Electronic Commerce Research and Applications 14 (2015) 351–360

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

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

A Secure M-Commerce System based on credit card transaction

Fang-Yie Leu *, Yi-Li Huang, Sheng-Mao Wang

Department of Computer Science, TungHai University, Taiwan

ARTICLE INFO

Article history:
Received 15 March 2015
Accepted 8 May 2015
Available online 12 June 2015

Keywords:
M-commerce
Binary adder
Data Connection Core
Secure Sockets Layer
Secure Electronic Transaction

ABSTRACT

Nowadays the demands for wireless Internet shopping are increasing. But credit card fraud has been serious, and SET and SSL have their own problems. To enhance the security of online shopping, in this paper, we propose a secure m-commerce scheme, called the Secure M-Commerce System (SMCS for short), with which users can create a safe credit-card transaction for Internet shopping. Basically, the SMCS coordinates the cash flow of a trading system and its credit card entities to effectively protect the issued transactions against different attacks and avoid information leakage. The proposed system also employs a Data Connection Core (*DCC* for short) to link the card-issuing bank and consumers before their wireless communication starts so as to significantly improve the security level of our m-commerce environment. Theoretical analysis shows that the SMCS is more secure than SET and SSL. The performance analysis indicates that the SMCS is indeed a feasible m-commerce system.

1. Introduction

Recently, the convenience and security of wireless communication have been greatly improved (Nabi 2005). Many people enjoy online shopping with their credit cards. But due to the infrastructure of a wireless system, the transactions issued are created via wireless. On the other hand, credit card fraud nowadays is serious (Mahmoudi and Duman 2015; Gold 2014), which significantly reduces online shopping attraction for some people. Also, owing to vigorous development of wireless networks, current mobile devices, such as mobile phones, tablet PCs and laptops, have provided users with diverse features and services, which have colored our everyday life and gradually changed people's shopping habits. Generally, a secure credit-card mechanism for m-commerce should securely protect the corresponding transactions and personal information. At present, when shopping in a wireless environment, e.g., to pay something by using the Secure Sockets Layer (SSL), one must send the card number, expiration date and other information to the merchant. In fact, SSL can ensure peer-to-peer delivery safety, but it cannot confirm the identities of the underlying users (Oppliger et al. 2008; Das and Samdaria 2014).

To solve this problem, the Card network organizations Visa and MasterCard put forward an electronic payment system specification for Secure Electronic Transaction (SET) (Lu and Smolka 1999). However, SET has its own problem, e.g., a consumers needs to apply for a certificate (Bella et al. 2003). That means on user side, the corresponding information of the credit card must be stored in a hard disk. Also, to improve its security level, SET takes a long time to calculate complicated asymmetric encryption and decryption key (Shedid and Kouta 2010; Yong and Jindi 2010), thus giving users an inconvenient m-commerce experience. Today, the increasing demands for m-commerce motivate us to construct a safe and convenient m-commerce mechanism. Therefore, in this study, we propose a secure m-commerce scheme, named the Secure M-Commerce System (SMCS for short) which coordinates the cash flow of a trading system and credit card entities to develop a safe and convenient m-commerce environment for users, without increasing extra restrictions and resources on the cash flow and credit card entities. Basically, we produce a credit-card dynamic authentication code to substitute for the credit card information so that the trading merchant cannot know the credit card number and its details. The SMCS also employs a Data Connection Core (*DCC* for short) to link the card-issuing bank and consumers before their wireless communication starts. Furthermore, the card-issuing bank authenticates the credit card's dynamic authentication code and merchant's dynamic authentication code rather than directly authenticating the credit card and merchant information. This can efficiently make sure the legitimation of the consumer and trading merchant so as to effectively increase the security level of the SMCS. Theoretical analysis shows that the SMCS is more secure than SET and SSL. The performance analysis indicates that the SMCS indeed a feasible m-commerce system.

* Corresponding author.
E-mail addresses: leufy@thu.edu.tw (F.-Y. Leu), yifung@thu.edu.tw (Y.-L. Huang), r79520@livemail.tw (S.-M. Wang).

http://dx.doi.org/10.1016/j.elerap.2015.05.001
1567-4223/

The rest of this paper is organized as follows. Section 2 introduces background and related work of this study. Section 3 describes the proposed system. Performance and security are analyzed and discussed in Section 4. Section 5 concludes this paper and outlines our future studies.

