Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

ELSEVIER

Electronic Commerce Research and Applications 3 (2004) 381–388

Electronic Commerce Research and Applications

www.elsevier.com/locate/ecra

PayCash: a secure efficient internet payment system

Jon M. Peha *, Ildar M. Khamitov

Carnegie Mellon University, Pittsburgh, PA, USA

Received 3 October 2003; received in revised form 4 June 2004; accepted 28 June 2004
Available online 23 July 2004

Abstract

This paper describes PayCash, an Internet payment system that was designed to offer strong security and privacy protection. This system is based on the concept of electronic cash, extended to support a flexible anonymity policy so as to accommodate privacy and security laws that differ from nation to nation. PayCash includes novel techniques to generate trustworthy records of all transactions, making it possible to detect many forms of fraud. This system also allows users to send a variable number of "electronic coins" in a single message, so both large and small amounts of money can be transferred efficiently.

Keywords: Payment system; Electronic cash; Privacy; Security

1. Introduction

Despite the many inherent security risks of the Internet, it has become an essential tool for commerce and financial services. This has created a tremendous need for secure and efficient payment systems that can operate over unsecure networks. Today's payment systems routinely undermine the security and privacy of their users. Moreover, many consumers are unable to perform transactions over the Internet at all because they lack access to computer technology, suitable financial instruments, or both. This paper describes Cyphermint's novel and effective new payment system called *PayCash*, which has quickly emerged as the leading Internet payment system in five nations of eastern Europe, and has begun expansion to top e-commerce merchants in the US [4]. Its uses include business-to-consumer electronic commerce, peer-to-peer funds transfers among consumers and among businesses, and transfers from one agent of a licensed international funds transfer company to another.

* Corresponding author. Chief Technical Officer at Cyphermint Inc., Professor at Carnegie Mellon University (CMU), and Associate Director of the CMU Center for Wireless and Broadband Networks. Address: Department of ECE, Carnegie Mellon University, Pittsburgh, PA 15213, USA.
E-mail address: peha@cmu.edu (J.M. Peha).
URL: http://www.ece.cmu.edu/~peha.

1567-4223/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2004.06.001

PayCash uses novel algorithms to advance traditional objectives of Internet payment system design, such as security, privacy, and efficiency. More specifically, this system creates verifiable records of all transactions that cannot be forged or undetectably altered by the party sending funds, the party receiving funds, or even by the operator of the payment system. Such records are essential to protect all parties from many forms of fraud [10,11]. Moreover, this is accomplished without sacrificing privacy of either sender or receiver, and without imposing a heavy processing burden on the payment system's servers. However, advancing these traditional objectives is not enough. An effective payment system must be consistent with laws and policies of all nations where it operates, which requires that some flexibility on issues of privacy and security be built into the technology. Not only do the laws vary from nation to nation, but in the US, policies have changed to address new security concerns in the wake of the September 11, 2001 attacks. The PayCash design has evolved accordingly.

Section 2 briefly addresses the state of payment systems today. Section 3 discusses the design objectives for a new payment system. Section 4 presents an overview of the electronic cash approach originally proposed by Chaum [2]. Section 5 presents Paycash, which builds on the electronic cash concept, with significant extensions to achieve the design objectives from Section 3. Finally, the paper is summarized in Section 6.

2. The status quo

Today, many financial transactions use mechanisms that offer little security or privacy protection, such as credit cards or simple password schemes. Most on-line purchases use credit cards. In the process, consumers often reveal credit card numbers and personal information to unknown merchants, and often to anybody who cares enough to watch the traffic pass from consumer to merchant over the Internet or through an exposed wireless connection. Anyone observing credit card information can use it to make additional purchases. It is no wonder that fraud and identity theft are rising at a tremendous rate [5]. Even if they are not victims of fraud or theft, consumers who reveal personal information compromise their own privacy, and may be rewarded with an avalanche of spam and telemarketer calls. In addition, many banks, merchants, and payment systems allow their customers to log in over the Internet to access personal information and initiate financial transactions. Such sites are often "protected" with passwords. Thieves can access a significant fraction of these sites using password-guessing software that is readily available over the Internet.

Security problems aside, many consumers cannot enjoy the e-commerce opportunities because they have no credit cards. Transaction costs are also an issue. For example, the market for inexpensive digital products, such as individual magazine articles or digitized songs, has been slow to emerge in part because the cost of transferring a payment can exceed the cost of the product itself. International funds transfers are particularly expensive, as anyone who has made a wire transfer knows. Most international money transfer companies have not yet reaped the benefits of secure Internet payment systems.

3. Design goals for an effective payment system

To protect security and privacy, PayCash was designed to achieve the following:

- *Tamper-proof records.* As described in Section 1, every financial transaction must produce a record that cannot be undetectably altered by sender, receiver, or operators of the payment system. In Paycash, digitally signed records are a byproduct of transactions, so trust among these parties is not required.
- *Privacy protection.* To protect privacy and combat identity theft in e-commerce, consumers must be able to send funds without revealing any personal information to the recipient, and receive funds without revealing information (other than an account number) to the sender. They reveal only what they choose to reveal.