International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.259-268
http://dx.doi.org/10.14257/ijsia.2013.7.6.26

Research on the Data and Transaction Security of Enterprise E-Commerce Countermeasure

Yongyong Zhu[1,2]

[1] *Civil and Commercial Law School, Southwest University of Political Science and Law, Chongqing 400031, China*
[2]*Department of economics and business administration, Chongqing University of Education, Chongqing 400067, China*
zhuyongyong@126.com

Abstract

In the process of transmitting Business E-commerce information, there are various risks that can put it at stake at any time. So in this article, for the purpose of ensuring the security of the devices, operating systems and data transaction, elaborate the security of Business E-commerce from the aspect of VLAN, application layer, session layer, dynamic password, symmetric key encryption and encryption of communication stack. In order to do that, we need to strengthen and improve education, publicity, and security awareness of enterprises; using multiple networks and cryptographic techniques to protect the security of information; strengthening risk analysis and prevention to reduce systemic risks; perfection of E-commerce legislation; using security strategies which protect the interests of both parties.

Keywords: *Enterprise E-commerce; Security System; Operating System; Secure Electronic Transaction; Security Strategies*

1. Introduction

Enterprise e-commerce refers to commercial trade activities – from the query and purchase of raw materials to the exhibition, purchase and manufacture, storage, transportation and e-payment of production – which are carried out via internet and information technologies [1~3]. Its purpose is to use network to establish internal management systems, solve problems, reduce cost, increase value and create new opportunities for commercial trades. Enterprise e-commerce has the characteristics of low transaction cost, fast transaction speed, interactive marketing channels and 24-hour network services, making e-commerce enterprises an improvement on traditional enterprises. Considering commercial activities as the core, computer network as the foundation and electronic techniques as the tool, e-commerce enterprises can fully take the advantage of electronic techniques and computer network to develop commercial activities under the scope of the law. Electronic commerce offers us interactive distribution channels. Such as use CRM platform and B2C platform more frequently which let the supplier participate in the commodity information inputting and after-sale service, and maximally ensure the suppliers' enthusiasm and the best decision of commodity and service, thereby advance the information feedback and sales performance [4].

ISSN: 1738-9976 IJSIA

2. Security of e-commerce

The carriers on which the enterprise e-commerce depends during it works mostly are internet platforms. During the process of information transfer, both secure and unsecure data are passing through, all kinds of risks thread e-commerce safety and enterprises take e-commerce information security more and more seriously [5~6]. The premise of information security is system safety. System safety includes the safety of network system, operating system and application system. The technologies used to make system safe always are network isolation, access control, authentication, data encryption, and monitoring and evaluation etc. As to the safety technology of e-commerce security system, we often control it by means of cipher graph, authentication technique, access control technology and firewall technology etc. Authentication technique of e-commerce is a process that the e-commerce users showing their identification to the system and being checked by the system. Authentication technique often combines access control technology, cipher graph and firewall technology. Firewall technologies are often divided into packet filtering, application proxy and circuit gateway. Access control technology includes the confirmation of strategy, model and mechanism, and it is always used in message authentication, identity authentication and e-signature.

3. Security system of enterprise e-commerce based on security strategies

3.1. Developing the education and training of e-commerce in enterprises to improve their security consciousness

Information security consciousness is an enterprise's awareness for the importance of information security and the combination of its sensitivity in discovering and impacting network security and its initiative in maintaining network security [10]. The cultivation of security consciousness is a long-term project. It takes a long time for both e-business employees and sellers to develop their security consciousness from knowing nothing to knowing well. Due to the specialty of e-commerce environment and operation methods, all groups involved in e-commerce should follow closely the pace of e-commerce information development and keep learning new knowledge by all means. For an enterprise, it should begin with all kinds of internal trainings to spread security consciousness among its employees. Through teaching security strategies on all components of e-commerce, the enterprise can improve the security consciousness of its e-commerce marketers and managers and the crisis-processing ability of its employees. In addition, it is also very important to popularize the security knowledge among e-commerce users through various forms of media. After learning the marketing methods of e-commerce and the potential consequences that may happen in all components of e-commerce, one e-business user can make a great improvement on his/her ability to find and solve risks. With the training of security consciousness on both enterprises and buyers, the security of e-commerce will be greatly improved.

