MicPay: Micropayments for Correlated Payments

Holger Petersen[1], Markus Michels[1], Daniel Som[1], George Fankhauser[2], David Schweikert[2], Burkhard Stiller[2], Nathalie Weiler[2], Renato Cantini[3], Felix Baessler[3], Dimitri Konstantas[4], Jean-Henry Morin[4]

1 Entrust Technologies Europe, Glatt Tower, Zürich-Glattzentrum
2 Computer Engineering and Networks Laboratory TIK, Swiss Federal Institute of Technology ETH Zürich
3 Swisscom Corporate Technology, Berne
4 Centre Universitaire Informatique (CUI), University of Geneva

Aims of the project

Cash is the best suited conventional payment instrument for low-value transactions.

Nevertheless, versatile as it is, it is limited in that no transaction can involve less than the value of the smallest coin (e.g. one cent). This poses a problem in a number of classes of goods and services where the value of the transaction is less than the smallest coin, like for example obtaining a single quotation for the current price of a share on the stock market or purchasing an isolated article from a newspaper. In conventional commerce, the solution to this is to use a subscription model for payment, where the buyer pays in advance a lump sum for accessing a large collection of low value items.

Although in the electronic commerce world the subscription model ensures that the content provider is paid for his services, this model does not address a large customer base of people who may only wish to use a service very occasionally. It also restricts the ability of people to try out a service. Thus it is clear that the subscription model does not adequately solve the problem of low value transactions in electronic commerce and that there is a need for a payment system that can efficiently transfer very small amounts, less than a cent, in a single transaction.

The first issue in the design of such a system is that communication, which itself costs money, must be kept to an absolute minimum. A system where the costs of conveying payment are greater than the payment itself is unlikely to succeed. A second issue stems from the fact that the low value per transaction means that the profit made on each transaction is small. Thus the server providing the required support must be able to process transactions at a high rate in order for the service to be viable. This gives rise to a further requirement, that micro-payment systems must be able to make the payment verification in an inexpensive way. Consequently a successful micro-payment system must not involve computationally expensive cryptographic techniques. In particular, emerging Internet based applications such as Internet telephony or distribution/purchase of electronic documents demand for a convenient, efficient payment method. The goal of the MicPay project is to design a smart card based solution for such small payments (in the order of magnitude of several cents) and to apply it to two application scenarios: continuous online charging for an Internet telephone call (IPPhone) and consecutive payment for a set of articles (HyperNews).

Key Results

The basic design of two micro-payment schemes applicable to the two application scenarios has been performed. For the IPPhone application a hash-chain based micro-payment scheme has been developed where the identities of all service providers are included in the root of the chain. That makes the cashing of the hash-chain easy and avoids fraud among the service providers. The protocol has been implemented on a JavaCard, which was one of the first commercially available JavaCards providing the necessary cryptographic functionality. For the IP Phone demonstrator, the Resource Reservation Protocol RSVP (RFC 2205) has been extended for carrying such hash chain payment information. The core extensions of RSVP for payments have been implemented in Java in order to integrate the needed micro-payment objects of the specified payment scheme. A first prototype illustrates the feasibility of the chosen approach: it allows for high audio quality IP telephony calls with a guaranteed bandwidth, if the user is willing to pay for his call, and in turn, the reserved network resources.

For the HyperNews application a balance based micro-payment scheme was developed, where the payment is combined with some operations inherent to that scenario, i.e., the decryption of encrypted article key. During off-line payment, the money is transferred from the purse into internal card slots, that represent the credits of different information providers (IPs). The slots are cleared with the bank before the next loading of money to the card. The bank is responsible for distributing the money to the IPs accordingly. The HyperNews demonstrator illustrates the off-line purchase of electronic articles using smart card based access control and payments. In particular, it is shown how the user can download encrypted articles from an Information Provider, including the unencrypted title and an abstract and can choose which article to purchase. The card controls the user's access to the full article after he has paid for it and also provides a receipt as proof of purchase. The receipt allows re-reading of already paid articles by the same user.

Technology and Know-How Transfer

The close cooperation with the SPP project CATI (Charging and Accounting Technology for the Internet) offered the possibility to apply the designed and implemented micro-payment protocol in a real world Internet telephony demonstrator. The cooperation with the SPP project HyperNews offered the ability to apply the micro-payment scheme to an existing E-Business application.

The outcome of the project could be applied to design and implement value cards for supporting the HyperNews and IP Phone applications. In particular, the results achieved with the design of payment and charging extensions for protocols will be utilized in the M3I project that is part of the European Union's Fifth RTD Framework Program.

The HyperNews application is being considered for access control use in a large privately founded project by the "Association pour le Bien des Aveugles (ABA)".

The combined payment and access control mechanism used in the HyperNews application is a basic technology for the planned ElCom 2000 "StreamCom" project, which deals with encrypted data streams (like digital video).

Contact

For more information, please contact Dr. Holger Petersen, Entrust Technologies Europe/ r^3 security engineering ag, Glatt Tower, 6.Floor, 8301 Glattzentrum.