessary for EC to build a payment protocol of integrated

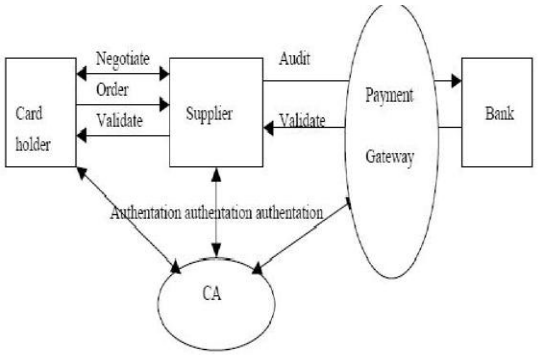

Fig1: Connection among components of e-commerce

3. Safety understanding of EC payment system

The safety of payment system is the key element of EC. Currently the key technology to ensure the safety of system is as follows: Security Socket Layer (SSL) and safety electronic transaction, which are mainly two kinds of important communication protocols, either of which can offer a method of reliable payment through internet. Several kinds of coding protocols are in use on Internet, every layer of the corresponding seven layers of the network modes has its relevant protocol. For instance, we have application layer of SET protocol, and session layer of SSL protocol. Among all the protocols, SSL and SET have the closest relation with EC.

3.1 Security Socket Layer protocol SSL

SSL is the protocol that encodes the whole session among computers and provides the safe communication service on Internet. It is widely used among sensitive information concerning capital balancing. Two kinds of coding are used in SSL: 1.Public coding key is used in process of connection 2. Special coding key is used in process of session. The type and intensification of encoding are different according to the declaration made during the process of connection of two ends. The server validates the customer computer's legality by way of: 1.Give a proven attest containing public code key 2. Demonstrate that it can decode the messages that are encoded by the public code key. 3. Customer computer can provide the attest, which can identify itself: the code key of session is conducted from the selective data of customer computer, the public keys of server 4 codes its data. Among each SSL session, it is required that the server fulfill one operation of code key and one operation of public code key of customer computer. 5. From view of method of coding, RSA coding method is widely used in all kinds of payment system, each operation need to fulfill the exponent operation under modulus arithmetic. Usually, decimal fraction is selected as the public exponent to cut the workload of operation. Thus one SSL session needs only one "hard" code operation. SSL provide the safe connection between two computers. The payment system is always constructed by way of transmitting credit card number through SSL connection; the bank of network and other financing payment system is constructed on SSL as well. Though the E-commerce development is accumulated by credit payment under base of SSL, yet more advanced technology of payment system should be adopted to make the E-commerce spread its area more broadly.

3.2 RSA arithmetic

3.2.1 The forming of code key

Selecting tow big prime number p and q, calculate: n = p * q

Then random selecting the coding code key e, requiring e and (p - 1) * (q - 1) mutual prime. Finally, calculate coding code key d by arithmetic of Euclid, to satisfy:

e * d = 1 (mod (p - 1) * (q - 1))

n and d need to be mutual prime as well,. e and n are the public key, d is the private key, the two prime number p and q are not needed anymore, and be cast off.

3.2.2 Encoding information and decoding action

While coding information m (binary system), m is divided into several data of equal length m1,. …m2mi, the block length is s, s <= n, s should be large as possible. The corresponding code message is;

Ci = mi^e (mod n) **(a)**
When the operation is done, decode:
mi = ci^d (mod n) **(b)**

At the same time, RSA can be used in digital signature; formula (a) is used for signature, and formula (b) is used for verification. Factors like safety and the large amount of information of m should be considered during practical operation, HASH operation is done firstly under general condition.

3.2.3 Secure preventive safety measures should be taken during RSA coding Arithmetic

(1) The safety of RSA depends on decomposing of large number, while on the other hand many large prime numbers (decimal system) can be decomposed presently. Thus, modulus n should adopt a large one to ensure the safety of system.

(2) To ensure the privacy of code message and to prevent the hacker from making the entity who own the private key to sign by blind information, we suggest the following: 1. Adopt good public key protocol, so as to ensure entity not decode information randomly produced by other entity, not to sign the information unknown to itself 2. Not sign the random documents sent by strangers, using One-Way Hash Function to documents before signing, or using different signing arithmetic at the same time.

