Electronic Commerce Research and Applications 10 (2011) 279–287

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

A fair online payment system for digital content via subliminal channel

Chin-Ling Chen [a,*], Jyun-Jie Liao [b]

[a] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan, ROC
[b] Department of Computer Science and Engineering, National Chung-Hsing University, 250 Kuo-Kwang Road, Taichung 40227, Taiwan, ROC

ARTICLE INFO

Article history:
Received 25 February 2010
Received in revised form 11 September 2010
Accepted 11 September 2010
Available online 17 September 2010

Keywords:
Subliminal channel
Payment system
Online
Digital content

ABSTRACT

In recent years, purchase of digital content using the Internet has been increasing both in popularity and convenience. On the other hand, there are a multitude of pirated editions for digital products which have become more available and easier to attain. Therefore, proving legal ownership of digital content has become important. Many researchers have proposed various schemes to protect consumer's ownership using watermark mechanisms on secure payment systems. In our scheme, we want to achieve this same result with the concept of subliminal channels and propose an intact arbitration mechanism to solve the fairness of the transaction between both the customer and the shop. Our scheme not only protects customers' legal ownership of digital content, but also provides a fair and secure protocol.

1. Introduction

In recent years, more and more people have been purchasing digital content over the Internet. We believe the number of e-commerce digital content transactions will grow tremendously. Therefore, better security and well-designed electronic payment schemes become an important issue for digital content over the Internet.

Generally, the electronic payment system involves four parties: customer, shop, bank, and trusted third party (TTP). Many E-cash schemes have been proposed to solve the problem of the withdrawal, payment and deposit (Chan and Chang 2006, Fan et al. 2006, Hou and Tan 2005, Kaufman et al. 2002, Wang et al. 2005, 2009). To ensure a fair transaction and prevent one of the participating entities in the transaction from refusing to fulfill their duty, fair payment protocols (Franklin and Reiter 1997, Zhou and Gollman 1996) aiming to take this approach often use a TTP to resolve the transaction. In fact, the TTP does not exist in real life. Most recent papers avoid the use of TTP in the transaction as much as possible, but ensure it is available to resolve disputes (Lin and Liu 2009).

In real life, when customers purchase digital content such as images, audio, and video using the Internet, they may be suspected of possessing illegal digital content. However, it is hard for these customers to prove they are the real owner of the digital content. So, our aim is to provide a method whereby the customer can prove he or she is in fact the legal owner. Therefore, customers should provide a legal message after they purchase digital content. The customer can provide the arbiter with a verifiable message when suspected of having illegal content. This message will provide proof so the arbiter can determine whether the customer is a legal owner.

Traditionally, ownership or copyright protections of digital content usually use the watermark insertion mechanism (Deng and Preneel 2008, Fan et al. 2009, Ibrahim et al. 2007, Katzenbeisser et al. 2008). However, the watermark insertion/extraction algorithm causes "loss of data compression" and "reduced quality" for digital content. In 1983, Simmons proposed the first concept of the subliminal channel (Simmons 1983, 1985, 1993, 1998). A subliminal channel is a covert signal provided with communication that can be used to send a subliminal message to the designated receiver, but the message cannot be recognized by any undesignated receiver. Toward the application of this concept, many researchers have proposed protocols for the subliminal channel (Chen and Liu 2009, Huang et al. 2005, Lee and Ho 2003). Using such a concept, our scheme will embed the digital content with a subliminal message to protect the customer's ownership. The proposed secure online payment system has the following characteristics:

- Customer cannot replay the same message to pass payment.
- Any forgery is not possible.
- Prevention of a DOS attack.
- Prevention of a man-in-the-middle attack.
- Anonymity.
- The fairness of the payment process.

* Corresponding author. Tel.: +886 4 23323000x4761; fax: +886 4 23742375.
E-mail addresses: chn1211@ms6.hinet.net (C.-L. Chen), s9756005@cs.nchu.edu.tw (J.-J. Liao).

1567-4223/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2010.09.001

- The digital signature is the proof of non-repudiation.
- Piracy is traceable.

According to the above requirements, we use the subliminal channel, Nyberg–Rueppel scheme, one-way hash function and Schnorr signature scheme to implement a fair online payment system for digital content. The remaining parts of this paper are organized as follows. Section 2 introduces the cryptographic techniques used in our scheme. Section 3 presents our proposed protocol, while the security issues are analyzed and discussions are made in Sections 4 and 5 concludes this paper.

2. Preliminaries

In this section, we introduce three cryptographic techniques used in our proposed scheme: Nyberg–Rueppel scheme, Schnorr signature and one-way hash function.

