2011 3rd International Conference on Signal Processing Systems (ICSPS 2011)
IPCSIT vol. 48 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V48.28

Study on E-commerce Information Security Technology

Yang Huaqing [+], Ling Haiyun , and Yang Wenwen

College of Computer, Liaocheng University, Liaocheng, China

Abstract. With the rapid developments of digital communication technology, computer network technology and multimedia technology, e-commerce has been developed rapidly, and the trading volume has increased exponentially. However, new technologies and services will inevitably bring some new issues, in particular the information security in electronic commerce. Reliance solely on the traditional information security technologies, such as encryption, authentication and access control technology has been not reliable enough. In this paper, it studies the application of fragile watermark to e-commerce transactions, which can be used for integrity detections of goods, and provides the principle framework diagram realizing the integrity authentication. In the future secure and reliable e-commerce system, it should be the integration of multiple technologies, such as the combination of authentication technology with access control technology, cryptography and digital watermark technology and so on. We believe that the digital watermark technology will play an increasingly important role in protecting the security of e-commerce transactions.

Keywords-E-Commerce; information security; digital watermark; authentication technology

1. Introduction

With the rapid developments of computers and network technologies, the Internet has been converted from the initial main applications to scientific researches and simple information issues to the commercial service. The majority of merchants and customers hope from their different perspectives the Internet will bring them practical benefits and conveniences. In order to adapt to changes in the globalized market economy, e-commerce has emerged in this environment, and it has gradually become the fundamental need of the majority of Internet users. E-commerce allows businesses to choose their ideal suppliers within the global range and to sell their goods in the global market; it also can make companies communicate more closely with suppliers to meet customers' needs more quickly. E-commerce uses the Internet technology to solve commercial issues of all users, such as connecting geographically dispersed work groups, and contacting new customers, to increase customers' degrees of trust for goods through the improved customer service, thereby enhancing the operational efficiency of enterprises. In recent years, more and more enterprises have used the Internet to carry out a wide range of commercial activities, and have received substantial returns on investment. The transfer of commercial activities to the Internet is faster and faster. The use of advanced Internet technology can reduce operating costs of enterprises, improve the business processing speed, expand sales channels, and help companies solve many difficult problems, such as to accelerate the time to market of new products, to keep businesses dominating the market advantages, to improve the operational efficiency of enterprises, and to solve international issues of enterprises, etc.

E-commerce conducts the electronic payment via the Internet to obtain electronic goods or promises of delivering physical commodities. In the traditional commodity trading process, because two sides of the transaction are face-to-face, it is easy to ensure the security of the transaction process and to build the trusting relationship. However, in the process of e-commerce transactions, both buyer and seller communicate information through the Internet; the Internet e-commerce depends on is highly open, virtual and dynamic, so that there are many security risks for e-commerce activities, and it is difficult to establish

[+] Corresponding author.
E-mail address: yanghuaqing12@163.com.

the security and trusting relationships between both buyer and seller. Therefore, buyers and sellers of electronic transactions face varying degrees of security threats. How to ensure the information security of e-commercial buyers and sellers is the main problem that needs to be addressed in e-commerce. The true realization of a secure e-commerce system should meet requirements of integrity, confidentiality, non-repudiation and authentication, etc. aspects.

2. Technologies Solving the Information Security in E-commerce

2.1. Authentication and access control technologies

The so-called authentication technology means that the user needs to be verified whether his identity is validated when he accesses the network or server. The common method to verify the identity is to use the user account and password, and it can also use the body's certain physiological characteristics, such as eye shading, fingerprints and so on. In order to strengthen the ID authentication, the concept of digital certificates has been introduced on the Internet. It is the digital certificate of an individual identity (or website) that is the digital identity card or passport. The so-called access control technology provides the user's authority to access the network or server. It is closely related to the user's ID authentication that determines the validated user has what kind of authorities to access and operate what information in the system.