(3) The number of the public modulus of RSA selected. It is dangerous if in a system only one modulus is shared together with different people having the different e and d; under most prevalent circumstances, a message is coded by different public key, if these public keys are share the same modulus and be prime with each other, then this information can be recovered without any private key. So, it is suggested not to share the modulus n together.

(4) It is essential for public key e and d to get a high value to prevent the public key from being decoded.

3.2.4 The main defects of RSA

- It takes time to create a code key; only one code can be made for one time because of the restriction of the technology of prime creation.

- The length of grouping is too long, to ensure its security, the n should be larger than 600 bits, thus cause the cost of operation very high, especially make the operation speed rather slow, down several times compare to coding arithmetic; while this length will be enlarged with the technology development of decomposing of large number, And this tendency will not be beneficial to the standardization of data format.

3.3 Secure Electronic Transaction SET

SET protocol aims to offer a solution for business by way of credit card payment among the customer, the supplier and the bank. Many parts are included in the SET, to meet the need of problem solving at different stage in business. SET was developed by international

organizations of Visa and MasterCard and now it has won support from many large internal companies like IBM, HP, Microsoft, Netscape, VeriFone, GTE, Terisa and VeriSign, etc., Thus it has become the industrial standard virtually, and gained the recognition of IETF standard. And SET aims to solve the safety problem in electronic payment of credit card:

(1) Ensure the confidentiality of information and avoid being wiretapped when information is transmitted on line. Only the authorized legal person can get and decode the information;

(2) Ensure the entity of payment information, secure the data transmitted can be received fully without any alteration in the middle way;

(3) Attest the supplier and the customer; verify the validity of supplier, card holder and business activity which do business on the public network;

(4) Secure wide mutual operationally, ensure the communication protocol, message formatting and standard being adopted have the common adaptability. Thus various products of different supplier can be integrated on public interlinking networks. SET protocol is more complex than SSL protocol, for by SET not only single session between two ends can be coded, but also multi-session among multi-ends can be coded and recognized. Three stages are included in the SET trade:

- In the inquiry stage, customer and supplier confirm the detailed information on the payment method;
- In the confirming stage of payment, the suppliers will confirm with the bank, they will get the payment as the trading proceeds;
- In the money-accepting stage, the suppliers will bring forth all the detailed information concerning all the relevant trading to the bank, and the bank will transfer the payment for goods in a proper way.
- A customer only has relation with the first stage, bank has relation with the second stage and third stage, while a supplier has relation with all the three stages, and every stage is involved in the data coding technology and digital signature by RSA.

SET made possible the work of information integration, verification of all financing data and coding of sensitive data. It realized the financing payment safety work of attesting cardholders, supplier, payment request, payment authorization and records of payment by use of advanced technology like data coding and digital signature. This standard meets the commercial demands in E-commerce activity specified as below:

- Safe transmitting of payment information and order information on internet, securing the data transmitted on network not be stolen by hacker;
- Separation of order information and personal account information, when the order containing the card holder's account information is sent to the supplier, only the order information can be seen by the supplier, while other account information of card holder can not be read;
- Mutual identification between the cardholder and the supplier, to make clear the identities of the two sides of communication; under most circumstances the trust guarantee on network is provided by the third party.

Currently, SET is widely applied as the public standard of safety payment of E-commerce. SET an enable the information of the cardholder to be reached, read and verified only by the bank, while supplier has the right to extend payment request and accept the payments.

3.4 Safety technology

E-commerce trade system needs to provide safe services for the E-commerce participants by use of safe technology. These services include the following:

There are service of identifying customer' identity, service of visit control, service of confidentiality, service of no denial. The main safe technologies in use in E-commerce include: coding, digital signature, E-certificate, E-tag, etc. After years of efforts an arithmetic method integrating the above technologies has been worked out by many research agencies and relevant software have been designed.

