Anonymous and Fair Micropayment Scheme with Protection against Coupon Theft

Andreu Pere Isern-Deyà, Department of Mathematics and Computer Science, Universitat de les Illes Balears, Palma, Spain

M. Magdalena Payeras-Capellà, Department of Mathematics and Computer Science, Universitat de les Illes Balears, Palma, Spain

Macià Mut-Puigserver, Department of Mathematics and Computer Science, Universitat de les Illes Balears, Palma, Spain

Josep L. Ferrer-Gomila, Department of Mathematics and Computer Science, Universitat de les Illes Balears, Palma, Spain

ABSTRACT

The development of new applications of electronic commerce (e-commerce) that require the payment of small amounts of money to purchase services or goods opens new challenges in the security and privacy fields. These payments are called micropayments and they provide a trade-off between efficiency and security requirements to pay low-value items. It is usual to assume low value fraud to achieve efficiency in micropayment systems. In this paper the authors present an improved version of an efficient and secure micropayment scheme which fulfils the security properties that guarantee no financial risk for merchants and the privacy of the customers. In addition, the proposed system defines a fair exchange between the coin and the desired good or service. In this fair exchange, the anonymity and untraceability of the customers are assured. Moreover, customers can request a refund whether they are no more interested on the services offered by merchants. As a novelty, an improvement of the scheme avoids customers to fraudulently use a refund operation to gain a little amount of money (called coupon). Thus, a new resolution subprotocol allows the merchant to avoid the loss of any single coupon.

Keywords: Anonymity, Fairness, Financial Risks, Micropayment, Privacy, Untraceability

INTRODUCTION

The field of electronic commerce (e-commerce) evolves day by day introducing new applications and services. One of these applications is the payment of small amounts of money to purchase low cost services or goods. This kind of payments is called micropayment and they have unique functional and security requirements inside the field of electronic payments. Here, a micropayment should offer advantages in contrast with other payment methods that tend to be costly because they are mainly designed for managing larger amounts of money. Therefore,
micropayments can easily be applied to the intangible selling of goods such as information (newspapers, product reviews, location-based services, etc.), virtual gifts or electronic data (music, videos, etc). All of these examples involve low-value transactions, so the operational cost has to be as low as possible in order to be profitable for merchants and customers.

On one hand, security properties are a primary concern for the development of micropayment systems to avoid financial risks for merchants and also to ensure privacy for customers. On the other hand, efficiency and the cost for individual transactions are critical factors for the development of these systems. However, efficiency and security are usually opposed, so micropayments must provide a trade-off between these requirements:

- **Contribution.** In Isern-Deyà et al. (2011) we proposed a novel, efficient and secure micropayment scheme to pay low value items assuring privacy for customers. In this paper we propose an improved version of the protocol. The system uses anonymous and untraceable coins which are used in a fair exchange between customers and merchants to pay the desired good or service. The system detects and avoids double-spending and overspending, protects from forgeability and moreover allows customers to request a secure refund for partially used or unused coins. Moreover, now the customers cannot use the refund subprotocol to fraudulently refund a single spent coupon. We have added a new resolution subprotocol that allows the merchant to deposit the received coupons even when the customers are trying to cheat, avoiding the loss of money, including very small amounts;

- **Organization.** The work is organized as follows. First we briefly describe the features and security requirements of micropayments. Next section surveys the related work. Following section summarizes the cryptographic background used in our scheme. Then we define the micropayment protocol. In the following section we present a security overview of the protocol. Finally, the work includes the conclusions and future works.

### MICROPAYMENTS SCHEMES OVERVIEW

In this section we list the involved parties and the common protocols in the micropayment model (Papaefstathiou et al., 2004; Poutanen et al., 1998; Schmidt et al., 1999). Moreover, we also enumerate and define the security requirements and functional features of an ideal micropayment system (Lipton et al., 1998; Papaefstathiou et al., 2004; Poutanen et al., 1998; Schmidt et al., 1999).

#### Involved Parties and Common Protocols

The typical involved parties in a micropayment scheme are:

- **Customer.** The party who wants to buy a good or service;
- **Merchant.** The party who wants to sell a good or service;
- **Broker or Bank.** The party who issues coins and manages payment accounts.

So, the common model consists of a customer who withdraws a coin from his broker account (withdrawal or issuing procedure) in order to purchase (payment, spend or transaction procedure) a good or electronic service (henceforth service) offered by a merchant. Finally, the merchant can request a deposit (refund procedure) in his broker account in exchange of a received coin from customer.

#### Security Requirements

An ideal micropayment system should accomplish a list of security requirements and functional features which are depicted below (Poutanen et al., 1998; Schmidt et al., 1999):
Engineering and Reengineering of Technology Enhanced Learning Scenarios Using Context Awareness Processes
[www.igi-global.com/chapter/engineering-reengineering-technology-enhanced-learning/56071?camid=4v1a](www.igi-global.com/chapter/engineering-reengineering-technology-enhanced-learning/56071?camid=4v1a)