Category: Applications of E-Technologies

Payment Mechanism of Mobile Agent-Based Restaurant Ordering System

Jon T. S. Quah
Nanyang Technological University, Singapore

Winnie C. H. Leow
Singapore Polytechnic, Singapore

Chee Chye Ong
Nanyang Technological University, Singapore

INTRODUCTION

The Internet, especially the World Wide Web, is moving from a free, academic domain to a profitable commercial world. This underscores the importance of a digitally secure means of electronic payment for an electronic commerce application. The payment is usually an important part of an electronic commerce transaction, and it deals with the transfer of trust, either as cryptographically signed promises, or as digital cash, between the customer, the merchant, and the payment service provider.

Due to the explosive growth of e-commerce transactions, many electronic modes of payment are devised to address a diverse set of Internet user requirements (Guida, Stahl, Bunt et al., 2004; Tsiakis & Sthephanides, 2005; Garfinkel, 2003; Usher, 2003; Polk, Hastings, & Malpani, 2003; Evans & Yen, 2005; Marchesini, Smith, & Zhao, 2005; Lancaster, Yen, & Huang, 2003; Lekkas, 2003; Medvinsky & Neuman, 1995; Schoenmakers, 1997; Levi & Koc, 2001; Mahony, Peirce, & Tewari, 2001; DigiCash Press, 1994; Neuman & Tso, 1994; Vivtek, 2000).

The background of this article is that we have developed a mobile agent-based restaurant reservation and ordering system whereby users are able to search for restaurants that fulfill a list of user-entered parameters (e.g., type of cuisines, ambiance, specialties such as steaks, etc.) (Quah & Leow, 2003). The system is built on the IBM Aglet mobile agent platform. (A mobile agent is a small executable code/program that can migrate itself to remote hosts and execute predefined instructions—e.g., information retrieval, and return the processed information to its originating host system) (Lanage & Oshima, 1998). Due to the uniqueness of our system, we find the existing e-commerce payment methods inadequate to fit our system's need. As such, we studied several existing methods and adapted one into our system operation structure. The use of mobile agent to implement the payment system adds robustness and scalability to the system.

DESCRIPTION OF THE ELECTRONIC PAYMENT SYSTEM

To support electronic commerce, various Internet payment protocols have been proposed and adopted by a variety of organizations. In fact, the existence of different payment mechanisms are justified because there are different needs to be satisfied in terms of:

- Cryptographic needs (strong, symmetric, exportable, importable, etc.)
- Latency of the transaction (micropayment must be very fast)
- Minimal and maximal amount for the transaction itself
- Minimal and maximal amount for the cost of the transaction
- Repudiation, notarization needs
- Involvement of financial institution (i.e., online vs. off-line)

Some of the above requirements may call for contradictory system requirements, and as such, trade-offs have to be made. In a nutshell, an electronic payment system should meet the following requirements:

1. Sufficient security means based on the amount of money transferred in a transaction.
2. Similar running scenario as the traditional business whenever possible to ease the doubts of the public and encourage them to participate.
3. Minimum changes on the current financial system to avoid tremendous costs when electronic commerce is introduced.

The participants of an electronic commerce transaction must be able to exchange trade and payment information over a network. The implementation addresses the problem of online payment by credit card in which anyone

with knowledge of the customer's credit card number can create an order for payment. It also tries to eliminate the requirement of a Certificate Authority (CA), and consequently a CA-based Public Key Infrastructure (PKI), in order to verify a public key-based digital signature.

Characteristics of the Mobile Agent-Based Restaurant Order Payment System

Secure Socket Layer- (SSL) (Rainbow Technologies, 2001; Freier, Karlton, & Kocher, 1996; Albrecht, 1998) based protocols used in credit card payment are convenient but have some authentication and non-repudiation problems. Secure Electronic Transaction standard (SET) (MasterCard, 1997) and other payment-card-based protocols, which require either intermediary agents or CA-based PKI, are secure, but not so convenient, particularly for financial institutions (FIs). The mechanism of our implementation tries to find a middle ground in the "security vs. convenience" trade-off.

In our payment mechanism implementation, both the customer and the merchant need to be registered off-line with a network payment service (or trusted party) with their credit card data and given a unique persona. This persona acts as a mapping between an identified user and that user's public key and credit card information stored in the trusted third-party system. The trusted third party then acts as an intermediary in collaborating with the customer's issuing bank and the merchant's acquiring bank in the settlement of the credit card bill.

The basic idea behind the mobile agent-based restaurant order payment system is to avoid the necessity of consumer certificates. It also provides a remedy to the inability of the traditional credit card payment system in authenticating the customer's identity. The trusted third party makes use of the stored public key to authenticate the identity of the customer and merchant. Only signed payment request from the customer and an order endorsed by the merchant can effect the payment. The merchant verifies the digital signature of the consumer in most of the electronic payment protocols. In our payment scheme, the trusted third party is the authority who verifies the consumer's digital signature.

The payment system serves like a credit card system without the online authorization with the issuing bank. This payment method does not require changing the existing credit card settlement infrastructure tremendously to adopt this scheme. Another important characteristic of the system is that messages transmitted among the consumer, merchant, and trusted third party are not encrypted. Justifications for this challenging characteristic are as follows:

1. The persona is not valid unless there is an accompanying digital signature issued by its owner. Any third party cannot take advantage of knowing the persona, since it cannot produce a digital signature. Thus, personas need not be encrypted.
2. The strong public private key authentication is sufficient to prevent the majority of consumer and merchant frauds. Using the persona concept and strong authentication make encryption a luxury in this payment system.

Mobile Agent-Based Payment Protocol

A payment protocol based on mobile agents is devised to structure the interactions and information exchange among agents to complete a payment transaction. The payment structure integrates the use of public key cryptography into the mobile agent framework for enhancing security in electronic payment.

The payment protocol consists of the following steps, as shown in Figure 1:

- CC—Consumer
- TTP—Trusted third party
- Mer—Merchant
- SigCC—Consumer's signature of payment data and order information
- SigMer—Merchant's signature of order information

1. Having decided the food to order, the consumer clicks on the "Pay" button at the Aglet Service center. The ASC launches the consumer aglet that carries the payment request which most importantly contains the merchant's persona and the payment amount.
2. At the merchant site, the consumer aglet passes the payment request to the merchant aglet. The merchant aglet carries the consumer's payment request with its own signature of the order and dispatches to the TTP site.

   Consumer payment request:
   Consumer persona, [payment data, H(Order)], SigCC

   Merchant signature of the order:
   Merchant persona, [H(Order)], SigMer

3. At the TTP site, the merchant aglet passes the consumer's payment request and merchant's signature of the order to the TTP aglet. The TTP aglet verifies the consumer's signature on the payment request and the merchant's signature on the order.