A Study on the Framework of the Security-Based E-commerce Applications

Jianhong Li

Abstract With the development of Internet, e-commerce is emerging as the key and hot transaction approach in the near future. However, more and more concerns about the security have been raised within these decades due to the confidentiality and privacy aspects through Internet. This paper introduces the related technologies in e-commerce development and proposes a detailed analysis of the existing Internet network and business security issues in e-commerce process. Given an electronic transaction process, this paper aims to achieve the security of e-commerce application framework. Several aspects of the development of e-commerce security technology, as well as the development of electronic commerce are taken measures in the paper.

Keywords E-commerce · Security · Electronic transaction · Application framework

1 Introduction

E-commerce is now an unstoppable momentum in the world rapidly growing popularity [1]. It is, in electronic technology, on the basis of commercial operation, the use of electronic technology is widely used to enhance, speed up, and carry out the expansion and enhancement, changing the process of business. On the one hand, the modern information technology is critical, on the other hand, goods and services greatly influence the efficiency and effectiveness of e-commerce. The

J. Li (✉)
Jiangxi Science and Technology Normal University, Nanchang, Jiangxi, China
e-mail: 23979446@qq.com

Y.-H. Han et al. (eds.), *Ubiquitous Information Technologies and Applications*,
Lecture Notes in Electrical Engineering 214, DOI: 10.1007/978-94-007-5857-5_69,

benefits of e-commerce to global economic development are still difficult to fully and accurately measure. But many benefits of e-commerce business are obvious: such as the improvement of the corporate image, providing of the latest product information can be non-store direct marketing, streamline processes, improved operational efficiency, as well as shorten time to market [2, 3]. It is predict that electronic commerce will become the main driving force for promoting economic development of the next century. E-commerce development, support technology, such as security technology, virtual reality technology, CA certification technology, cannot be separated from research and applications, conducive to the popularization and promotion of electronic commerce, and long-term development.

E-commerce transactions are conducted on the Internet. However, over the Internet, a comprehensive e-commerce, doing business online will be much more quick with much more security concerns [4]. It is not only thoroughly dispelling the doubts of the people's minds, but also faces many practical problems. Security threats to the Internet to e-commerce have brought a lot of security issues. For example, from February 7th to the 9th 2000, Yahoo, Amazon, CNN, including the major U.S. network company's Web sites met a series of attacks by the hacker. The same well-known Microsoft has not escaped a similar attack. Internet-based e-commerce security risks are mostly concerned in the following areas:

Openness: the generation of the Internet stems from a shared computer resources, precisely because of its openness and sharing on the Internet. User's computer security problems, you can easily access someone else's computer, other people also can enter your computer system to view, use, modify and even delete your files and data.

Transfer Protocol: Internet uses TCP/IP and FTP, RPC, NFS [5]. These agreements did not take any security measures to transfer the contents, thus, a third party can easily steal transfer contents.

Operating system: Internet uses a large number of operating systems like UNIX, whose system source code is open, in which is a "hacker" to find loopholes to provide convenient conditions. As modern system integration and expansion, they support procedures for dynamic linking and data exchange. The existing operating systems support dynamic linking of the program, including the I/O drivers and service system which can be used to patch the dynamic linking. One of the concerns is the risk of Internet security.

Thus, the safety risks of the Internet bring great challenges to e-commerce. The following security issues are commonly concerned:

Leakage: the leakage of information refers to business activities which aim to steal or use of non-traders. Theft detection of transmission channels or unauthorized access is necessary to information stored in the entity or pretending to obtain the required information [6]. Theft can steal the device loaded into a transmission channel can also be awakened income received computer equipment, transmission equipment, as well as electromagnetic radiation detection within a certain distance.

Posing: This is a common failure mode. Third parties may be issued by the transaction information, such as by posing as the identity of the trader, so as to

Fig. 1 Five step approach for establishing e-commerce environment

achieve the purpose of a deal breaker. It is necessary for traders to have the authentication.

Deny: It refers to the transaction cannot recognize submitted, received or sent messages. During the transactions, contracts, deeds, bills and other news in the submission, transmission, and delivery of any part of the denial or repudiation are very serious.

Destruction of information: Information destruction may be caused by network transmission and vandalism. The information is transferred through the network to lose. Network hardware and software failure may lead to information loss and distortion. In e-commerce activities, the passing of electronic information may be maliciously modified, tampered with the label of the information, content, attributes, recipient and sender, thus making the information lost its authenticity and integrity.

In order to deal with the security issues within e-commerce, this paper outlines the framework of the security-based applications. The concerned issues are dealt by suitable methods so as to improve the security level and may propose some solutions for end-users for various conditions.

