Secure E-payment Protocol

Sattar J Aboud sattar_aboud2yahoo.com
Information Technology Advisor
Iraqi Council of Representatives
Baghdad-Iraq

Abstract

The vast spreading of information in the last decade has led to great development in e-commerce. For instance, e-trade and e-bank are two main Internet services that implement e-transaction from anyplace in the world. This helps merchant and bank to ease the financial transaction process and to give user friendly services at any time. However, the cost of workers and communications falls down considerably while the cost of trusted authority and protecting information is increased. E-payment is now one of the most central research areas in e-commerce, mainly regarding online and offline payment scenarios. In this paper, we will discuss an important e-payment protocol namely Kim and Lee scheme examine its advantages and delimitations, which encourages the author to develop more efficient scheme that keeping all characteristics intact without concession of the security robustness of the protocol. The suggest protocol employs the idea of public key encryption scheme using the thought of hash chain. We will compare the proposed protocol with Kim and Lee protocol and demonstrate that the proposed protocol offers more security and efficiency, which makes the protocol workable for real world services.

Keywords: E-payment protocol, Public key cryptography, Signature scheme, Blind signature scheme, Over-spending, E-commerce

1. INTRODUCTION

With the increasing impact of intangible merchandise in worldwide economies and their immediate delivery at small cost, traditional payment systems tend to be more costly than the modern methods. Online processing can be worth of value smaller than the smallest value of money in the manual world. However, there are two methods of running e-payment systems.

1. Online payment: in which vendor checks the payment send by purchaser with a bank before serving the purchaser.
2. Offline payment: in which over spending must be detected, and consequently, no online link to the bank is needed.

The e-payment schemes [1] can be sub-divided into two groups according to the online assumptions.

1. Payments by transaction method: in which single payment does not need previous arrangements between purchaser and vendor.
2. Payments by account method: in which purchaser and vendor should have system account with bank and certain type of agreement between both before carrying out the real payment transaction.

The payment by transaction can further be divided into two subgroups.

1. The credit card payment transaction: is tailored for large charge payment of some hundreds or even thousands of dollars. In contrast, net money transaction is usually low value payment with difficult transaction cost and online features, similar to the thought of the e-payment transaction. The drawback of the credit card payment transaction is the fee of transactions, particularly from the perspective of the vendor that have to pay some invoices to the clearing house according to the contract agreement with them. This certainly will have straight impact on the cost policy and the interest between the possible users.
2. The e-payment by small value transactions on service: This is acquiring certain interest from the area of research. A number of important services of e-payment are e-publishing and multimedia service. In these services, due to the small transaction amount, the merchant acquires relatively shopping mall revenue from every transaction.

As a result, expensive calculations such as digital signature should be limited in order to reduce the investments in software applications. In the recent years, e-payments [2] [3] [4] [5] offering a relatively key improvement in the online revenue malls. The foundation of e-payments is to take benefit of the high level of viewers by present content for a low price. Other alternative of this thought is to rating fractions of cents for equally fractional contents sums. The main features in e-payment protocol are less charges of payment amount and high occurrence of transactions on the e-commerce system.

2. E-PAYMENT PROTOCOL REQUIREMENTS

The e-payment protocol encompasses three participants

1. User: The user (customer) purchases e-currency from the bank employing actual money by e-payment. The user can then utilize e-currency to carry out e-payment to buy goods.
2. Merchant: The merchant is the data storage which provides user with both services and information.
3. Bank: The bank is the trusted authority. It mediates between user and merchant in order to ease the duties they carry out. In general, the bank acts like a broker offers the e-coins for the e-payments.

While using e-currency, a shared set of characteristics for an e-payment protocol is:

1. Anonymity: e-cash must not supply any user with information; it means that it must be anonymous e-currency transaction.
2. Divisibility: e-cash can be sub-divided since the notes have a basic piece.
3. Transference: e-cash can be transferred to a trusted authority by providing the suitable amount of currency.
4. Over spending detection: e-cash must be used for only once.

The e-payments are stored and then converted to digital type. This will cause new difficulties during the developing secure e-payment protocol. The payment is simply be duplicated against the conventional physical paying methods. As the digital payment is characterized as simple sequences of bits, nothing in them stops them copying. When a security of the payment protocol is reliant on the method the payments are hidden from unknown. Every individual that can have access to payments maybe utilize them numerous times. We notice that getting anonymous cash transaction is an essential issue, and at the same time giving efficiency is another matter. In this paper, we study a merchant Kim and Lee [6]; that gives anonymity characteristic using the idea of blind signature scheme and hash chain. We then proposed a blind signature scheme that will be used in the protocol for reaching better efficiency without concession its security characteristics. Therefore, before discussion the rest of this paper, we will list the notation used.

