Digital signature in E-Commerce security

DR. Ibrahim Sayed Abdelwahab Mohamed

E-mail: ibrahimlasheen97@yahoo.com

Received: 11 Jan. 2018, Revised: 18 Jan. 2018, Accepted: 3 Feb. 2018

Published online: 6 Feb. 2018.

Abstract

P2P (Peer-to-Peer) e-commerce has rapid development and progressive maturity. It brings benefits along with the new business risk simultaneously. The lack of trust has become the main obstacle to e-commerce development. P2P is an equity network that connects up individual computer terminal directly to execute a variety of communication. Within the P2P network, people can directly connect to another computer to exchange files, rather than connect to a central server to browse and download as in the past. Lightshare is an example that has implemented e-commerce on the P2P network successfully. However, the users involved in the transaction have anonymity, and dispersion in space, which not only increase the convenience and flexibility of business activities but enlarge the risks and security threats of business activities. So, in this study, we will discuss the security and identity trust problem of e-commerce based on P2P.

Keywords: Security, Digital Signature, E-Commerce, P2P.
Introduction

As more and more information is available on the web, securing that data becomes increasingly important to protect users.

The Internet is the global network of non-executive directors and has a lot of security risks. Cybercrime carried out on the Web can include identity theft, fraud, espionage, and intelligence gathering. Web-based vulnerabilities now outnumber traditional computer security concerns. So, the information system based on the Internet is facing a wide range of security threats.

ZHU Junxuan and colleagues see that the existing Web systems have the following defects in the security aspects:

1- The system lacks an effective authentication mechanism.

2- The Web server cannot determine whether the web information has been tampered with.

3- The transmission of information is not encrypted, which is easy to cause disclosure of sensitive information.

4- The lack of user-level classification is easily lead to excesses access control failure(Zhu, 2010).

The study problem

This study focuses on the Digital signature and its role in E-Commerce security and answering the following questions:

1- What are the protocols for secure E-Commerce transactions?

2- What is the digital signature and what its application in E-commerce?
What distinguishes this study from previous studies?

In this study, we talk about E-commerce security from some aspects, like the protocols that secure E-commerce transactions and digital signature and its application in E-commerce security.

The Study Content

1.0 Protocols for Secure E-Commerce Transactions

An e-commerce transaction protocol is a collection of rules that governs how the operations in an e-commerce transaction should be executed. Among other things, it specifies the exact set of actions, and how they (or some of them) are ordered to realize purchasing atomicity under various circumstances. It, however, does not tell how to handle exceptions arising from behaviors of untrustworthy players that may compromise the atomicity. A protocol can be conveniently described by a tree, called protocol tree. Each path originating from the root represents a possible sequence of action executions, which is termed a run of the protocol. Thus, a run is a class of transaction executions that follow the same execution pattern. The nodes of the tree represent the stages of possible runs of the protocol. A node has a content, which is the transaction state at that stage. The letters inside the nodes identify the nodes and their subscripts distinguish contents. Two nodes have the same contents if and only if the inside letters have the same subscripts. The arcs, and therefore paths in general, are state transitions. Each arc is labeled with the action that causes the transition. A path originating from the root and ending at a leaf is called a complete path. A run may or may not be protocol conformance. We require that all the runs conforming to the protocol be presented in the tree. If a run does not follow the protocol but can be predicted in advance,
then it can also be represented (Dumas, O’Sullivan, Heravizadeh, Edmond, & ter Hofstede, 2003).

2.0 Trust risk of P2P E-Commerce

In P2P e-commerce mode, users have a more flexible mode of communication transactions. Each user node may have mutual access to each other and direct transactions. P2P can make better use of idle PC resources and improve the efficiency of transactions and achieve better anonymity. But P2P e-commerce may confront more risks, such as the selfishness of the nodes, anonymity, and identity arbitrary.

To minimize the probability of risk, one is technical means of risk mitigation, and the other is strictly control and supervision of businesses behavior to reduce risk through a transaction trust mechanism.

Opportunistic behavior in business activities will occur usually. Some people may use a new registration name or a new identity after the fraud, or one real entity may register two identities to achieve an assessment of the satisfaction or different online behavior.

The identity uncertainty leads to lack of trust between both parties of the transaction in P2P e-commerce. So, the management of identity trust must make certain improvements on traditional security technologies to adapt to P2P network environments (D. Wang & Lu, 2012).

3.0 Digital signature

Digital Signature (DS) is a mathematical scheme for demonstrating the authenticity of a digital message or document. DS gives a recipient reason to believe that the message or document was created by a known sender and that it was not altered in transit. DSs are commonly used for software distributions, financial transactions, and in other cases, where it is important, to detect forgery and tampering.
The purpose of a DS is to guarantee that the individual sending the message or document really is who he or she claims to be. Where the goal is to facilitate both e-government and e-commerce applications over the Internet. DSs are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, DSs must be non-forgable. There are a number of different encryption techniques to guarantee this level of security.

