ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2011, Vol. 40, No. 2

SECURE SMART CARD BASED PASSWORD AUTHENTICATION SCHEME WITH USER ANONYMITY

Chun-Ta Li

Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.)
e-mail: th0040@mail.tut.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.40.2.431

Abstract. Recently, a smart card based authentication and key agreement scheme preserving the user anonymity was proposed by Wang, Juang and Lei, that is designed to provide users with secure activities in ubiquitous computing environments. The authors proved that their scheme delivers important security properties and functionalities, such as without maintaining password/verification tables, freedom on password selection and alteration, mutual authentication, user anonymity, no time synchronization problem, key agreement implementation, forgery attack resistance and computation efficiency. However, we show that Wang et al.'s scheme has potential security flaws, which enable malicious attackers to counterfeit an application server to spoof the victim client and damage the security of session key and the property of user anonymity. In this paper, we propose an enhanced version of Wang et al.'s scheme to remedy these flaws. The proposed scheme not only ensures the merits of their scheme but also enhances the security of their scheme without raising any computation cost.

Keywords: network security, password authentication, smart card, ubiquitous computing environments, user anonymity.

1. Introduction

The movement towards ubiquitous computing environment has raised a number of security concerns among the remote application servers and the login clients. At any time and any place, a client can access the desired services from an application server by using his/her mobile devices such as PDA, laptop and smart phone etc. Remote user authentication based on easy-to-remember passwords over insecure networks is the conventional method of authentication and has already been accepted warmly. An application server is responsible for managing and supplying network services to login clients for which password authentication schemes have been provided during a login request. A number of relevant researches and authentication mechanisms have been investigated in recent three decades and the key concepts include:

1. Without maintaining verification or password tables in server side to prevent stolen verifier attacks [5, 7].
2. Using a smart card to help clients to remember secret information [3].
3. Users can freely choose and change passwords [2].
4. Resistance to password disclosure to any other users [17-22].
5. Using a nonce-based mechanism to prevent time synchronization problem [9, 13].
6. Resistance to replay, modification, parallel session [4] and password guessing attacks [14].
7. Protect the system against impersonation attacks on both the user and the server side [1, 16].
8. Low communication cost and computation complexity.
9. Achieve mutual authentication and key agreement implementation between login users and remote servers [10, 12, 15].
10. Prevention of smart card security breach attacks. Note that secret information stored in a smart card can be extracted by analyzing and monitoring its power consumption [6, 20].
11. Revocation of smart card in case of stolen or smart card loss problems [25].
12. Provision of user anonymity and the client's identity and location cannot be traced by any users over public networks [8, 11, 23, 25].

Recently, Wang et al. proposed a security enhancement on two efficient remote user authentication schemes using smart cards [24]. Remote user authentication scheme is a very important mechanism in distributed computer network systems for preventing unauthorized network access. Many remote user

authentication schemes have been proposed using smart cards because of the low cost. In 2011, Wang et al. [25] found that the Wang et al.'s scheme is vulnerable to the known-key attack and the smart card loss problem. To remedy these weaknesses, they proposed an improvement on the Wang et al.'s scheme. However, we found that the Wang et al.'s scheme is still vulnerable to two kinds of sever counterfeit attacks and thus damage the security of session key. To resolve these security problems, we propose an enhanced version of Wang et al.'s scheme in this paper. The proposed scheme not only inherits the advantages of their scheme but also enhances the security of their scheme without raising any computation cost.

The remainder of this paper is organized as follows. A brief review of the Wang et al.'s scheme is given in Section 2. We analyze their scheme to show their security flaws in Section 3. In Section 4, we propose our improved scheme and the security analysis of the proposed scheme are presented in Section 5. Finally, we conclude this paper in Section 6.

2. A Review of Wang et al.'s scheme

Recently, Wang et al. proposed a robust authentication and key agreement scheme preserving the user anonymity [25]. There are seven phases in their scheme which includes registration, precomputation, authentication and key agreement, password change, revoking smart card, user eviction and user anonymity phase. For convenience of description, terminology and notations used in the paper are summarized as follows:

- id_i: the identity of a client i.
- cid_i: the identity of a smart card.
- S: an application server.
- pw_i: the password chosen by the client i.
- p: a large prime number and a and b are two integers, where $4a^3 + 27b^2 \bmod p \neq 0$.
- E_p: an elliptic curve equation over finite field p: $y^2 = x^3 + ax + b \bmod p$.
- G: a base point of the elliptic curve with a prime order n.
- O: a point of the elliptic curve at infinite, where $n \times G$ is equal to O, $n > 2^{160}$ and $\times$ denotes the elliptic curve point multiplication operation.
- x: the permanent master key of S; it cannot be derived by the brute force attack.
- $||$: string concatenation operation.
- $\oplus$: the bitwise exclusive OR operation.
- $h(.)$: a cryptographic one-way hashing function.
- T_i: an entity i's current timestamp.

In the following subsections, we briefly review Wang et al.'s scheme.