3.2. Adopting multi-layered network and cryptography to guarantee information security

With the expansion of e-commerce, large-sized electronic payment data warehouse or decision-supporting system is required to reduce credit risk, market risk and financial risk [11]. Database or data warehouse can be used to store and process information, provide decision support for all components of e-commerce and reduce credit risk that may appear in the electronic payment process. On the whole, the large-sized electronic payment data warehouse or decision-supporting system should be designed to: collect information resources and process and analyze them; scientifically manage assets, debts and intermediary business of customers; store, manage and analyze data while ensuring the symmetry, completeness, transparency and correctness of information; classify, organize, analyze, count and monitor various types of data according to their roles. In order to realize the sharing, transmission and storage of network resources, security measures including firewall, physical isolation and VPN can be used to defend against attacks from unauthorized users. With the link transmission of data over logical networks such as Internet and Frame Relay, the extension of a private network where data is enclosed, encrypted and identified will be achieved. In the process of maintaining e-commerce, we should periodically troubleshoot the internal and external network to find all kinds of physical isolations, update operating system patches, and maintain the security of operating system, database, web servers and e-mail serves [12~13]. In addition to the multi-network technique, the application of cryptography and digital certificate also shows increasing influence on e-commerce. For the trust management, authorization Control and responsible mechanism in e-commerce, they all demand the authenticity, integrity and confidentiality of information. When various types of data are encrypted, transmitted through encrypted channels and decrypted after being received, interactive verification will be carried out among peer entities. The application of cryptography including identity verification and digital integrity, encryption and signature will guarantee the verification of identity and the authenticity and integrity of information.

3.3. Enhance risk analysis, prevention and control to reduce system risk

Because enterprise e-commerce is characterized by complex participants, various types of transactions and large amount of processing data, daily preventive measures should be taken to maintain the normal running of facilities and system. Aside from periodically troubleshooting network to find physical isolations, we should establish: network security maintenance log to record security-related information and events which is convenient for the enterprise to find problems in an emergency; classified management system where data stored in database is encrypted on the principle of classified management; real-name authentication system to prevent someone from illegally occupying legal users' accounts and passwords. The reinforcement of daily operational maintenance can reduce the possibility of the system being broken and attacked and defuse different types of crises in daily maintenance. And thus, the risks to the system are reduced and the efficiency of e-commerce is improved. Aside from daily maintenance to hardware and system, we also develop risk analysis strategies to assess the security risks of the system. Risk analysis strategies mainly include risk identification, risk analysis and risk control. Risk identification is to identify security risks that may pose potential threats to e-commerce system from all kinds of collected threats, bugs and other information. Risk analysis is to use qualitative and quantitative methods (analysis, comparison and assessment) to determine the danger classes of all security risks in e-commerce to assess the possible consequences that they may cause to all components of e-commerce. It mainly includes risk probability analysis, assessment matrix analysis and sensitivity analysis. In the analysis, it is difficult to quantize all influencing factors, so we can analyze the risks by mainly using the qualitative method and complementarily the quantitative method. Risk control is to control the risks at the affordable level by using risk control methods, such as risk control measures and Risk compensation measures. It mainly includes risk transfer, loss control, and insurance selection and risk assumption. The final purpose of risk control is to control the risks assumed by e-commerce enterprises at the lowest level by risk control strategies. Technically, enterprise e-commerce usually adopts a multi-layered security model. Even though one layer is broken, the other layers can operate normally to protect the security of e-commerce resources [14].

3.4. Complete e-commerce legislation to guarantee the interests of all involved parties

Meanwhile, wide-range multi-channel electronic payments are bringing new difficulties for the legislation of e-commerce. In order to prevent risks brought by new types of crimes, we should accelerate progress in e-commerce legislation while improving technical measures and management system [15-16]. As for problems appearing in e-commerce electronic payments, we should absorb and borrow foreign experiences in legislation of network information security, and then make some investigations for the establishment of e-commerce laws, such as Personal Privacy Protection Law, Trade Secret Protection Law, Database Promotion Law, Information and Network Security Law, Digital Certificate Law and Online Intellectual Property Law. Therefore, there will be legal bases for network control, information control and information resources management. In the operation of electronic payments, we can establish regulations for the risk responsibility of electronic fund transfer and the jurisdiction and arbitration of criminal cases in electronic payments. And thus, a relatively complete legal system of the security management in e-commerce is built, and an electronic payment environment with legal permission, legal guarantee and legal restriction is formed. Only by establishing a complete legal system for the security management in e-commerce, can we establish guarantee the interests and rights of all e-commerce participants. With the efforts of enterprises and their administrative departments as well as the supervision of functional departments, the establishment and management of the e-commerce legal system must be promoted and thus the regular running of network transactions will be guaranteed.

