Contents lists available at SciVerse ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

A robust e-commerce service: Light-weight secure mail-order mechanism

Jung-San Lee, Kun-Shian Lin *

Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wunhua Rd., Situn Dist., Taichung City 40724, Taiwan, ROC

ARTICLE INFO

Article history:
Received 16 September 2011
Received in revised form 30 March 2012
Accepted 3 April 2012
Available online 13 April 2012

Keywords:
E-commerce
Mail-order
Smart card
Mutual authentication
BAN logic

ABSTRACT

Mail order systems offer a convenient purchase service, in which buyers need not visit the store physically and instead choose what they want via a table of contents. Without a third party to play the roles of verifier and recorder, however, buyers face a potential problem of being cheated by a malicious seller. Thus, we aim to develop a mail order system over the Internet that can guarantee user anonymity and secrecy during the transaction process. The low computation of the mutual authentication between the parties involved contributes to the practicality of this new system, while the correctness of this process can be confirmed by the BAN logic model.

1. Introduction

In recent decades, the rapid development of the Internet has led to the great popularity of electronic commerce services. People often buy something or handle financial investments through electronic commerce services, such as electronic auctions, lotteries, and payment systems. Due to the convenience and economic benefits of e-commerce, more and more traditional services have been converted to the electronic mode, like e-voting, e-traveler checks, and e-invoices. As a result, people are now paying more attention to the issues of security and privacy; however, the digitalization of one traditional commerce service that is applied very often in our daily life, i.e., the traditional mail order service, has received very little attention.

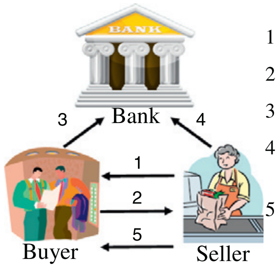
Traditional mail order service (Fig. 1) is a commonly used approach to shopping. As a simple transaction, it has many advantages. The seller sends a menu of commodities to individual guests or buyers in schools and companies who order regularly. The buyer chooses the commodities she/he likes from the menu, sends the purchase order back to the seller, and pays the money to the seller's account. Then, the seller checks to see whether she/he has received the money. If so, she/he sends the commodities to the buyer and the transaction is complete. This system deals with business as a simple transaction flow. More specifically, the buyer does not need to visit the store each time in person but only the bank once. The bank is just a third party to handle the money; it does not serve as the verifier or recorder of the transaction. Thus, in this system, no one records the details of the transaction. This may cause a serious problem in that a malicious seller could feasibly choose not to send the commodity in order to cheat the buyer after receiving payment.

Inheriting the merits of the original mail order mechanism, we aim to realize this concept over the Internet, which can eliminate the above-mentioned security problem. The Internet mail order system is a money-concerned mechanism that uses an electronic payment system, such as electronic cash (E-Cash) (Ling et al. 2007, Wang et al. 2007, Chaum et al. 1990), electronic check (Chaum et al. 1989, Chen 2005, Chang et al. 2009), or electronic traveler's check (Chang and Chang 2009, Liaw et al. 2007). Many scholars have analyzed the various types of electronic payment systems (Yu et al. 2002, Ferreira and Dahab 1998). According to their analyses, even though electronic cash has the advantages of being simple and convenient to carry, it retains the same characteristics as actual cash. When electronic cash is lost or stolen, the user must bear the risk since it cannot be reissued. Although the electronic check has added the signature protocol, it is still vulnerable to the problem of being stolen or embezzled. Due to the requirement for personal identification with a check, an electronic traveler's check seems to be more secure; however, it also involves the drawbacks of a complex authentication procedure, as illustrated in Fig. 2.

When the seller receives the check, she/he cannot confirm the validity of the check, so she/he must send the check to the bank or a fair third party. Another problem is that, in the electronic check and electronic traveler's check system, personal information is usually stored in the bank's database directly. If an intruder or bank employee accesses the database and obtains the user's

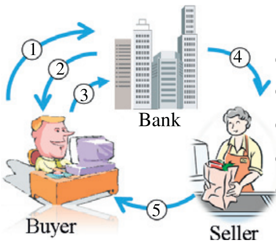
* Corresponding author. Tel.: +886 4 24517250x3721; fax: +886 4 27066495.
E-mail addresses: leejs@fcu.edu.tw (J.-S. Lee), logoduo@hotmail.com (K.-S. Lin).

1567-4223/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.elerap.2012.04.001



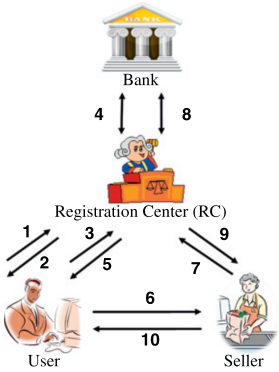
1. Seller sends menu to buyer
2. Buyer sends the purchase order to seller
3. Buyer pays money to the account of seller
4. Seller checks whether his/her account has received the money or not
5. Seller sends the commodity to buyer

Fig. 1. Flowchart of traditional mail order system.