2.2. Cryptography

Cryptography is a means to protect important information from being directly read by others. Cryptography includes two processes of encryption and decryption, in which encryption is the process to transform the original information in a certain way into the information that cannot be directly read, and decryption is the reverse process of encryption. There are two main factors that affect cryptography: algorithm and key. Cryptography can be divided into symmetric cryptography and asymmetric cryptography. In the symmetric cryptography, the encryption and decryption use the same key. DES (Data Encryption Standard) is a typical symmetric cryptography, which is a block cipher technique; the size of each block is 64bits, adopting 56-bit key, and the ciphertext is obtained after 16 rounds of XOR, S box replacement, and P box replacement. Its decryption and encryption processes are similar. Whereas in the asymmetric cryptography, the encryption and decryption use different keys, one of which is the public key that can be opened to the public, and the other of which is the private key to be kept secret. RSA is currently the most widely used asymmetric cryptography, which is a cryptographic technology based on a number theory problem, namely the discrete logarithm problem. The security of cryptography depends mainly on the confidentiality of the key, instead of the confidentiality of the algorithm.

People often think that the implementation of information security can be accomplished by using the encryption technique, but which cannot fundamentally solve the problem. The reasons are that: (1) The encrypted file prevents the release of the multimedia information for it is unreadable; (2) The encrypted information leads to the hacker's curiosity and attention easily, and it is possible to be deciphered; once the encrypted file is deciphered, its secret information is completely exposed; (3) With the continuous development of computer hardware technology, and as the parallel computing power continues to strengthen, the approach to use the encryption algorithm to enhance the system security has been severely tested, and the increase in the key length alone to improve he information security has been not the only possible means. To solve those problems, in recent years, a whole new technology in the field of information security has been proposed internationally, namely digital watermark technology.

2.3. Digital watermark technology

The research work of digital watermark originated from the early 90s of last century. In 1993, A.Z.Tirkel, et al published a paper entitled "Electronic Watermark", and later published another paper named "A Digital Watermark". Their first use of "Watermark" marked the birth of a formal study subject - digital watermark technology since then. Digital watermark technology hides the serial number, text, numbers, image signs and other important information in the multimedia data. Because the technology has a very wide range of application prospects in copyright protection, integrity authentication, mark hiding and secret communication, etc. aspects, it has now become a frontier hot topic in the international academic research. Although scholars in China have devoted considerable human and financial resources to the leading topic, unfortunately fully mature technologies or products have not come out so far. With the popularity of electronic goods in China, in particular, as Internet users double and redouble in the next few years, e-commerce will have been rapidly developed; the direct sale of electronic products through the network will bring about tremendous business opportunities for enterprises, which is a shortcut for Chinese goods to enter the international market. Then how to effectively protect the copyright of electronic goods will be the problem of great interest to businesses. People of vision should seize the favorable opportunity to develop our own digital watermark products to adapt to changes in the new situation.

3. Application of Digital Watermark to E-commerce Security

The application of digital watermark technology to the Electronic Commerce mainly shows in the security protection of e-commerce transactions. E-commerce security includes network security and information security, and how to protect the security of e-commerce under the existing Internet environment has received everyone's increasing attention. Digital watermark technology is an effective way to solve this problem. In this chapter, it first introduces the main applications of digital watermark technology in e-commerce, and then studies the implementation programs for robust and fragile digital watermarks to achieve the copyright protection and integrity authentication in e-commercial security, respectively, and provides their formal descriptions. Digital watermark as a new technology in the field of information hiding is considered to be the most promising means of protection of information security. Its current applications in e-commerce mainly include the following aspects:

1) Among the copyright protection of goods in today's increasingly sophisticated intellectual property laws, the copyright of digital products has increasingly become a focus of everyone’s concern, and is also the problem the original author of digital products must pay attention to. Researchers try to find a technology that does not injury original products, while maintaining the role of copyright protection. As a result, digital watermark technology has been applied to e-commerce security. Digital watermark technology uses the information hiding principle to hide the copyright information in the digital product, making it invisible or inaudible, that is transparent. The watermark used for copyright protections is required to be robust, so that unauthorized users in the case of not knowing the key are difficult to erase or destroy the watermarking information embedded in the vector.

2) Authenticity and integrity authentications implant fragile watermarks into digital products; as long as the original products have been changed, it will cause watermarks in the products to change, and hereby validated users can determine the authenticity and integrity of the products. Fragile watermarks are usually applied to the authenticity and integrity authentications of digital products.