U :	User
M :	Merchant
B :	Bank
ID_E :	Identity of entity E , such that $E \in \{U, M, B\}$

A_E :	Address of entity E
m :	Message
$\oplus$:	XOR
PK_E :	Public key of entity E
SK_E :	Private Key of entity E
K :	Secret key of bank B
P :	A generator point on elliptic curve
r_E :	Arbitrary number selected by entity E
C_U :	User certificate
CE_U :	User certificate expiry information
I_U :	User certificate serial number credit card information
OI :	Order information (category, amount, etc)
EI_R :	Expiry information for redemption
h :	Secure hash function
$\|\|$:	Concatenation

3. RELATED WORKS

In 1988 Chaum, Fiat and Naor proposed their protocol entitled untraceable electronic cash [7] which is relied on a single use token method. The user creates blinded e-bank currency note and passes it to the bank to be signed using bank public key. The bank signs the currency note, subtracts the value from the user account, and returns the signed currency note back to the user. The user removes the blind thing and utilizes it to buy goods from the super market. The super market checks the authenticity of the bank currency note using the bank public key and passes it to the bank where they are verified contrary to a list of currency note already used. The amount is deposited into the supermarket account, the deposit approved, and the supermarket in turn emits the merchandise. In 1995, Glassman, Manasse, Abadi, Gauthier and Sobalvarro present their protocol entitled "The Millicent protocol for inexpensive electronic commerce"[8] which is a decentralized e-payment protocol, and it allow payments as low as 1/10 of a cent. It employs a type of e-coins. It is introduced to make the cost of committing a fraud, more than the cost of the real transaction. It utilizes asymmetric encryption techniques for all information transactions. Millicent is a lightweight and secure scheme for e-commerce through the internet. It is developed to support to buy goods charging less than a cent. It is relied on decentralized validation of e-currency at the seller server without any further communication, costly encryption, or off-line processing. Also, in 1997, Rivest suggested his protocol entitled "Electronic lottery tickets as e-payments" [9]. In this protocol there is a possibility to reduce the number of messages engaged with every transaction. Also, the lottery ticket scheme is relied on the assumption that financial agents are risk neutral and will be satisfied with fair wagers. In 1998, Foo and Boyd proposed another protocol called "A payment scheme using vouchers" [10]. The e-vouchers can be moveable but the direct exchange between purchasers and vendors is impossible. As a result, a financial agent is needed and this will raise the transactions charges of exchange. However, during the last decade several new e-payment protocols [11] [12] [13] have been suggested. In this section, we will discuss Kim and Lee protocol [6] which is an efficient and flexible protocol.

4. KIM AND LEE PROTOCOL

In 2003, Kim and Lee [6] proposed e-payment protocol that supports multiple merchants. The protocol is divided into three schemes: certificate issuing scheme, payment scheme, and redemption scheme.

Certificate Scheme

User U requests a certificate to a bank B by sending his secret information through a pre-established secure channel. The bank B passes C_U , which guarantees to be justified and S_U which will be employed for the root value in payment scheme later. Every user U creates his public and secret key pair (PK_U, SK_U) and passes PK_U with I_U that contains the maximum number of merchants N , the size of hash chain n with his credit card information to the bank B . As a user certificate signed by a bank B , those who intend to employ this key should trust him. The bank B generates special information T_U *,* which acts as a key factor of the root value. It is employed to make clear that the new hash values created by the bank B are published to whom, because no individual except the bank B can generate it.

$T_U = h(U, r_B, K)$, where K is the private key of the bank B
$S_U = (s_i \mid s_i = h(s_{i+1}, T_U), i = N-1,...,0)$, where s_i is created by a shared user-bank private key.

The certificate C_U , in which all the elements as well as the expiry date of the certificate E_U are signed by the bank B and pass to the user U with S_U and a nonce r_U .
$C_U = (ID_B, ID_U, PK_U, T_U, I_U, E_U)SK_B$.