2. Background and related work

2.1. Credit card transaction

Generally, the most important feature of a credit-card transaction is to transform the relationship on trading from "seller to buyer" into a series of contractual relations. Due to away from face-to-face purchase, the authorization and security will be the two major concerns. In such a transaction, after confirming the identity of a buyer, the seller receives guaranteed payment from the acquiring bank, and the acquiring bank also receives guaranteed payment from international organizations. The card-issuing bank then judges the authorization of the payment based on the payer's up-to-date credit, and promises to fulfill the payment to the international organizations. Finally, the credit card holder (buyer) is obligated to settle the money with the card-issuing bank based on his/her credit-card contract. This seemingly complicated process, in fact, greatly simplifies the trading relationships between buyers and sellers, because the time difference between the payment and settlement system is no longer a problem, and the information flow and cash flow are separated when the bank and the new contractual relationship intervene (CreditCards.com, http://www.creditcards.com/). Also, the corresponding information flow can be recognized by the merchant immediately to authorize the transaction. Although the seller is requested to pay around 3% of total trading amount of price, this mechanism can greatly increase sale opportunities.

Meanwhile, the merchant is licensed with a message to confirm whether the transaction is completed, and authorization is only an instant of the information flow. Regarding the cash flow, for each day, all the network transactions from different participating member banks will be calculated later by the international organizations. After the member banks are recognized on the date of the network shopping, they will use the "real-time gross settlement system" to transfer the funds to the international organizations, and the international organizations transfer funds to the card-issuing bank. From this moment, you can say that the importance of the role a bank plays in this process is lower, since cash flow is really performed sometimes later after the information flow, and the purchase is completed after the accomplishment of information flow. VISA proves a thing "the information of money is sometimes more important than the money itself!"

2.2. Secure Sockets Layer (SSL)

SSL has two main features. The first is the use of a public-key and private-key mechanism to connect two sides of a network connection. With this mechanism, they can securely exchange encrypted messages with each other. The second is making use of the third party certification to enable both sides of the connection to confirm each other's information (Bicakci et al. 2014; Badra and Urien 2004).

SSL secures electronic transaction specification by using the consumer's credit card number and expiration date or cardholder relevant information as the certification parameters, and transmits encrypted messages to the merchant. The merchant reuses the encrypted messages to request card-issuing bank for payment. The consumers prefer this way, because the system does not request users applying for an electronic wallet and a safety certification from the card-issuing bank.

But SSL has two shortcomings. The first is that the two sides of an SSL connection can only determine whether or not the other side is allowed to use the SSL mechanism. That means the consumer does not know who the merchant is, a legitimate merchant or a hacker. The merchant does not know the identity of the consumer, either, and also cannot confirm whether the consumer's credit card number is correct or not (Bisel 2007).

The second is that although SSL is convenient for consumers to perform Internet shopping through a wireless system, when SSL is invoked by a transaction, the card number and cardholder's related information can be clearly seen on the merchant side, thus possibly being unscrupulous businesses use. Besides, if the card number and other relevant information are stolen by hackers, they may be illegally used for Internet shopping, causing the loss upon not only the cardholder, but also the merchant who would lose the unpaid products if the cardholder submits relevant evidences to deny this transaction. When SSL completes a transaction, the merchant cannot determine whether this transaction is completed before receiving the receipt from the funding or certified bank. The SSL handshake process on Credit card transaction has four stages (Zhao and Liu 2009; Du et al. 2009; Petridou and Basagiannis 2012). In the first stage, consumer informs merchant what version of the SSL, an encryption-algorithm list and a compression-algorithm list that his/her terminal device supports. The merchant chooses the highest versions of SSL, an encryption algorithm and a compression algorithm for use. In the second stage, the merchant sends his/her own certificate and Diffie–Hellman's public key to the consumer. In the third stage, the consumer delivers its own certificate and Diffie–Hellman's public key to the merchant. With merchant's (consumer's) public key and consumer's (merchant's) own private key, consumer (merchant) can derive the Diffie–Hellman common secret key. In the fourth stage, a message is transmitted from acquiring bank to the merchant to prove that the key exchange and authentication process has been successfully completed.

2.3. Secure Electronic Transaction (SET)

SET was jointly developed by the VISA, MasterCard, IBM and other organizations (Venkataiahgari et al. 2006). Like SSL, it uses the public key and private key as the basis to secure message exchange process. However, SET requires that both consumer and merchant apply for SET's certification and obtain the SET's electronic certification and software from card-issuing bank, and then use the software to complete a transaction online.

The greatest advantage of SET, unlike that in SSL, is that both trading sides of a connection can confirm each other's identity. In addition, SET can protect consumers' credit data, since the merchant only requires the consumer's SET credential before it can bill the card-issuing bank (Guan 2009; Li 2008; Sherif et al. 1998).

With the SET mechanism, if a consumer wants to transact, his/her computer needs to install electronic wallet software (Chaudhary et al. 2014), which like a real purse, is responsible for the storage of electronic cash. Before the transaction, the consumer has to first withdraw some amount of electronic cash from the bank. The bank then verifies the identity of the consumer, deducts the amount of money from the consumer's account, and deposits the amount of electronic cash to the consumer electronic wallet. After that, the consumer can purchase goods from manufacturers or shops. The above process is not very friendly to consumer since it is not an "enjoy-first-pay-later" mechanism. It has not achieved the stage of convenience for m-commerce anywhere (Chaudhary et al. 2014).