2.1. Nyberg–Rueppel scheme

In 1993, Nyberg and Rueppel provided a signature scheme (Nyberg and Rueppel 1993) which could be used for message recovery. The system parameters consist of primes p and q such that $q|(p-1)$ and an element $g \in Z_p$ with order q. A user generates a private key x_k and a corresponding public key y_k, i.e., $y_k = g^{x_k} \bmod p$. To sign a message $m \in Z_p$, the signer selects $k \in Z_p$ at random and computes r ($r = mg^k \ mod \ p$) and s ($s = x_K r + k \ mod \ q$). The pair (r,s) is the signature of the message m. To verify the validity of a signature, one checks whether the $m = g^{-s} \cdot y_k^r \cdot r \bmod p$ equality holds.

2.2. One-way hash function

A one-way hash function $H(\cdot)$ is a transformation taking an input x and returning a fixed-size string y. The basic requirements for a cryptographic one-way hash function (Menezes et al. 1997) are shown in the following:

(1) The input can be of any length.
(2) The output has a fixed length.
(3) Given x, it is relatively easy to compute $H(x)$.
(4) Given y, it is infeasible to compute x such that $y = H(x)$.
(5) It is hard to find x_1 and x_2 such that $H(x_1) = H(x_2)$.

2.3. Schnorr signature scheme

In 1991, Schnorr provided a signature scheme (Schnorr 1991) based on the discrete logarithm problem. The system parameters are the same as in the previous scheme. To sign a message m with the private key x_k, the user chooses a random number $u \in Z_q$, and then performs the following steps:

Step1: Computes $N = g^u \ mod \ p$.
Step2: Computes $r = H(N,m)$.
Step3: Computes $s = (u - x_K \cdot r) \ mod \ q$ and sends the signature (r,s).

To verify the signatures (r,s) for message m with the public key y_K, a verifier computes $r' = g^s \cdot y_k^r \ mod \ p$ and checks whether $r = H(r',m)$.

3. Our proposed scheme

In this section, we describe a payment scheme for the digital content using a subliminal channel to verify whether a customer is legal. The method consists of four phases: the open account phase, the withdrawal phase, the payment phase and the arbitration phase. In this paper, we assume the communication channel with the bank is secure (for example a secure socket layer (SSL) channel). The structure of our scheme is illustrated in Fig. 1, and there are four parties described as follows:

1. C → B : The customer opens an account in the bank.
2. C → B : The customer withdraws an E-cash from the bank before processing the transaction.
3. C → S : The customer sends the purchase messages to the shop.
4. S → B : After the shop sends the withdrawal message to the bank, the bank verifies whether the withdrawal message is valid and then responds to the shop.
5. S → C : The shop responds to the customer's purchases request.
6. C → A : If the customer does not receive digital content from the shop or he or she is suspected of possessing illegal digital content. The customer can send an arbitration request to the arbiter.

Details of these phases are shown in the following. First, the system parameters consist of primes p and q such that $q|(p-1)$ and an element $g \in Z_p$ with order q, i.e. $g^q = 1 (mod \ p)$, $g \neq 1$. The following notations are used in our scheme.

x_K, y_K	the private key and public key selected by K, where $x_K \in Z_p$ and $y_K = g^{x_K} \ mod \ p$
ID_K	the identity of the K
u_i	the ith random number, $u_i \in Z_q$
amount	the amount of digital content
V_i	the ith verification information
A_C	the customer's account
$H(\cdot)$	one-way hash function
C	the hash value of the withdrawal message
r	the withdrawal response message
T_K	the timestamp generated by K party, e.g.: shop or customer
AUC_{DC}	the authorized code of digital content
M	the digital content
M_{cs}	the subliminal message generated by the customer to prove is the owner of the digital content
M_W	the withdrawal message
$Cert_M$	the certification of digital content signed by the shop
$Y \ ? = Z$	compare whether Y is equal to Z
$Y \ ? \leqslant Z$	determine whether Y is less than or equal to Z
⟹	secure channel, for example secure socket layer (SSL) channel
⟶	insecure channel

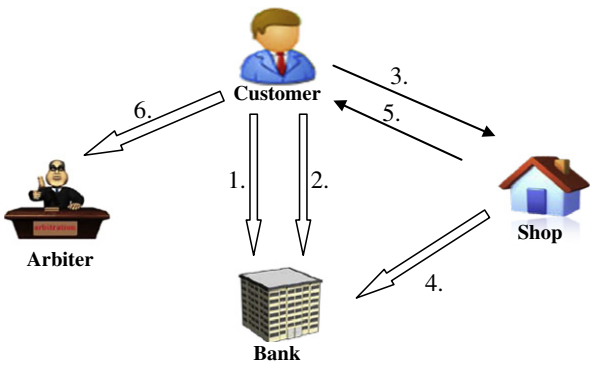

Fig. 1. Overview of the structure our scheme.