Payment Scheme

The root value of pay-words is merged with s_i that obtained from the bank B , which enables the user U to employ the rest of the unspent pay-words in chain for multiple payments to other merchants. The user who obtains the certificate in preceding scheme can now generate pay-words and commitment. The commitment contains the identity of the merchant with whom a user intends to do commerce, the certificate, the root elements which are modified into w_j , $h(w_j, s_k)$, the expiry date of the commitment E_M and other data I_M ,such that $0 \le j \le n$ employed to setup root value for other merchants. Then the user U signs the elements $M_U = (V, C_U, w_0, h(w_j, s_k), E_M, I_M)SK_U$

To spend the remainder of the pay-words in chain, the user U must set the root value of pay-words to be spent in subsequently payment scheme with the merging of hash chain values respectively created by a user U and the bank B . For instance, when it is supposed that a user U employed pay-words as many as *wj-1* in preceding transactions and spent *l* pay-words at the present transaction with k^{th} merchant, the root value of pay-words must be identical with $h(w_j, s_k)$ to be suitable for the payments. The user U can apply his pay-words to other merchants up to the maximum transaction limit of N unless the last pay-word surpasses w_n . The merchant keeps the last received payment data of $P_j + 1 = (w_j + 1, j + 1)$ and the commitment, and finishes the payment scheme.

Redemption Scheme

Merchant must perform the redemption process with a bank B within a pre-agreed period of time. The bank B verifies if the payment request of the merchant is correct or not by checking the certificate.

First, the merchant orders for redemption to a bank B by passing the user U commitment and payment parameter. From this information, the bank B checks his signature noticeable at the certificate and redeems $P_j + 1$ to an equivalent amount of money. We note that the bank B can check pay-words only from w_j to w_{j+1} for that order. However, since the equivalent source value is w_{j+1} , the only thing imposed to the bank B is that the last received pay-word w_{j+1} is identical with w_j by applying hash function *l* times. The bank B processes redemption orders from merchants less than N before being overdue. Finally, the bank B completes the redemption process when the last received value w_1 is less than the maximum value of the hash chains.

Remarks

The scheme supports multiple merchant payments and prevents overspending payment. Moreover, in pay-word system, whenever a customer wants to establish transactions with each vendor, he has to obtain a certificate from a broker and create a series of pay-words, while a customer is able to make transactions with different merchants by performing only one hash chain operation in Kim and Lee scheme. Nevertheless, we observe the following limitation on this scheme:

- The system performance is reduced by necessarily frequent signing in each transaction;
- The customer has to keep different hash chains and corresponding indices; however the overhead of merchants is relatively high. To securely deposit, the bank has to collect all pay-words belonging to the same chain. It needs an additional storage space and wastes undetermined waiting time; and
- The dispute arises if the merchant forges transaction records or the customer double spends.

5. THE PROPOSED PROTOCOL

We will suggest an efficient protocol in this section, which gives more efficiency than its present version of the pay-word scheme; we describe a bit more on this protocol in order to make a simple comparison between both. Thus, gauging the efficiency and security of the protocol will be described in section 6. However, the protocol is divided into four schemes, registration scheme, blind scheme, transaction scheme, and redemption scheme. Also, in this section, we will introduce a blind scheme using RSA-typed blind signature [14]. We will show this improvement makes the pay-word protocol more efficient and keeping all other characteristics consistent.

Blind Scheme

The user passes a withdrawal order to the bank prior to his order for any service from merchant. The steps of the scheme are as follows:

Step 1: Bank
1.1. Select secretly and randomly two large prime p and q
1.2. Calculate modulus $n_B = p * q$
1.3. Compute $\theta(n) = (p-1)(q-1)$
1.4. Choose exponent key e where $1 < e < \theta(n)$ and $\gcd(e,(\theta(n)) = 1$
1.5. Calculate private key w where $e * w \equiv 1 \bmod \theta(n)$
1.6. Determine the public key (e, n_B) and private key $(w, \theta(n), p, q)$

Step 2: User
2.1. Select arbitrary numbers r and u
2.2. Calculate $a = r^e * h(x_0)(u^2 + 1) \bmod \theta(n)$
2.3. Pass (b, a) to the bank

Note that information b can indicate the expiry date; the value of cash (higher limit) that the user can employ that is the funds of every hash currency.

Step 3: Bank
3.1. Select an arbitrary number $x_1 < \theta(n)$
3.2. Pass x_1 to the user

Step 4: User
4.1. Choose an arbitrary value r_1
4.2. Calculate $b_2 = r * r_1$
4.3. Pass $\beta = (b_2)^e * (u - x_1) \bmod \theta(n)$ to the bank

Step 5: Bank
5.1. Calculate $\beta^{-1} \bmod \theta(n)$
5.2. Compute $t_1 = h(b)^w * (a(x_1^2 + 1) * \beta^{-2})^{2*w} \bmod \theta(n)$
5.3. Pass (β^{-1}, t_1) to the user