3.4.1 Electronic Tagging

Electronic tagging is a form of non-surreptitious surveillance consisting of an electronic device attached to a person or vehicle, especially certain criminals, allowing their whereabouts to be monitored. In general, devices locate themselves using GPS and report their position back to a control centre, e.g. via the Cellular phone network. This form of criminal sentencing is known under different names in different countries, In order to confirm the authenticity of the both parties of a trade on network, KDC offers electronic tags to do trading. Supposing A wants to do payment trading on network with B, then A should firstly communicate with KDC, and encode by using the code key known only to A and KDC, then A will tell KDC that he wants to communicate with B, KDC will randomly select a dialog code"*******" key for the trading between A and B, and then create a tag at the same time. The tag is coded by the code key between KDC and B. A will deliver this tag to B when A starts to trade with B. The function of the tag is to let A confirm the other party's real identity. For this tag is coded by the code key known only to B and KDC, thus even if the forger get the tag sent by A, he can not decode that message; only B can decode the message after he receives it, thus B is identified as the right person in dialogue with A.

3.4.2 Certificate Authority

Since E-commerce is running commerce activity by way of electronic or network, the parties involved cannot see each other face-to-face, thus it becomes crucial to validate personal identity and ensure communication safety. One solution is to establish a nonaligned, authoritative, candid E-commerce certificate center— a CA certificate center, to issue digital certificate for the individuals, enterprises and government organizations, a kind of ID card on network, to confirm each other's ID in E-commerce activities, and to achieve safe information exchange and safe trading on network by way of coding or decoding. The digital certificate is an electronic certificate based on safety standardization, protocol and coding technology, it is used to confirm the ID of an individual or a server; it can bind a pair of electronic code keys used for the message and the signature, and ensure that this pair of code keys really belongs to the

appointed individual or organization. Digital certification can be electronically published or cancelled by certificate authority—CA, the incept party of message can download the verification message of the sender party from the CA Web station. As the certificate center of E-commerce, CA center is the core of PKI system. It issues public code key certificates, manages certificates for the customers, and at the same time provides a series of management service in the life cycle of the code key. It associates the public code o and the name of an object and other attributes, thus providing sound safety for customers. It is therefore a third party agency of authority, reliability and notarization. It is the base of E-commerce. And it can identify the legality of the supplier, customer and business activity itself in electronic trading process.

3.4.3 Pretty Good Privacy coding PGP

PGP is coding software based on RSA public coding system. It can code toward the data flow to avoid illegal interception. It adopts technology listed below: prudent code key management, one kind of mixed arithmetic of RSA and traditional coding technology, mixed arithmetic of digest arithmetic using in digital signature, zipping before coding toward digital signature, the specialty of this technology lies in the high speed combination of easiness of RSA public key system and traditional coding system, and smart design in management mechanism of digital signature and coding key recognition. Thus the function is powerful, and the speed is fast.

4. CONCLUSION

E-commerce is the developing trend of the economic development of 21 century, among which financing industry plays a key role. Network payment relies on the establishment and completeness of electronic safe trading. Payment gateway is the medium of the connection between information networks and financing networks. They bear the payment information transfer of both parties. The establishment of payment system on network will be a long process, for it is closely related with much regulation of financing and law.

Only the network payment suitable for localization condition is fulfilled, can the payment problem be solved totally, can the E-commerce promoted entirely. EC has got a bright prospect, yet it is not easy to arrive at. A safe commerce environment will help broaden the E-commerce applications. With the establishment of State financing CA certificate center, and with the development of safety technology research, E-commerce activity of India is sure to develop in a fast and healthy way.

REFERENCES

[1] Abrams, M.D., Jajodia, S., Podell, H.J. (eds.). , *Information security: an integrated collection of essays*. IEEE Computer Society Press, 1995.

[2] Mortaza Bargh,, Wil Janssen & Alko Smi., *E-commerce, E-business and E-government* (I3E 2001)", pp. 45-58, October 3-5,2001

[3] Nabil, Adam R.; Yesha, Yelena (Eds.). E-commerce: current research issues and application. LNCS 1028, Springer, Heidelberg, 1996.

[4] S. Jones, M. Wilikens, Philip Morris and Marcelo Masera, 2000, *Trust requirements in E-commerce, a conceptual framework for understanding the needs and concerns of different stakeholders*, Communications of the ACM, December 2000, Vol. 43, No. 12.