A Simple and Secure Credit Card-Based Payment System

Chi Po Cheong
University of Macau, China

INTRODUCTION

Credit card is the most popular payment method used in Internet shopping. The idea of credit card payment is to buy first and pay later. The cardholder can pay at the end of the statement cycle or they can pay interest on the outstanding balance. Therefore, there are many credit card-based electronic payment systems (EPSs) that have been developed to facilitate the purchase of goods and services over the Internet such as CyberCash (VeriSign), iKP (Bellare, Garary, Hauser, et al, 1995), SET (Visa and MasterCard, 1997), CCT (Li & Zhange, 2004), and so forth. Usually a credit card-based EPS involves five parties: cardholder, merchant, acquirer bank, issuer bank, and financial institution.

Internet is an open system and the communication path between each other is insecure. All communications are potentially open for an eavesdropper to read and modify as they pass between the communicating endpoints. Therefore, the payment information transmitted between the cardholder and the merchant through Internet is dangerous without a secure path. SSL (Zeus Technology, 2000) is a good example to secure the communication channel. Besides the issue of insecure communication, there are a number of factors that each participant must consider. For example, merchant concerns about whether the credit card or the cardholder is genuine. There is no way to know the consumer is a genuine cardholder. As a result, the merchant is incurring the increase in losses due to cardholder disputes and frauds. On the other hand, cardholders are worried about the theft of the privacy or sensitive information such as the credit card number. They don't want any unauthorized usage of their credit cards and any modification to the transaction amount by a third party. These security issues have deterred many potential consumers from purchasing online.

Existing credit card-based EPSs solve the problems in many different ways. Some of them use cryptography mechanisms to protect private information. However, they are very complicated, expensive, and tedious (Xianhau, Yuen, Ling, & Lim, 2001). Some EPSs use the Certificate Authority (CA) model to fulfill the authentication, integrity, and nonrepudiation security schemes. However, each participant requires a digital certificate during the payment cycle. These certificates are issued by independent CAs but the implementation and maintenance cost of this model is very high. In addition, the validation steps of Certificate-based systems are very time-consuming processes. It requires access to an online certificate server during the payment process. Moreover, the certificate revocation list is a major disadvantage of the PKI-based certification model (The Internet Engineering Task Force). The cardholder's certificate also includes some private information such as the cardholder's name. The requirement of a cardholder's certificate means software such as e-Wallet is required to be installed on the cardholder's computer. It is the barrier for the cardholder to use Certificate-based payment systems. To solve this problem, Visa Company has developed a new payment system called Verified by Visa (VbV) (http:www/visa-asia.com/ap/sea/merchants/productstech/vbv_implementvbv.shtml). However, sensitive information such as credit card number is still passed to the merchant. Therefore, the cardholder is not protected by the system.

Evaluation Factors

A successful credit card-based EPS should be simple, secure, and easy to use and has low deployment and maintenance cost. A set of evaluation criteria is described by Sahut (2005). Security is one of the important factors in identifying a good EPS. However, factors such as cost, convenience, ease of use, and so forth, must be also considered when designing a new EPS.

The new EPS must have a balance between security and convenience, especially on the cardholder side. This

article proposes a new payment system called simple and secure credit card-based payment system (SSC-CPS) which is a "cryptography free" and "certificate free" system.

Traditional Credit Card Payment Systems

Most credit card-based EPSs do not utilize on the traditional credit card payment infrastructure. Many credit card-based EPSs have been designed and developed but most of them, such as SET, have been poorly received by consumers. The main problem is that lots of requirements must be fulfilled by all participants, especially the cardholder. However, the complex or technical requirements to the cardholder will prevent the successful implementation of the system in the marketplace. For example, during the authentication process, the cardholder has to use a smart card reader, which is to be installed at home. In addition, software such as e-wallet and e-certificate has to be installed in the cardholder's computer. All the requirements act as barriers to the adoption of credit card-based EPSs. The objective of this article is to design a simple and secure credit card payment system which utilizes the existing infrastructure and minimizes the complex mechanism.

Traditional Payment Flow

The payment flow of the traditional transaction is shown in the Figure 1, and consists of five participants, including Issuer Bank, Acquirer Bank, Consumer, Merchant, and financial institution. The cardholder gives the credit card to the merchant cashier. The cashier swipes the credit card through an electric draft capture (EDC) or point of sale (POS) equipment and keys in the transaction amount. The EDC/POS dials a stored telephone number to call a gateway and sends the captured data to the acquirer bank. The acquirer bank constructs an ISO 8583 (Financial Transaction Card Orginated Messages) authorization request message and sends it to the issuer bank through tradition financial network. The issuer bank extracts the information from the authorization request message such as primary account number, expiration date, currency code, merchant type, transaction date time, and so forth, and goes through the local validation policies. The issuer bank constructs the authorization response message and sends it to the acquirer bank either approved or declined. The acquire bank forwards the response code to the merchant to complete the transaction.

There are many different types of financial messages defined in ISO 8583. Each type of message is composed of different data fields. The values in each data field may be redefined by individual credit card

Figure 1. The payment flow of traditional credit card payment system