2 Information Security in E-commerce

Information security is an issue of universal concern in the field of electronic commerce. Merchants or customers do not want to cause the loss of their interests due to the insecurity of electronic means. A safety construction method of the five stages of e-commerce environment is shown in Fig. 1.

This section emphasizes on the second stage, risk analysis, and design a security framework to adapt to a variety of security needs. The current approach to risk analysis has two methods. The first is the traditional risk analysis strategies, such as CRAMM or Marion2000 [7]. The second method is the use of common safety standards. The most commonly used method of risk analysis is building on top of the three basic security needs, namely: confidentiality, integrity and availability. With the further development of reform and opening up a distributed network, the traditional approach has been somewhat sub-put forward a number of new security requirements.

The well-known security standard is ISO 7498-4. “Information Technology—Open Systems Interconnection - Basic Reference Model” is its excellent feature. This standard is built on five basic safety needs: authentication and identification, authority, confidentiality, integrity and non-repudiation. The five security

requirements constitute a recognized safety standard [4]. But the application of e-commerce on the Internet, this standard only is not complete. There are some more standards such as BS7799 and NIST General Rules.

2.1 Security Aspects

With the development of the Internet and e-commerce, new security requirements have been obtained more attention with regard to traditional risk analysis, including the heavy demands of the current safety standards. E-commerce security requirements were specified as follows: authentication and identification, uniquely identify a person or an entity identity.

Authority: control its activities according to the real identity.

Confidentiality: prevent the illegal deciphering the data information. As a mean of trade, e-commerce information is direct on behalf of personal, business or trade secrets. The e-commerce is to establish a more open network environment (especially the Internet) [7]. And the maintenance of trade secrets is an important guarantee for e-commerce to promote a comprehensive application. Therefore, it is necessary to prevent illegal information access and illegal theft during transmission.

Integrity: ensure that the data has not been illegally modified. The e-commerce is to simplify the trade process, reducing human intervention. It also brings to maintain the integrity of the trading parties' commercial information as well as the problem of unification. The integrity of the trading parties' information will affect the parties to the transaction of trade and business strategies. Free to generate information to prevent, it is suitable to modify and delete at the same time to prevent loss of information in the data transfer process and repeat.

Several aspects should be highlighted as follows.

- Non-repudiation: to prevent acts of repudiation of the entity for its operation.
- Availability: provide continuous uninterrupted service.
- Privacy: to prevent the illegal use or misuse of information or data.
- Audit: the correct records for all of the interactive behavior.

2.2 Security Requirements in E-commerce

Figure 2 indicates that the security requirements of how to construct a complete e-commerce security environments.

The following will be the core of e-commerce—E-commerce interaction process can be simplified, thus underlining the security requirements framework for how it works. Figure 3 shows an e-commerce environment. Customers want to buy a product from the business office.

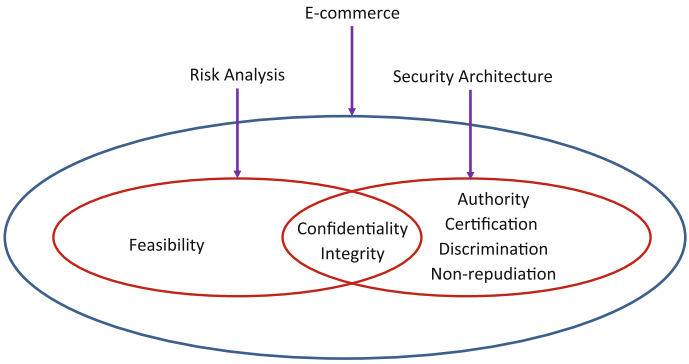
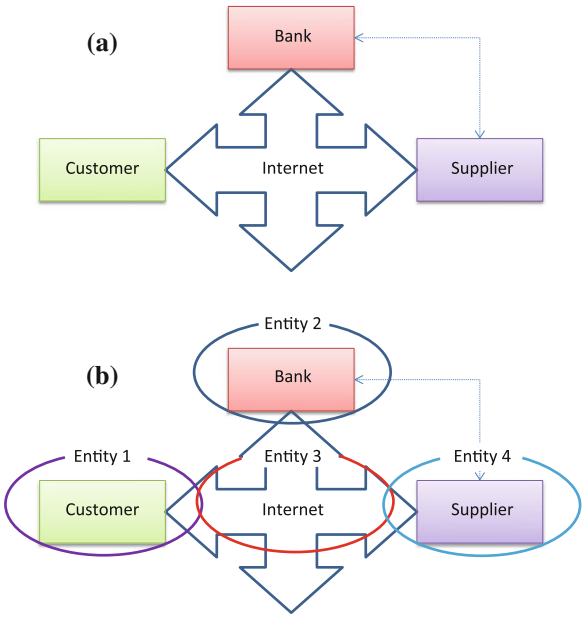


Fig. 2 Security requirements within e-commerce

Fig. 3 A typical e-commerce environment



There are three participants in electronic transactions: customer, supplier and banks. They interact via the Internet (a). For simplicity, there is no taxes, etc. added to the mix. They can be distinguished by four entities (b). Each part has its own specific security needs.