3) The information of digital signature is combined with digital signature technology to be embedded into the seal image in the form of watermark, and its combination with digital products can obtain the written confirmation in black and white, and it can sign the paper documents. The watermark information still can be extracted after documents are printed, making the documents have double security.

4) With regard to the protection of web contents in many specific applications, owners often wish that the digital products to be sold can be opened for free browse on the Internet, to achieve the purpose of advertising their products. But it needs also to beware of those contents to be used for commercial profits by unauthorized users. Then the identification information can be embedded in the e-commerce transaction pages, so that it can allow potential customers to browse the Web, and it also protects the intellectual property of pages.

5) Secret communications can be used for secure communications of electronic transactions to protect the watermark information embedded into the vector. The use of secure communication technology hides the business information to be kept confidential into the ordinary digital vector to spread, making the confidential information not easy to be detected or stolen, and therefore it can transfer a number of business information to be kept confidential.

6) Anti-fake electronic notes use the digital watermark technology to embed the transaction time, place, and digital signatures and other authentication information into the electronic notes of both parties to business transactions, so that the transaction process is non-negative and non-repudiation. Moreover, the invisible landmark information is embedded in the electronic invoice, thereby increasing the difficulty for

unauthorized users to forge or alter electronic notes. The extracted watermark can also be used as the legal evidence; when both parties to the transaction have legal disputes, it can present the watermark evidence in court for the judge’s reference.

7) Use restrictions in some special applications, so that it needs special hardware to copy, watch and use multimedia data; if it embeds the watermark information used to identify the permitted copy number into the multimedia, the copy hardware will modify the watermark information in each copy; the permitted copy number minus 1 can prevent multimedia data from being pirated and illegally distributed in a large scale.

8) Copy tracks and digital fingerprints to prevent digital products being illegally copied and distributed, and it can embed different watermark information in each product copy, respectively, like digital fingerprints and so on. Thus, once the unauthorized illegal copies are found, it can retrieve the fingerprint watermark to track its source. Watermarks in such applications should have good transparency and good stability to be able to resist malware removal, forgery and other attacks.

4. Secure Transaction Programs Combining Digital Watermarking with Encryption Technology

In the e-commercial secure transaction system based on digital watermark technology, it usually can be described by the three roles that are digital goods provider or owner of CP, digital goods purchaser or user of User and the authoritative trusted third party - Watermark Certification Center of CA (Certification Authority). Considering from the actual application needs and safety point of view, a complete digital watermark technology-based transaction system should make the roles of various roles, tasks and responsibilities clear.

In e-commerce, electronic transactions of digital products are often conducted on the network through CA, and its copyright protection consists of two aspects, namely the copyright protection and copyright tracking, while in the copyright tracking it is involved to distinguish responsibilities of CP, CA and User in the certification process. The CP sells Product I embedded with watermarks to User1 and User2, respectively, and User3 now also has the same digital product embedded with watermarks, but without the legal purchase contract or procedures, and then who is to assume the responsibility? If the CP sells Product I embedded with watermarks to the User through CA, meanwhile CA sells Product I embedded with watermarks illegally to other N users, in this case, how the User clearly defines the responsibilities with CA? Also, for example, a consumer purchases via the Internet and obtains the right to use Digital Product I with the watermark, when it is hung on the Web page, how to ensure it will not be downloaded and illegally spread by other users? However, in today's digital watermark technology, it mainly considers the protection of rights and interests of CP, with little consideration of the protection of the User's consumer rights and interests. To be fair, in the provision of copyright protection programs, the legal CP and User should be provided with equal protection measures. Therefore, in the application of digital watermark technology to e-commerce, we need a way to protect the CP and User.

To address the above problems, we design a trading program to protect rights and interests of CP and User based on the robust digital watermark. In order to protect the rights and interests of CP, CP is required to provide his proof of identity for CA to register his digital products and copyright watermarking, and to protect the rights and interests of User, User is required to provide his proof of identity for CA to obtain the unique authorization code. The formal descriptions of the program are given below (the principle block diagram is shown in Fig.1).