4. The e-commerce security strategy

4.1. The e-commerce network devices safety security strategy

The security strategy of enterprise e-commerce system level often consisted by system isolation, access control and authentication technique. System isolation is an effective isolation way in e-commerce operation process. Isolation means dividing the network into several non-communicating networks according to the difference of network security level, so that the networks or devices of different security levels have no access to each other and get the safety isolation goal. At the present stage, we often take VLAN network technique based on the original isolation way to segregate the service network or the office network, by this we can set effective and reasonable access strategy to executive access strategy of different network resource and prevent illegal users visit the protected resource. The main way and strategy is according to the access control list and security strategy to control the information flow, to check and filter network information and data, to screen out the effective and reasonable data and to intercept unsafe information and data. The interception means after the scanning, tracking and early warning to network system, distinguish it initiatively, timely and effectively, and then block it. This process will check and analyze the network device and the security holes, including network service, firewall, router, mail servers and web server etc. As to end-customers, we often use the authentication which is used on e-commerce customers, for example, electronic business links network account, account password, dynamic password, Ukey secret key, IC card, magnetic card, fingerprint technique etc. By all means of authentication, we prevent illegal users visit enciphered data, ensure the identity materials, property information and other data will not be revealed, tampered or destructed [7~8].

4.2. E-commerce operating system security strategy

Operating system is a collection of system software includes the software control running of other programs and the software offer users interactive operation interface. Because e-commerce refers to all kinds of transaction and payment under many circumstance, its operating system is related to Android, BSD, iOS, Linux, Mac OS X, Windows, Windows Phone and z/OS etc. To some extent, operating system plays the key role of e-commerce hardware resource. For operating system is in charge of device management, data storing, information sending and the scheduling of all kinds of system resource, the security of operating system directly influences the safety of application system and information data. When we test the security of operating system as the server-side, we should scan and analyze different versions operating systems, divide operating systems according to their security risk level, make test report about the security hole of system based on the scanning result and repair the data hole leakage and system bug in time, so to protect applications and data from embezzling or destructing from the server system level. As end-customer, when choosing the operating system which that suits us, we should try to avoid installing dubious software, protect and back-up the system. When some abnormalities occurred, we should recovery system and reduce the damage to e-commerce transaction course caused by operating system.

4.3. E-commerce documents and data security strategy

Application runs in user mode. It's a computer program interactive with users though visible user interfaces. When e-commerce is running, the storage and transferring of most text documents, pictures and applications need to depend on the management and operation of computer files. So the security strategy of computer files storage and transfer process becomes the key focus of e-commerce operation process. As to the transfer of file information in e-commerce, we can use security disposal mechanism like encryption, electronic signature, integrity authentication etc. to make effective security disposal and let the transferred files can be only deciphered and read under the condition the receivers use related security identification mechanism. This kind of security precaution strategy took during the file transfer to some extent reduce the possibility of the files being intercepted, tampered or destructed. As to the storage security of e-commerce files, we can use the way of authentication and password protection taking effect simultaneously. The important files stored in local network or the network is in the state of double-encryption, even when the others get the file by illegal way, he also needs to crack two security protection precaution strategies if he wants see the content of the file. To take effective security precaution on storage and transfer of e-commerce files can prevent external illegal incursion and internal information revealing. The files and data in the operation of e-commerce enterprises depend on database to be stored. In database itself, the security level and system level security can meet the routine application of enterprises. For e-commerce enterprises have higher requirements on data and information security level, we can increase related security components based on database, like installing anti-virus software and firewall software, create backup data and recovery system, disposal and backup data regularly. By changing database password regularly, improving password strategy, managing database hierarchically, we can achieve the goal of overall process encryption and control for the visiting, access and transfer of database [9].

4.4. Strategies for the security of e-commerce transactions

Under the e-commerce, a security transaction usually passes through the following steps: verifying the identity of involved parties, encrypting the commands and data being transmitted, checking the data integrity, and preventing either party from denying the trading results. In another word, an e-commerce transaction involves the identity verification of all involved parties, the application of digital certificate and digital signature, and the encryption of transmitted commands and data under SSL protocol. Compared with traditional commerce, e-commerce is encountering some new problems, such as the information leakage, revision and falsification as well as attacks from computer viruses. Therefore, safe and reliable communication networks should be established to ensure the security of the data and information as well as the promptness, effectiveness, reliability, integrity and confidentiality of e-commerce transactions. In the e-commerce transactions, there are two major security standards, namely, SET (Secure Electronic Transaction) at the application layer and SSL (Security Socket Layer) at the session layer. SET protocol is a security standard raised by VISA and MasterCard for protecting e-wallet, e-mall and certificate authority. It is used to protect the confidentiality of information and the reliability of data and identify the accounts of both the buyers and the sellers. Particularly, financial institutions like banks use it to approve a transaction.