Entity 1—Client is difficult to estimate whether a client security mechanisms to protect. Most users are using browsers, supporting for digital certificates and SSL security protocol. The essence of e-commerce is that most Internet users can be seen as potential customers and therefore cannot in any way interfere with their participation in the electronic interaction.

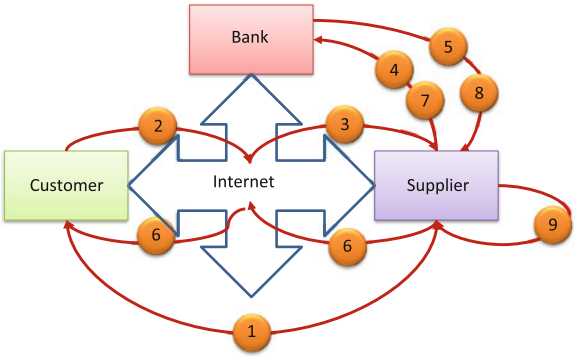


Fig. 4 Typical transactions in e-commerce environment

Entity 2—Bank points out the inter-bank business. This entity will be a number of bank's activities to understand as a whole. The inter-bank business can be understood as the entity's internal activities. Banking entities, including credit cards, digital cash, or E-CASH and other institutions are involved in the security. The role of the banking entity is first examining whether the transactions are legal and proper authorization, and its principle is similar to the principles applied in SET.

Entity 3—Internet generally is understood as a network. No one is responsible for the safety on the Internet. It is also by the individual ego for the consequences of transactions on the Internet [8]. Although the Ipv6 in many test environments have been proved the fact of success, the Internet is still Ipv4 protocol dominant. Unfortunately, Ipv4 do not have many security features provided by IPv6. Therefore, the information passed on the Internet security is uncertain.

Entities 4—suppliers want to provide goods or services to customers. Therefore, they must provide the appropriate hardware and software facilities to protect electronic transactions, normally, while reducing the risk.

2.3 Typical Transactions in E-commerce

The whole transaction will be in the description of the various entities in the transaction process. The next step is to further refine the typical electronic transactions can be completed (see Fig. 4) consists of the following activities:

1. The customer queries and joins the merchant's website via the Internet;
2. Customer browses the site to determine the buying behavior, purchase orders and payment information submitted by the user so as to start an electronic trading;
3. The order and payment information is sent over the Internet to the merchant;
4. The supplier receives orders and payment information to establish the connection with the bank, which verifies the payment information is correct;

Table 1 The safety requirements

		Stage 3 operation								
Entity		A1	A2	A3	A4	A5	A6	A7	A8	A9	Stage 4 mapping
Stage 2	Customer	★	★				★				
	Internet	★	★	★							
	Supplier	★			★	★	★	★	★	★	
	Bank				★	★		★	★		
Security	Requirement										Stage 5 security architecture
Stage 1	Certification discrimination	★	★		★			★			
	Authority					★		★			
	Confidentiality		★	★	★		★	★	★		
	Integrity		★	★	★		★	★	★		
	Non-repudiation		★		★		★	★	★		
	Feasibility				★						
	Privacy	★								★	
	Auditability					★	★	★	★		

5. Bank checks feasibility of the transaction, and the results are sent back to the business;
6. If the transaction is feasible, which means that there are sufficient funds in the customer's account to buy the goods he needs, the supplier will provide customers return confirmation message;
7. Before the end of the transaction, the payment instructions will be submitted to the bank;
8. Bank specifically confirms the payment operations, and returns the evidence;
9. Supplier works out decisions through the analysis of the transaction information to decide the next marketing strategy.

3 Decision Table in E-commerce

In e-commerce environment, the following decision table could be used to help identify the necessary safety requirements (see Table 1). All requirements to meet the security of Step 1 to Step 2 are listed. The entities involved in the transaction, operation in the transaction are listed in Step 3 Step 4. Operation is mapped to a specific entity, described in Step 5. Each security needs some kinds of operations.