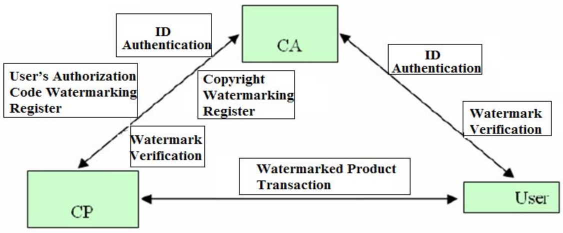
ID Authentication
CA
User’s Authorization Code Watermarking Register
Copyright Watermarking Register
ID Authentication
Watermark Verification
Watermark Verification
Watermarked Product Transaction
CP
User

Fig. 1: Copyright protection and tracking block diagram

9) After the CP encrypts his own identity proof, digital products and the copyright watermarking of w_1 encrypted by the key of Kw_1 with CA's public key of K_{CA2}, submits them to CA through the network, and then after CA receives them, uses his own provivate key of K_{CA1} to proceed decryption register;

10) After the registration is OK, CA uses CP's public key of K_{CP2} to encrypt the confirmation information and sends it to CP, and then CP uses his own provivate key of K_{CP1} to decrypt to obtain the confirmation information of registration OK;

11) The User uses CA's public key of K_{CA2} to encrypt his own identity proof, and applies for registration to CA;

12) After the registration is OK, CA encrypts the unique authorization information code with the User's public key of K_{user2} , and returns it to the User, and then after it is received by the User the unique authorization code can be obtained by using his own private key of K_{user1}.

13) In the process of transaction, the User encrypts his own authorization code with CP's public key of K_{CP2} and sends it to CP;

14) After CP decrypts the User's authorization code, the authorization code is made into watermarking of w_2, and it is embedded into the digital product with the copyright watermarking of w_1 to obtain the watermarked digital product of X, and then it is submited to the User for use. To improve the security, the key of K_{w12} can be added when the watermark is embeded;

15) Meanwhile, CP uses K_{w2} to encrypt w_2 and submits it to CA for registration, and it is used for future copyright tracking;

16) In the process of copyright verification, CA provides CP's registering encrypted copyright watermark and timestamp, and CP provides the private key of Kw_1 to decrypt it to obtain the original watermark of w_1 and extracts the copyright watermark of w_1' from the image X' to be tested (in accordance with the key of K_{w12}); w_1 and w_1' are carried out the correlation test to resolve copyright conflicts;

17) In the process of copyright tracking, CA provides the registered user authorization code and timestamp, decrypts in accordance with the key of K_{w2} to obtain the original watermark of w_2, and extracts the user authorization code watermark of w_2' from the image X' to be tested (requiring the key of K_{w12}); w_2 and w_2' are carried out the correlation test to resolve issues of copyright tracking and responsibility attribution.

5. Conclusion

With the rapid developments of digital communication technology, computer network technology and multimedia technology, e-commerce has been developed rapidly, and the trading volume has increased exponentially. However, new technologies and services will inevitably bring some new issues, in particular the information security in electronic commerce. Reliance solely on the traditional information security technologies, such as encryption, authentication and access control technology has been not reliable enough. In this paper, it studies the application of fragile watermark to e-commerce transactions, which can be used for integrity detections of goods, and provides the principle framework diagram realizing the integrity authentication. In the future secure and reliable e-commerce system, it should be the integration of multiple technologies, such as the combination of authentication technology with access control technology, cryptography and digital watermark technology and so on. We believe that the digital watermark technology will play an increasingly important role in protecting the security of e-commerce transactions.

6. References

[1] Gao Jianhua, "Analysis and Study of E-Commerce Security Technology". Computer and Digital Engineering, 2009,35 (2) :108-109.

[2] Zhang Feng, Qin Zhi-guang, Liu Jinde, et al, "E-commerce Security Architecture". Computer Science, 2008,29 (11) :121-123.

[3] Guo Tao, Li Tang, Wu Shizhong, et al, "Review on E-commerce Secure Payment System". Computer Applications, 2009,20 (1) :1-4.

[4] Wang Xiaobin, Wu Zhihong, "Network Security and E-commerce". Journal of Shenyang Institute of Aeronautical Technology, 2009,20 (2) :32-34.

[5] Yao Zhihai, “Discussions on E-commerce Network Security Issues and Countermeasures”. Market Weekly • Theoretical Research, 2008,3:134-135.

[6] Zhang Bin, “Information Security in E-commerce”. Journal of Jinzhong Teachers College, 2009,20 (2) :131-133.