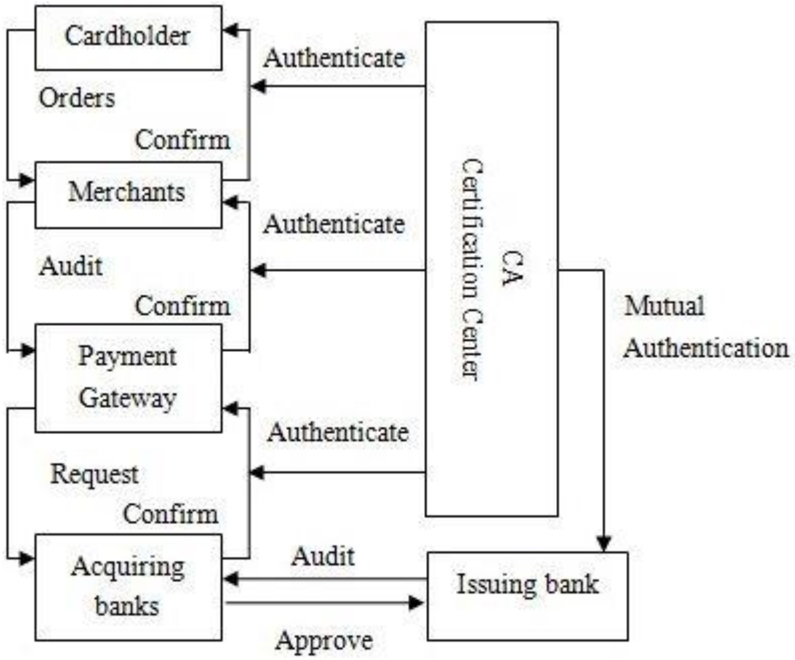

Figure 1. The Secure Electronic Transaction Protocol Data Exchange Process

As shown in Figure.1, “The Secure Electronic Transaction Data Exchange System Composed of Issuing Banks, CA, Cardholders and Sellers”, it can be seen that: each order between a cardholder and a seller must be sent to the CA for approval; after “approval” command is given by the CA, the order will pass through the payment gateway to the acquiring bank; with the mutual requests, authorization, approval and confirmation between the acquiring bank and the issuing bank, a complete data exchange is completed under the SET protocol. In addition to this, because modern e-business transactions usually operate under the framework of network communication platform, this paper introduces another form of SET data exchange system based on this platform, which is shown in the Figure.2. From the Figure.2, it can be seen that: it has more payment platforms for the sellers, banks and users to select; these payment platforms are based on a network platform composed of electronic tellers, e-package, payment gateway and CA; it changes single transaction process into diversified payment options for users to choose in their e-commerce transactions; in order to ensure the security of each payment, the digital certificate authorized by the CA is closely linked to the whole payment process. The SSL at the session layer is the security protocol raised by Netscape for protecting the confidentiality, integrity and openness of data and for verifying the identity of involved parties. It is mainly used to prevent data in the web pages of e-commerce transactions from being stolen and destroyed. In an e-commerce transaction, what a user deals most with is various forms of passwords, which are equivalent to encryption techniques in the cryptography. Encryption techniques can be classified into symmetric encryption system and asymmetric encryption system. For symmetric encryption system, it is a high-efficient encryption system, but hard to distribute and manage. For asymmetric encryption system, although not as efficient as the symmetric encryption system, it is easy to distribute and manage. Because confidentiality level is determined by the encryption method and strength, an enterprise can select appropriate encryption method and strength based on its demands for confidentiality level and then determines which encryption system should be adopted.