In the Table 1, A1 operating businesses must identify the customer's identity and identification in order to ensure the conduct of normal trading. This does not mean the loss of customer anonymity here privacy is that other businesses cannot be obtained because of the transaction of customer's information. The A3 operating on the Internet to transmit information to ensure its confidentiality cannot be

changed. Customers have to submit orders and payment information [9]. The A6 operational requirements consist of the business to return a confirmation to the customer to ensure that the confidentiality and integrity of information submitted. At the same time, customers also want to ensure that the businesses will not deny the confirmation record its operation in order to complete the audit required by the business [10].

4 Conclusion and Remarks

The establishment of the above framework proposed in this paper is to follow a structured approach and can help the parties to the transaction to confirm the relevant safety requirements. Security needs by using the above method would not only pay more attention to, and not because of the complexity of the effects of security settings to the development of electronic commerce. The findings of this paper are some potential issues of the security in e-commerce as follows:

1. A complete e-commerce security solution and the complete model and architecture should be studied.
2. Although some systems are increasingly becoming standards, only a very few API standards. From the point of open market view, the agreement between API and gateway is absolutely necessary.
3. Most e-commerce systems are closed, that is, they use a unique technology only supports certain protocols and mechanisms. They often require a central server as a trusted third party for all participants. Sometimes they also use a specific server or browser.
4. Although most programs are using the public key cryptography, but the multi-party security concerns are far from enough.
5. Most systems will be the relationship between the vendor server and the consumer's browser assumes that the main limit in these systems to perform complex protocol from the relationship. This asymmetrical relationship, and does not allow direct transactions between users.

These findings are the development of secure e-commerce issues to consider. The basic status of China's e-commerce to promote e-commerce development, must take the following measures: the introduction of a unified and effective management; strengthen the information infrastructure; to achieve the interconnection of the professional network.

In addition, the Secure Sockets Layer technology currently used in the United States is 128-bit, but the algorithm's key exports are only allowed to reach the 40-bit. Its security is clearly much worse than the 128-bit key algorithm [6, 8]. Therefore it is necessary to develop high-strength encryption technology, which can seize the initiative in the security and confidentiality of information.

References

1. McKnight, D.H., Hervany, N.L.: What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. Int. J. Electron. Commer. **6**(2), 35–59 (2001)
2. Dai, Q.Y., Zhong, R.Y., Huang, G.Q., Qu, T., Zhang, T., Luo, T.Y.: Radio frequency identification-enabled real-time manufacturing execution system: a case study in an automotive part manufacturer. Int. J. Comput. Integr. Manuf. **25**(1), 51–65 (2012)
3. Zhong, R.Y., Huang, G.Q., Dai, Q.Y., Zhou, K., Qu, T., Hu, G.J.: RFID-enabled real-time manufacturing execution system for discrete manufacturing: software design and implementation. In: Proceeding of the 2011 International Conference on Networking, Sensing and Control, Delft, The Netherlands, 11–13 April, pp. 311–316 (2011)
4. Zhong, R.Y., Pang, L.Y., Pan, Y., Qu, T., Huang, G.Q.: RAPShell for RFID-enabled Real-time Shopfloor Production Planning, Scheduling and Execution. In: Proceeding of 42nd International Conference on Computers and Industrial Engineering (CIE 42), 16–18 July, 2012, Cape Town, South Africa (2012)
5. Delone, W.H., Mclean, E.R.: Measuring e-commerce success: applying the DeLone and McLean information systems success model. Int. J. Electron. Commer. **9**(1), 31–47 (2004)
6. Zhong, R.Y., Dai, Q.Y., Zhou, K., Dai, X.B.: Design and implementation of DMES based on RFID. In: Proceeding of the 2nd International Conference on Anti-counterfeiting, Security and Identification, Guiyang, 20–23 Aug pp. 475–477 (2008)
7. Delone, W.H., McLean, E.R.: The DeLone and McLean model of information systems success: a ten-year update. J. Manag. Inf. Syst. **19**(4), 9–30 (2003)
8. Zhong, R.Y., Dai, Q.Y., Zhou, K., Dai, X.B., Wang, J.: Universal external database design program. Comput. Aided Eng. **18**(1), 83–86 (2009)
9. Wang, M.L., Qu, T., Zhong, R.Y., Dai, Q.Y., Zhang, X.W., He, J.B.: A radio frequency identification-enabled real-time manufacturing execution system for one-of-a-kind production manufacturing: a case study in mould industry. Int. J. Comput. Integr. Manuf. **25**(1), 20–34 (2012)
10. Oxley, J.E., Yeung, B.: E-commerce readiness: institutional environment and international competitiveness. J. Int. Bus. Stud. **32**(4), 705–723 (2001)