Step 6: User
6.1. Calculate $c_1 = (u * x_1 + 1) * \beta^{=1} * (b_2)^e = (u * x_1 + 1)(u - x_1)^{-1} \bmod \theta(n)$
6.2. Calculate $s_1 = t_1 * r^2 * (r_1)^4 \bmod \theta(n)$

The parameter $(b, c_1 . s_1)$ is the signature on message x_0. Anybody can check this signature by verifying if $s_1^e \equiv h(b)h(x_0)^2 * (c_1^2 + 1)^2 \bmod \theta(n)$

6. DISCUSSIONS

In this section we will discuss both security and efficiency of the proposed protocol

6.1 Security

The proposed protocol withstands the following threats:

Forgery Detection

The user U gets the bank B signature on x_0 prior to any transaction. The blind signature is relied on RSA scheme, which is extensively employed a secure signature scheme. Also, in order to process an accurate redemption, the merchant M should have information of the payment transaction. It is almost unfeasible for any entity to forge the user U payment without knowing the private key K_{UM} and K_{UM} .

Thus, the opponent cannot forge signature. But to successfully achieve the verification of the formula:
$s_1^e \equiv h(b) * h(x_0)^2 * (c_1^2 + 1)^2 \bmod \theta(n)$ .An opponent has to calculate s_1 where $s_1 \equiv h(b)^w * h(x_0)^{2*w} * (c_1^2 + 1)^{2*w} \bmod \theta(n)$ provided the results of $h(b)$, $h(x_0)$ and c_1. However, it is computationally intractable to obtain the value of w without factoring $\theta(n)$ that is hard to solving such problem. In contrast provided s_1, $h(b)$ and $h(x_0)$ it is intractable to calculate c_1 where $c_1^2 \equiv (s_1^e * h(b)^{-1} * h(x_0)^{-2})^{1/2} - 1 \bmod \theta(n)$ without factoring $\theta(n)$. Provided b and c_1, the opponent is unable to obtain s_2 where $s_2 \equiv s_1 * h(x_0)^{-2*w} * h(x_0^{'})^{2*w} \bmod \theta(n)$ without given w .Without factoring $\theta(n)$, it is hard to obtain c_2 where $(c_2)^2 \equiv (s_1^e * h(b)^{-1} * h(x'_0)^{-2})^{1/2} - 1 \bmod \theta(n)$. It is also hard to derive message $x_0^{'}$ with $x_0^{'} \equiv x_0 \bmod \theta(n)$ where $h(x_0) \equiv h(x_0^{'}) \bmod \theta(n)$. Thus, the opponent is unable to forge the signature.

Over Spending Prevention

The proposed protocol adopts the same transaction scheme of the pay-word [6]. The user U sends $(f_{UM},(b,c_1,s_1),x_0,(x_j,z),c_d,OI,Expire)K_{UM}$ to Merchant M prior to taking service from Merchant M. The payment source f_{UM} is identical to $h(x_j \oplus (c_d \parallel K_{UM}))$. However, note that the c_d , K_{UM} will be different in each purchase. As a result, the bank B would be able to identify over spent payment when the user U spends twice the payment.

Connectivity Unallowable

For any provided valid signature (b,c_1,s_1) no one except the requester can connect the signature to its preceding signing order. This means that the signer is incapable to get the connection between the signature and its equivalent signing process order.

Multiple Payments

In the transaction scheme, the user U sends an order to the bank B to obtain K_{UM} and generates the payment transaction $R_{UM} = h(x_j \oplus (c_d \parallel K_{UM}))$ such that x_j is the first unused payment in the sequence. As a result, each time if the user U makes a purchase R_{UM} is not the same that enables the user U to make payments with multiple merchants.

6.2 Efficiency

In the e-payment protocol, the profit acquired by a merchant is little in every transaction. It is unwise to check the transaction employing a complicated technique that leads the average cost of the protocol more than the profit [15] [16] [17]. On the other hand, large calculation in e-payment is not wise. In order to gauge efficiency of the proposed protocol, we compare the enhanced blind scheme with the pay-word scheme [6]. The time complexity of the remaining scheme stays the same in both protocols. We employ the following notation to gauge the efficiency of the schemes.