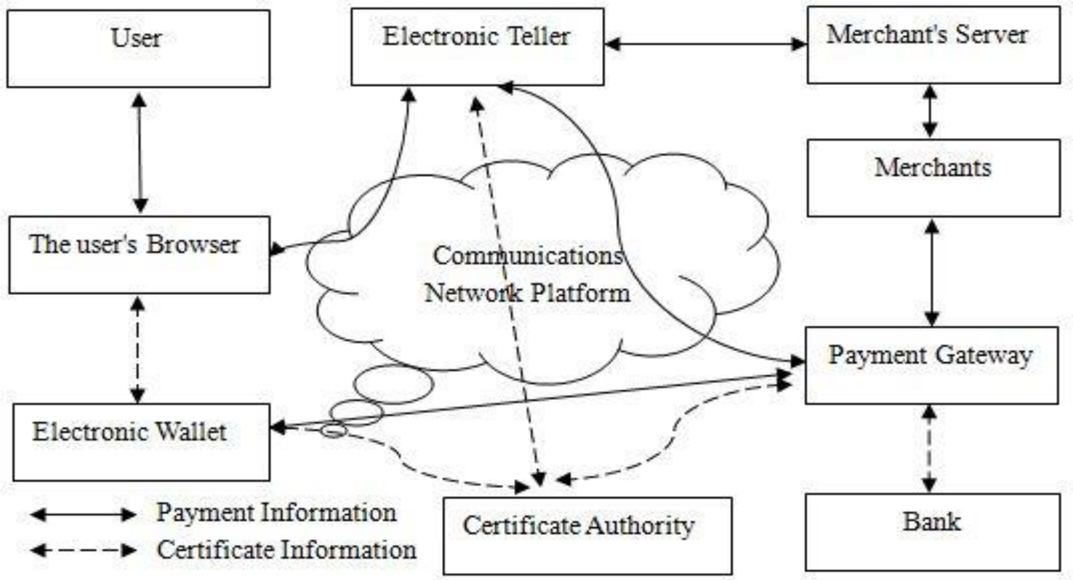

Figure 2. Payment and Certificate Information

For an e-commerce enterprise, it always demands a reliable data transmission which can meet the different functions of the data exchange system. Therefore, we can divide the system into different physical layers based on its communication architecture. In protocol stack, each layer processes the data from its upper layer and marks it with a particular method, ensuring that the data can be identified and decrypted by the same layers of other computers. From the comparison between the encrypted communication stack and the unencrypted stack as shown in Figure.3, it can be seen that when data need to be encrypted in transmission, one application program should adopt encrypted communication stack, of which the biggest difference with the non-encrypted communication stack is that it will negotiate with the whole system when building security parameters required by encrypted communication. In the negotiation system, the identity verification is needed. The security protocols which are widely used are transport layer security protocol and security socket layer protocol. From Figure.3, we can see that only physical layer undertakes the task of sending data to wireless or wired network while other layers simply play their role in error detection, correction and encryption.

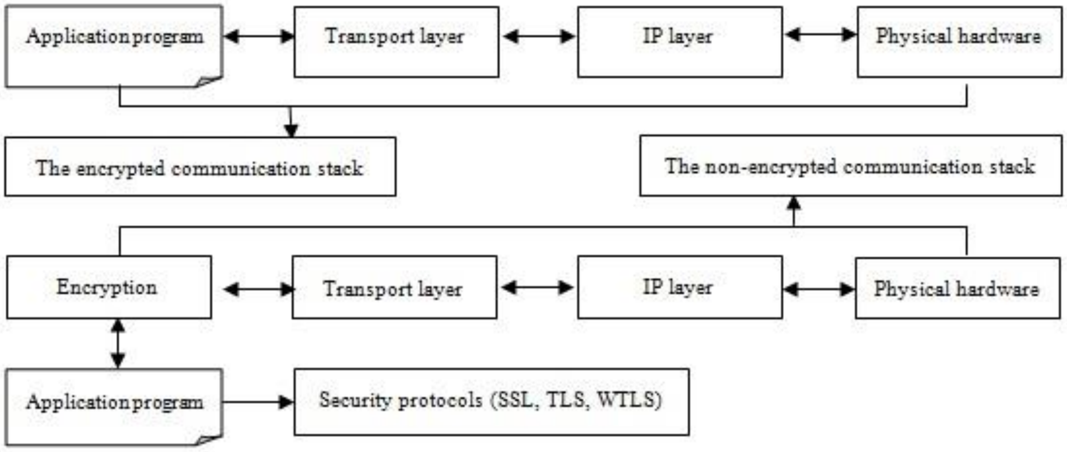

Figure 3. The Comparison between the Encrypted Communication Stack and the Unencrypted Communication Stack

5. Conclusion

With the rapid development of e-commerce, many new problems and contradictions emerge. In the globalization of economy, e-commerce brings great influences on economy, politics and law. There are many strategies for e-commerce security: developing the education and training of e-commerce in enterprises to improve their security consciousness; adopting multi-layered network and cryptography to guarantee information security; enhance risk analysis, prevention and control to reduce system risk; complete e-commerce legislation to guarantee the interests of all involved parties. The research on e-commerce security strategies will help to improve e-commerce security techniques, complete e-commerce management system, create conditions for the healthy development of e-commerce and inject new vitality into e-commerce.