① Buyer has to register at bank
② Buyer receives the smart card
③ Buyer sends purchased request to Bank
④ Bank stores and forwards the request to seller
⑤ Seller sends an “accept” message to buyer

Fig. 3. Flowchart of the Internet mail-order system.



1. User registers to RC
2. RC gives user an anonymous ID
3. User sends a request message and money to RC applying for electronic traveler’s check
4. RC sends the money to bank, and bank generates electronic traveler’s check for User
5. RC sends the electronic traveler’s check to user
6. User sends the electronic traveler’s check to seller to pay for commodity
7. Seller forwards the electronic traveler’s check to RC to confirm the validly of the check
8. RC forwards the electronic traveler’s check to bank and bank searches the database to verify the check
9. RC sends the verification result to seller
10. Seller sends the transaction result to user

Fig. 2. Flowchart of the electronic traveler’s check payment system.

information to apply for services, it may lead to a stolen verifier attack or insider attack. To remedy these drawbacks, Nakamoto introduced the concept of BitCoin in 2009, which depends on no central institution to ensure the transaction (Nakamoto 2012). It applies a database of nodes distributed over P2P networks to handle and record the E-Cash transaction. This can enhance the efficiency of E-Cash verification and the system security. Nevertheless, a trustworthy third party does not get involved in the transaction. Thus, an illegal deal or a dispute occurrence is usually beyond being prevented.

Previous studies of electronic payment systems have focused on the secrecy of the data transmitted between the buyer and the seller, without considering the computation cost in the encryption and decryption process. They often neglect the dispute caused in the shopping flow phase. For example, if a buyer has paid money but cannot receive the commodities ordered, then rights and interests are seriously damaged. In such a situation, the buyer cannot find a reasonable way to inquire about the transaction data in order to prove his/her loss, and the seller is unable to propose valid proof of his/her innocence. Considering these reasons, the Internet mail-order system has adopted a digital cash mechanism based on the hash chain (Lamport 1981), which can overcome the weakness of previous payment systems and ensure practicality. Referring to the famous BAN logic model (Burrows et al. 1990), we prove the correctness of mutual authentication in the new mechanism.

To illustrate that our proposed system can be employed in real life, we assume that Citibank and PayPal are the notaries in our system (Citibank 2009, PayPal 2009). Citibank and PayPal provide mail order service. These providers email commodity menus to buyers and then receive orders as well as money. These companies play the role of intermediary to consult with sellers and order the commodities that the buyers have requested. We bring in a fair third party to serve as the verifier and recorder in the transaction. Thanks to the fair third party, i.e., the bank, it is easy for the buyer and seller to query the transaction data in order to confirm the non-repudiation of involved participants.

The rest of this article is organized as follows. In Section 2, we define the system requirements in detail. In Section 3, we specify the shopping environment and mechanism. Discussions and the comparisons between related work and the novel mechanism are given in Section 4. Then we demonstrate how the new mechanism resists malicious attacks in Section 5. Finally, we make conclusions in Section 6.

2. System requirements

In this section, we define the requirements of the Internet mail order system and specify the significance of each requirement in detail.

(**1**) **Mutual authentication**
The sender and the receiver can confirm each other’s identity in order to avoid man-in-the-middle and masquerading attacks.

(**2**) **Integrity of transaction data**
Transactions of data between buyer and seller are protected from modification. Additionally, the transferred data are confirmed only by a fair third party.

(**3**) **Anonymity of buyer**
The personal information of the buyer is concealed to protect his/her privacy so that no one can trace the transaction records. Here, even the seller is unable to learn the real identity of the buyer.

(**4**) **No forgery of digital cash**
For the purpose of confirming the profits of both seller and buyer as well as keeping the whole process fair, only the bank that acts as a fair third party can distribute the digital cash.

(**5**) **Double spending**
The digital cash can only be used once.

(**6**) **Reissue of smart card**
To avoid losing smart cards, the buyer is allowed to reopen a new smart card in order to get his/her digital cash.

(**7**) **Non-repudiation**
To protect the legal rights of both seller and buyer, the bank records the data of the whole process. This way, if there are any disputes, neither the seller nor the buyer can deny their actions.

(**8**) **Perfect forward secrecy**
To protect the privacy of the communication, the compromised current key cannot be used to derive or recover the session key for previous or future sessions.

3. Mechanism

The proposed ordering mechanism consists of four phases: registration, payment, dealing confirmation, and smart card reissue.