DSs are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use DSs. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

DS is implemented by attaching a digital code to an electronically transmitted message that uniquely identifies the sender. DSs are equivalent to traditional handwritten signatures in many respects, properly implemented DSs are more difficult to forge than the handwritten type. DS schemes in the sense used here are cryptographically based and must be implemented properly to be effective. DSs can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a timestamp for the DS, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything that can be represented as a bit of a string, examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

There are few commercial applications that supporting a DS, as an example Adobe, Excel, MS Outlook and etc...
There are many common methods in DS, one of them is to use a Public Key Cryptography, DSs are created and verified by cryptography. Public key cryptography employs an algorithm using two different, mathematically related "keys", one "public key" for creating a DS or transforming data into a seemingly unintelligible form, the other key "private key" for verifying a DS or returning a message to its original form.

The disadvantage of this method is, if many people need to verify the signer's DS, the public key must be available or distributed to all of them, probably by the means of distributing it in an online repository or directory where it is easily accessible.

Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge DSs, but they can try.

Another fundamental process, named a "hash function", is used in both creating and verifying a DS. The hash function is an algorithm that creates a digital representation or a "fingerprint" in the form of a "hash value" of a standard length which is usually much smaller than the message's length but nevertheless substantially unique to it. Any changes to the message lead to producing an invariably different hash value when the same hash function is used. Hash functions enable the software for creating DSs to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it has been digitally signed (Elmadani, 2012).

4.0 Application of digital signature in E-commerce

In a classic business model, the specific responsibilities of parties in the contract are prescribed by written autograph and seal, which can certify, approve
and make relevant documents into force. In the field of e-commerce, digital signatures are validation certificates used to validate transitive data.

Digital signature technology can effectively solve the information security vulnerabilities made by data encryption, and other problems like negation, counterfeiting, forgery and maliciously modification. The message receiver cannot carry deliberately forgery on real data, or any changes to receive the message. The actual owner of the message will not be replaced by counterfeit criminals. The signature process is generally divided into three phases: system initialization process, signature generation process and signature verification process. In the P2P network, the signature scheme selects the authoritative node as authentic CA according to the trust degree provided by the node trust model.

The signature scheme works as shown in fig.1. Superior CA needs to find the n peer nodes and be also responsible for P2P CA node network construction and the establishment and maintenance of the Combiner node.

![Figure 1. The general process of digital signature](image)

During initialization, the superior CA uses the Elliptic Curve digital signature algorithm to calculate the key pair S and P of CA system signature and certification, where S is the private key. By using of threshold cryptography algorithm, superior CA decomposes CA private key S into n sub-key Si (i= 1,2, ..., n), then sends sub-key Si to n Share CA nodes. When the signature is required, the combiner server assembles t servers to calculate the part of the signature M(Si), then the complete signed certificate M(S), and transmit to the user finally. Through
the initial public key, the user can calculate signature information, and compare the homogeneity of the verification information and the original information to receive the same and refuse the different and find the error node in the system at the end (D. Wang & Lu, 2012).

The Results of the study

The development of the e-commerce boom, e-commerce security has become a major bottleneck restricting the development of e-commerce.

How we can ensure the security of data transmitted over the Internet and the identity of each trading party is the key to the development of e-commerce. It can be said that the most critical issue is the security issue; and Digital Signatures technology is an effective solution to ensure the confidentiality of information transmission, data exchange integrity, non-repudiation of sending messages, the certainty of the identity of traders. It is an important part of e-commerce security (Chen & Xu, 2010).

The suggestions

Applying the Trust Principles to all of the e-commerce activities will develop the fullest possible sort of trusting relationship between the seller and the buyer. The trust-based transaction is not only a sales process model but also a powerful way of creating shared value for the seller and the buyer. The application of the four principles to every transaction is the key factor for e-commerce development.

1- Strengthen and Advocate “Client-focus” and “Customer-centric” in E-commerce.

2- Foster the Collaboration Awareness among the Transaction Parties.

3- Focus on the Long-Term Relationship in E-commerce.

4- Being Transparent in E-commerce (L. Wang, n.d.).
Conclusion

This study discusses the e-commerce security issues and the way to apply a digital signature, a very powerful tool, to solve practical problems. Digital signature technology needs further improvement and great efforts should be put to improve technology involved in the security of digital signatures.

It is essential to continuously improve the infrastructure of the digital signature environment and address the legal as well as technical issues in order to develop digital signatures.

References


