International Journal of Innovative Computing, Information and Control
Volume **5**, Number **9**, September **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 2881–2891

AN AUTHENTICATED PAYWORD SCHEME WITHOUT PUBLIC KEY CRYPTOSYSTEMS

Chia-Chi Wu[1], Chin-Chen Chang[2] and Iuon-Chang Lin[3,*]

[1]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi, Taiwan

[2]Department of Information Engineering and Computer Science
Feng Chia University
Taichung, Taiwan

[3]Department of Management Information Systems
National Chung Hsing University
250 Kuo-Kuang Rd. Taichung, 402 Taiwan
*Corresponding author: iclin@nchu.edu.tw

Received April 2008; revised September 2008

Abstract. *Rivest and Shamir proposed a PayWord scheme in 1996 that is an efficient micro-payment scheme using a one-way hash chain. However, Adachi et al. thought that Rivest and Shamir's PayWord scheme suffered from a vulnerability to credit abuse attack and bank falsification attack. Therefore, they proposed an improved version to prevent these attacks in 2005. Unfortunately, there are still some drawbacks. First, the efficiency is degraded because the improved version using a public key cryptosystem. Second, it is vulnerable to an unauthorized settlement attack because it does not satisfy the requirement of authentication. Third, they change the PayWord scheme from a postpaid to a prepaid payment method. It is not practical because it is good for the vendor but is not fair to the customer. In this paper, we propose an authenticated PayWord scheme to eliminate these drawbacks and enhance the performance. Our scheme does not require a public key cryptosystem and the customer's rights can be assured.*

Keywords: Hash chain, Key agreement, Micro-payment, PayWord

1. Introduction.

Nowadays, electronic commerce is very flourishing over the internet. To achieve payment security, many payment schemes have been proposed to perform online payment procedures, such as E-cash [4], Millicent [6], PayWord [15], NetBill [3] SET [17], WebMoney [19] and so on.

Generally, electronic transactions can be divided into two main categories, the sale of tangible goods and the sale of non-tangible goods. If the sale is the tangible goods, it usually requires relatively large payments. Therefore, vendors have to assure the customers that the transaction is secure. Security is the main requirement for this kind of transaction. However, if the sale is the non-tangible goods such as pay TV programs, music, on-line games, electronic books and so on, the main factors in such transactions are relatively small payments and the transactions occur frequently. Thus, performance is the main requirement for this kind of payment system. Consequently, the payment system has to minimize the transaction cost and it must be lower than the value of the payment. This kind of payment scheme is called micro-payment.

According to the draft of the World Wide Web Consortium's (W3C) Micro Payment Transfer Protocol (MPTP) [20], they stipulate that the micro-payment transfer protocol must consider related security risks as follows.