4 Security Technologies in E-commerce

Zheng Qin¹ Li Shundong² Han Yi³ Dong Jinchun³
Yan Lixiang¹ Qin Jun³

¹ School of Software, Tsinghua University, Beijing 100084, China
² School of Computer Science, Shaanxi Normal University, Xi’an 710062, China
³ Panda Electronics Group Co., Ltd. Nanjing 210002, China
⁴ School of Information Management and Engineering, Shanghai University of
  Finance and Economics, Shanghai 200433, China

Abstract One of the key issues emerged in the process of transforming a traditional business into an electronic one is the security problem. Compared with tradition paper-aided transaction, information has to be transferred through public Internet network under the electronic environment. The record media of e-commerce has changed from paper to magnetic media. The characteristics that the information recorded on magnetic media can be easily copied, deleted and modified, and the openness of Internet result in that e-commerce information can be easily leaked, tampered, counterfeited and denied. In order to develop e-commerce, the confidentiality, integrity and authentication of e-commerce transaction data must be ensured. The technologies used to handle these issues mainly come from cryptography, and they include such technologies as encryption, authentication, hash, digital signature, firewall, intrusion detection etc. This chapter gives a brief description on those mentioned technologies which gives a basic understanding of how they work so that we can consciously apply these technologies to protect the security of e-commerce during the business process.

Key Words e-commerce, security, reality, encryption, public key encryption, signature, hash function, authentication, firewall, intrusion detection, SSL, SET.

4.1 Introduction to Security Problems in E-commerce

As e-commerce is being rapidly developed and widely applied, e-commerce technology has exerted influence on various aspects of our daily life, and becomes the key factor of a nation’s competitive power. The e-commerce information system of enterprises stores a great deal of commercial secrets concerning the long-term development of enterprises. In economic activities, e-commerce systems
can bring convenience, efficiency and low cost to commercial activities. Personal information system usually stores private information of property and accounts; individuals are able to communicate with each other via the Internet, such as inquiring information, getting messages; moreover, there are also other personal consumption such as purchase, ticket booking and e-settlement. E-commerce security is closely concerned about the protection of citizens’ privacy, and the survival and development of enterprises. The capability of guaranteeing e-commerce security has become a symbol as well as an ace of trumps of the competitive power of enterprises in the 21st century.

The first and the most important problem encountered in the process of digitalizing the traditional commercial activity is the security problem. A complete security problem includes the response reliability of the e-commerce system when it reacts to various accidents and vicious attacks. This chapter focuses on study of problems that are shown by e-commerce under the malicious attacks and relevant countermeasures. Traditional commercial activities are carried out from face-to-face negotiations, signing contracts to fund transfer via banks and delivery of goods. Traditional commercial process is exposed to tremendous risks; for example, one of both parties might not fulfill the contract after signing it, or fail to provide the required cargo after receiving the payment, or fail to pay after receiving cargo. Problems like these can be controlled within certain limit through careful operations, mutual understanding and relevant legal means; however, negative examples are also very common. E-commerce has transcended the restriction of space and time, making it possible to negotiate and sign contracts at any time and any place. In this process, both parties do not have to meet, and the contracts and payment are digitally made. Thus security problem will become very important. Major issues are listed below:

The authenticity of the identity of both parties is how to know the participant of the negotiation is not counterfeited by someone else. If we are negotiating with some cheater, we might let out some important information, which may cause serious losses. How can we judge whether a document comes from someone really as declared?

The secrecy of information exchange: in the process of negotiation, a tremendous amount of information should be exchanged, which usually includes the names, prices, quality of the commodities, as well as the time and place of the commodity exchange. All such information has great value and needs to be protected. If the information is divulged to the competitors, they are likely to take advantage of what they know so as to cause tremendous losses to the negotiator. Thus it is of great importance as to keep the crucial information confidential.

The integrity of information: how can the receiving party make sure that the information received is the complete message that is sent from the other party? And is the message not replaced by another faked message in the process of being transmitted.

Non-repudiation: If one party wants to invalidate the contract which has been signed because of adverse marketing situations, one of the choices it may make is