Acknowledgements

This work was supported by the Humanity and Social Science Youth foundation of Ministry of Education (No. 13YJC880133), Chongqing Education Committee educational reform (No.1202096), Chongqing science of education plan and the key Research Foundation of Chongqing University of Education (No.JG201210).

References

[1] T. P. Van Dyke, V. Midha and H. Nemati, “The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce”, Electronic Markets, vol. 17, no. 2, **(2007)**, pp. 68-81.

[2] C.K. Ayo, J.O. Adewoye and A.A. Oni, “Business-to-consumer e-commerce in Nigeria: Prospects and challenges”, African Journal of Business Management, vol. 5, no. 13, **(2011)**, pp. 5109-5117.

[3] W.J. Deng, and P. Wen, “Fuzz neural based importance performance analysis for determining critical service attributes”, Expert Systems with Applications, vol. 32, no. 2, **(2009)**, pp. 3774-3778.

[4] Granova, A. and J.H.P. Eloff, “Online banking and identity theft: Who carries the risk?”, Computer Fraud and Security, vol. 11, **(2004)**, pp. 7-11.

[5] C. C. Wang, C. A. Chen and J. C. Jiang, “The impact of knowledge and trust on e-consumers’ online shopping activities: an empirical study”, Journal of computers, vol. 4, no. 2, **(2009)**, pp .11-18.

[6] D. Gefen, “E-commerce: the role of familiarity and trust”, Omega-Oxford-Pergamon Press, vol. 28, no. 6, **(2000)**, pp. 725-737.

[7] D. Mao, “A Study of Consumer Trust in Internet Shopping and the Moderating Effect of Risk Aversion in Mainland China”, Hong Kong Baptist University Hong Kong, Hong Kong, **(2010)**.

[8] D. J. Kim, D. L. Ferrin and H. R. Rao, “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents”, Decision support systems, vol. 44, no. 2, **(2008)**, pp. 544-564.

[9] S. A. Majore, , H. Yoo and Taeshik Shon, “Next Generation Electronic Record Management System based on Digital Forensics v”, International Journal of Security and Its Applications, vol.7, no.1, **(2013)**, pp. 189-194.

[10] P. A. Pavlou, “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model”, International Journal of Electronic Commerce, vol. 7, no.3, **(2003)**. pp. 69-103.

[11] M. S. Shahibi and S.K.W. Fakeh, “Security Factor and Trust in E-Commerce Transactions”, Australian Journal of Basic and Applied Sciences, vol. 5, **(2011)**, pp. 2028-2033.

[12] G. B. Murphy and A. A. Blessinger, “Perceptions of no-name recognition business to consumer e-commerce trustworthiness: the effectiveness of potential influence tactics”, The Journal of High Technology Management Research, vol. 14, no.1, **(2003)**, pp. 71-92.

[13] M. K. O. Lee and E. Turban, “A trust model for consumer internet shopping”, International Journal of Electronic Commerce, vol. 6, no.1. **(2001)**, pp. 75-91.

[14] S. A. Aghdaie, S. Fathi, A. Piraman, “An Analysis of Factors Affecting the Consumer’s Attitude of Trust and their Impact on Internet Purchasing Behavior”, International Journal of Business and Social Science, vol. 2, no. 23, **(2011)**, pp. 147-158.

[15] R. Gururajan, “A Discussion on Security Risks in Mobile Commerce”, e-Business Review, vol. 7, no. 2, **(2006)**, pp. 9-39.

[16] Q. Y. Jin, K. Lee and D. Won, “Study on A Secure Remote User Authentication Scheme Using Smart Cards”, International Journal of Security and Its Applications, vol. 7, no. 2, **(2013)**, pp. 107-116.

Author

Yongyong Zhu is currently pursuing his Ph.D. at Southwest University of Political Science and Law. Since 2011 he has been working as Associate Professor at Chongqing University of Education. His research interests include Civil Law and Commercial Law.