T_h : Calculation time for hash function operation

T_a : Calculation time for point addition in elliptic curve or modular multiplication

T_m : Calculation time for point multiplication in elliptic curve or modular exponentiation

T_e : Calculation time for asymmetric key encryption

Protocol Name	Blinding Scheme
The pay-word Protocol	$5*T_h+9*T_a+5*T_m+3*T_e$
Proposed Protocol	$3*T_h+7*T_a+3*T_m+1*T_e$

TABLE 1: Time complexity in blinding scheme

7. CONSLUSION & FUTURE WORK

In this paper, we described the characteristics of e-payment protocol and evaluate one of the most important e-payment protocols that relied on a hash chain [6]. The hash chain typed scheme gives anonymity security characteristic besides to other security features of e-payment protocol. The use of the blind signature scheme and one-way hash function makes the protocol more efficient and it guarantees the payment untraceable. Though, we notice that the blind scheme of the protocol [6] takes significantly more computing time and we present an alternate blind scheme using the RSA signature scheme that gives more efficiency than the existing protocol. While the enhanced protocol needs large key length, around 1024-bit, in comparison with 160-bit key with elliptic curve encryption scheme, but we think that time complexity and rapidity are two significant issues than storage cost, and in this situation, the proposed protocol will give major benefit to small value payments. The research work accomplished in this paper has vast future prospects and can be extended towards a substantial protocol using hash function so that the modular exponentiation and costly operation can be shunned and also similar security depth can be reached.

8. REFERENCES

[1] Y Mu, K Nguyen and V Varadharajan, "*A fair electronic cash scheme*", In Proceeding of the International Symposium in Electronic Commerce, LNCS 2040, Springer-Verlag, pp. 20–32, 2001.

[2] N Someren, "*The practical problems of implementing Micro mint*", In proceeding of the International Conference of Financial Cryptography, LNCS 2339, Springer-Verlag, pp. 41-50, 2001

[3] N Someren, A Odlyzko, R Rivest, T Jones and D Scot, "*Does anyone really need micropayments*", In proceeding of the International Conference of Financial Cryptography, LNCS 2742, Springer-Verlag, pp. 69-76, 2003.

[4] C Wang, C Chang and C Lin, "*A new micro-payment system using general pay-word chain. Electronic Commerce*", Research Journal, 2(1-2): 159-168, 2002

[5] S Yen, L Ho and C Huang, "*Internet micro-payment based on unbalanced one-way binary tree*", In Proceeding the International Conference of Cryptec'99, 155-162, 1999.

[6] S Kim and W Lee, "*A Pay-word-based micro-payment protocol supporting multiple payments*", In Proceeding of the International Conference on Computer Communications and Networks, pp. 609-612, 2003.

[7] D Chaum, Fiat and M Naor, "*Untraceable electronic cash*", In Proceeding Advances in Cryptology, LNCS 403, Springer-Verlag, pp. 319-327, 1988.

[8] S Glassman, M Manasse, M Abadi, P Gauthier and P Sobalvarro, "*The Millicent protocol for inexpensive electronic commerce*", In Proceeding of the International World Wide Web Conference, pp. 603–618, O'Reilly, 1995.

[9] R Rivest, "*Electronic lottery tickets as micropayments*", In Proceeding of the International Conference of Financial Cryptography, LNCS 1318, Springer-Verlag, pp. 307–314, 1997

[10] E Foo and C Boyd, "*A payment scheme using vouchers*", In Proceeding of the International Conference of Financial Cryptography, LNCS 1465, Springer-Verlag, pp. 103-121, 1998.

[11] Baddeley M, "*Using e-cash in the new economy: An economic analysis of micro-payment systems*", Journal of Electronic Commerce Research, 5 (4), 2004

[12] J Hubaux, and L Buttyan, "*A micro-payment scheme encouraging collaboration in multi-hop cellular networks*", In Proceeding of Financial Cryptography, LNCS 2742, Springer-Verlag, pp. 15–33, 2003.

[13] Koblitz N, "*Elliptic Curve Cryptosystems*", Mathematics of Computation, 48(2), 203-209, 1987.

[14] H Chien, J Jan and Y Tseng, "*RSA-based partially blind signature with low computation*", In Proceeding of the International Conference in Parallel and Distributed Systems, pp. 385–*389, USA, 2001.*

[15] Matthew N. Anyanwu, Lih-Yuan Deng & Dipankar Dasgupta, "Design of Cryptographically Strong Generator by Transforming Linearly Generated Sequences", International Journal of Computer Science and Security, (IJCSS) Volume (3): Issue (3), 2009

[16] Anil Kapil and Sanjeev Rana, Identity-Based Key Management in MANETs using Public Key Cryptography, International Journal of Security (IJS), Volume (3) : Issue (1), 2009

[17] Ankur Agarwal, System-Level Modeling of a Network-on-Chip, International Journal of Computer Science and Security, (IJCSS) Volume (3): Issue (3), 2009