Available online at www.sciencedirect.com
ScienceDirect
Electronic Commerce Research and Applications 6 (2007) 91–101
Electronic Commerce Research and Applications
www.elsevier.com/locate/ecra

NetPay: An off-line, decentralized micro-payment system for thin-client applications

Xiaoling Dai [a,*], John Grundy [b,c]

[a] Department of Mathematics and Computing Science, The University of the South Pacific, Laucala Campus, P.O. Box 1168, Suva, Fiji
[b] Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand
[c] Department of Electrical and Electronic Engineering, University of Auckland, Private Bag 92019, Auckland, New Zealand

Received 23 October 2004; received in revised form 22 July 2005; accepted 31 October 2005
Available online 7 March 2006

Abstract

Micro-payment systems have become popular in recent times as the desire to support low-value, high-volume transactions of text, music, clip-art, video and other media has increased. We describe NetPay, a micro-payment system characterized by de-centralized, off-line processing, customer anonymity and relatively high performance and security using one-way hashing functions for encryption. We describe the motivation for NetPay and its basic protocol, describe a software architecture and two NetPay prototypes we have developed, and report the results of several evaluations of these prototypes.

Keywords: Electronic commerce; Micro-payment; Software architecture; Electronic wallet

1. Introduction

Current macro-payment systems used by most e-commerce sites are not suitable for high-volume, low-cost transactions, such as charging on a per-page basis for web site browsing. These macro-payment payment technologies suffer from use of heavy-weight encryption technologies and reliance on always on-line and slow-response authorization servers. Micro-payment systems offer an alternative strategy of pay-as-you-go charging, even for very low cost, very high-volume charging. There are a variety of micro-payment systems, such as Payfair [25], Millicent [19], Mpay [11], e-coupons [22] and PayWord [24]. Most existing micro-payment technologies proposed or prototyped to date suffer from limitations with communication, security, and lack of anonymity or being vendor-specific.

To address these we issues we have developed a new micro-payment protocol called NetPay to address these problems [4]. NetPay uses "electronic coins" (e-coins) encoded as a "payword chain" of elements encrypted by fast one-way hash functions. The NetPay protocol shifts the communication traffic bottleneck from a broker and distributes it among the vendors by using transferable e-coin Touchstones and Indexes. Customers are prevented from double spending as the index of the payword chain indicates the balance of the customer's e-wallet, and the touchstone can be used to verify the payword chain has not been tampered with [1].

In this paper, we give an overview of existing micro-payment approaches and briefly discuss the limitations of these models. We present the NetPay micro-payment model and an architecture we have been developing to realize NetPay-based e-commerce systems. We describe a design and prototype implementation of NetPay for deployment with thin-client vendor user interfaces for customers. We describe two example applications which include NetPay micro-payment support, a purpose-built e-newspaper and a pre-existing component-based e-jour-

* Corresponding author.
E-mail addresses: dai_s@usp.ac.fj (X. Dai), john-g@cs.auckland.ac.nz (J. Grundy).

1567-4223/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2005.10.009

nal web site. Both use NetPay support to sell content on a per-page usage basis. Our protocol is compared with previous micro-payment protocols and we describe three kinds of evaluations we have conducted on our prototypes. We conclude with an outline of our further plans for research in this area.

2. Motivation

Consider a customer browsing an electronic journal site. To access content the customer typically logs in, identifying themselves, searches for articles of interest, and browses and/or downloads the articles to print or read off-line. In a similar manner, customers browsing electronic news provider sites will typically browse headline pages and select articles of interest to view. Many journal and newspaper sites once provided such content for free, or relied on only revenue from on-line, paid advertisements. However, due to the need to recover costs for providing such services, more and more content providers are switching from once free content or services to a paid subscription model or a "pay-per-click" model [10,19,23]. Some existing e-newspapers and e-journals provide free content with embedded advertisements for revenue, while others require subscription to typically all of the newspaper content. Some even provide a printed hard copy in addition to the electronic one. Other forms of emerging on-line content provision include purchase of music and video clips, clip art, stock market and other financial data, and so on [12,18,20,21]. For example, on-line music can be downloaded as a single at a time from an on-line music site by paying small amounts of money per single. There is also a multitude of game sites [2] using a small fee-per-play charging model, and various clip-media services where customers can purchase graphics, audio, and video online [17].

Many "free" content sites currently use intrusive embedded advertising for revenue, which are often annoying to customers, and the revenue for the vendor very difficult to predict. Alternatively where a subscription model is used, the large up front cost can prove a great deterrent to potential customers. It can also be inefficient if the customer actually wants to use a small portion of the information or services for which they have paid. Payment on a per-click basis using traditional macro-payment (e.g., credit card or digital cash) schemes is infeasible due to cost and performance overheads of using slow response authorization servers. An alternative is to use micro-payment systems. In the above scenarios a customer could find and download an article, song or clip-art and only pay a small amount of money e.g., 1c, 2c, 10c or 20c on a pay-per-use basis. Key requirements for such micro-payment systems are generally agreed to be [9,11,13,24]:

- Ease of use for customers, ideally requiring nothing but point-and-click to purchase.
- Security of the electronic coins ("e-coins") from both fraud and double-spending by customers.
- Ideally anonymous like traditional cash – the vendor has no idea who the customer is.
- Vendor-transferable e-coins allowing customers to buy coins from a broker and spend at many different e-commerce sites.
- Off-line processing of payments, i.e., no on-line bank authorization server needed by vendor or client during payment processing, and highly scalable architecture to support very large numbers of clients concurrently using a vendor site with low-impact on vendor site efficiency.

The area of micro-payment on the Internet has attracted much research over the past 10 years. *Millicent*, a micro-payment system by Digital Equipment Corp [19] uses no public-key cryptography and is optimized for repeated micro-payments to the same vendor. Its distributed approach allows a payment to be validated, and double spending prevented without the overhead of contacting the broker on-line during purchase. Key drawbacks are that the broker must be on-line whenever the customer wishes to interact with the new vendor; the customer must nearly always be able to connect to the broker in order to be sure of the ability to make payments; and the vendor scrip is vendor-specific and has no value to another vendor. The *Mpay* micro-payment system was proposed by IBM [11] and is similar to billing mechanisms of third party value-added services of phone networks. Mpay is based on a notational model and has off-line capability in its daily certificate. Mpay only uses one or no public key operation per purchase, so the transaction cost is low. The major shortcoming of the system is that the customer can pay nothing to the issuer who still needs to pay the bank after purchasing goods. Furthermore, the protocol does not support anonymity for customers due to Mpay's after-the-fact policing requirements.

Several micro-payment systems have been developed that are based on a Payword-based micro-payment protocol. These systems can be classified as credit-based and debit-based. Payword [24] is an off-line credit-based system. The customer only needs to contact the broker at the beginning of each certificate lifetime in order to obtain a new-signed certificate. The system aims to minimize the number of public key operations required per payment using hash operations instead whenever possible. It is a credit-based scheme where a user's account is not debited until some time after purchases. This provides more opportunities for fraud since a large number of purchases can be made against an account with insufficient funds. PayFair [26] is a debit-based micro-payment system that employs some parts of the Payword scheme. A payword chain purchased from the broker will be bound to a specific vendor. NMP [15] is a credit-based protocol that improves the fairness for customers from the Payword protocol. The Payword-based micro-payment systems described above share a key disadvantage – they are all vendor specific. The e-coins (paywords) in these systems are only usable