2.1. Registration Phase

In this phase, all the communications between the client i and the application server S are through a secure channel.

1. Client i chooses the identity id_i and sends it to the application server S.
2. S computes $B_i = h(x||id_i||cid_i) \times G$, stores ($id_i$, B_i, G, E_p) into client i's smart card, issues it to client i, and maintains a ID table which contains (id_i, cid_i).
3. On receiving the smart card from S, the client i must activate the smart card and input the easy-to-remember password pw_i. Then smart card computes $B_i' = B_i \oplus h(pw_i)$ and replaces B_i with B_i'. Finally, client i's smart card contains (id_i, B_i', G, E_p).

2.2 Precomputation Phase

Before the client i starts to access the application server, the smart card computes $T_1 = R \times G$ as a point over E_p and stores T_1 into its memory for using in the authentication and key agreement phase.

2.3 Authentication and Key Agreement Phase

When client i intends to login S, the client attaches his/her smart card into the card reader and inputs the password pw_i. Then, the smart card and the remote application server perform the following steps:

1. The smart card computes $B_i = B_i' \oplus h(pw_i) = h(x||id_i||cid_i) \times G$ and $T_2 = h(R \times B_i) = h(R \times h(x||id_i||cid_i) \times G)$ and sends (id_i, T_1, T_2) to S.
2. On receiving the login request from client i, S checks its ID table to verify the validity of client i's id_i and checks if computed $T_2' = T_1 \times h(x||id_i||cid_i) = R \times h(x||id_i||cid_i) \times G$ equals received T_2. If it matches, S computes $K = h(W \times T_1)$, $V_1 = h(T_2' \,||\, K)$ and $T_3 = W \times G$ and sends (T_3, V_1) back to the smart card, where W is a random number in Z_n^*.
3. On receiving the response message from S, the smart card checks if computed $V_1' = h(R \times B_i||K')$ equals received V_1, where $K' = h(R \times T_3)$. If it matches, the client i successfully authenticates S and sends a response $V_2 = h(R \times B_i||K' + 1)$ to S. On receiving V_2 from the client, S checks if computed $h(T_2'||K + 1)$ equals received V_2. If it holds, S successfully authenticates the client i.
4. The value $K = h(R \times W \times G) = K'$ computed by the client and the application server can be used as the session key for securing future communications.

2.4. Password Change Phase

When the client i wants to change his/her password pw_i with a new password new_{pwi} , the client inserts his/her smart card into the card reader and enters the original and new passwords. Then, the smart card computes $B_i'' = B_i' \oplus h(pw_i) \oplus h(new_{pwi})$

and replaces B_i' with B_i". Now, the client *i*'s new password new_{pwi} is successfully changed and this phase is finished.

2.5. Revoking Smart Card Phase

In case of stolen or lost smart card, there should be provision in the scheme for revoking the illegal use of stolen or lost smart card and the client should notify the application server of the revocation. Then smart card and the remote application server perform the following steps:

1. *S* generates the identity of a new smart card cid_{inew}, computes $B_i = h(x||id_i||cid_{inew})$, stores ($id_i$, B_i, G, E_p) into client *i*'s new smart card, issues it to client *i*, and maintains a ID table which replaces (id_i, cid_i) with (id_i, cid_{inew}).
2. On receiving the new smart card from *S*, the client *i* must activate the card and input a memorable password pw_i. Then smart card computes $B_i' = B_i \oplus h(pw_i)$ and replaces B_i with B_i'. Finally, client *i*'s smart card contains (id_i, B_i', G, E_p).

2.6. User Eviction Phase

In case of a client is evicted by the application server, *S* can delete (id_i, cid_i) from its ID table and the client cannot use (id_i, cid_i) to login the application server anymore.

2.7. User Anonymity Phase

In Wang et al.'s scheme, authors extend their scheme to provide the user anonymity and the user's identity and location cannot be traced by any users over public networks. We briefly review Wang et al.'s scheme with user anonymity as follows:

1. In the registration phase, the client *i* sends a registered information to the application server and the server stores (IND_i, B_i, G, E_p) into client *i*'s smart card, where IND_i denotes an indicator and $B_i = h(x||IND_i||cid_i)$. Then, the client activates the smart card and replaces B_i with $B_i' = h(x||IND_i||cid_i) \oplus h(pw_i)$. Note that server's ID table will become (cid_i, IND_i) and smart card includes (IND_i, B_i', G, E_p).
2. The precomputation phase is the same as before.
3. The authentication and key agreement phase is extremely similar to that presented in Section 2.3. The major differences are as follows:
   (a) In Step 1, the client *i* sends the login request (IND_i, T_1, T_2) to the application server.
   (b) In Step 2, after verification of client *i*'s login request, *S* computes a symmetric encryption key $K_1 = h(W \times T_1)$ and sends a response (V_1, T_3) back to the smart card, where $V_1 = E_{K1}[h(T_2'+1)||IND_{inew}||B_{inew}]$, $E_K[M]$ denotes a symmetric encryption algorithm using a key K, $B_{inew} = h(x||IND_{inew})||cid_i) \times G$ and $T_3 = W \times G$.
   (c) In Step 3, the smart card reveals V_1 by computing $D_{K1'}[V_1] = h(T_2' +1)||IND_{inew} || B_{inew}$ and checks if computed $h(R \times B_i+1)$ equals received $h(T_2' + 1)$, where $K_1' = h(R \times T_3)$ and $D_K[M]$ denotes a symmetric decryption algorithm using a key K. If it matches, the application server is authenticated, the smart card sends a reply $V_2 = h(R \times B_i + 2)$ to *S* and *S* verifies whether V_2' is the same as V_2 or not. If it holds, the identity of the client is also authenticated.
   (d) In Step 4, the smart card replaces (IND_i, B_i) with (IND_{inew}, B_{inew}) and the server renews the ID table as (cid_i, IND_{inew}).

3. Cryptanalysis of Wang et al.'s Scheme

In this section, we show that two kinds of server counterfeit attacks and the session key cryptanalysis attack exist in Wang et al.'s scheme [25].

3.1. Server Counterfeit Attack I

In server counterfeit attack I, a legal but malicious client (or attacker) can easily apply a valid smart card and extract the secret information G and E_p from this applied smart card by monitoring its power consumption [6, 20]. Since the secret information G and E_p are concurrently used for all clients and this design helps the attacker to counterfeit an application server to spoof the victim client. We briefly describe this attack as follows:

1. In Step 1 of the authentication and key agreement phase, the attacker intercepts a login request (id_i, T_1, T_2) sent by a victim client.
2. Upon intercepting the login request (id_i, T_1, T_2), the attacker selects a random number W' in Z_n^* and computes a fake response ($T_3" = W' \times G$, $V_1" = h(T_2||K")$, where $K" = h(W' \times T_1)$. Then the attacker sends ($T_3"$, $V_1"$) back to the victim client.
3. Upon receiving the response ($T_3"$, $V_1"$) from the attacker, the victim client's smart card checks if computed $V_1' = h(R \times B_i||K')$ equals received $V_1"$, where $K' = h(R \times T_3)$. Obviously, the value $V_1' = h(R \times B_i||K')$ is the same as the attacker's value $V_1" = h(T_2 = h(R \times h(x||id_i||cid_i) \times G)||K")$ and the verification will pass. Therefore, the victim client believes that he/she currently communicates with a legal application server and sends a reply $V_2 = h(R \times B_i||K' + 1)$ back to the attacker. Of course, the attacker will ignore and discard this response. Hence, Wang et al.'s scheme is vulnerable to server counterfeit attack I.

3.2. Server Counterfeit Attack II

In server counterfeit attack II, we demonstrate that Wang et al.'s scheme with user anonymity cannot defend against the server counterfeit attack. We assume that the attacker can get the secret information G and

E_p and the details of this attack are described as follows:

1. In Step 1 of the authentication and key agreement phase, the attacker intercepts a login request (IND_i, T_1, T_2) sent by a victim client.
2. Upon intercepting the login request (IND_i, T_1, T_2), the attacker selects a random number W' in Z_n^* and computes a fake symmetric key K_1" = $h(W' \times T_1)$ and a response V_1' = $E_{K1"}[h(T_2+1)||IND_{ifake}||B_{ifake}]$, where IND_{ifake} and B_{ifake} are meaningless values chosen by the attacker. Then the attacker sends V_1' with T_3" = $W' \times G$ back to the victim client.
3. Upon receiving the response (T_3", V_1') from the attacker, the victim client's smart card reveals V_1' by computing $D_{K1'}[V_1'] = h(T_2 + 1) ||IND_{ifake}||B_{ifake}$ and checks if computed $h(R \times B_i+1)$ equals received $h(T_2 + 1)$, where $K_1' = h(R \times T_3")$. Obviously, the symmetric key $K_1' = h(R \times T_3")$ and the value $h(R \times B_i+1)$ computed by the victim client are the same as the symmetric key $K_1" = h(W' \times T_1)$ and the value $h(T_2+1)$ computed by the attacker. Thus, the attacker will pass the verification and the victim client believes that he/she currently communicates with a legal application server and sends a reply $V_2 = h(R \times B_i+2)$ back to the attacker. Similarly, the attacker will ignore and discard this response and Wang et al.'s scheme with user anonymity is vulnerable to server counterfeit attack II.
4. The execution of Step 4 is almost the same as in the Wang et al.'s extended scheme and the victim client's smart card will replace original (IND_i, B_i) with (IND_{ifake}, B_{ifake}). Finally, the attacker can use the fake values (IND_{ifake}, B_{ifake}) to trace the victim client's identity and location and the user anonymity cannot be achieved in Wang et al.'s extended scheme.

3.3. Session Key Cryptanalysis Attack

According to Section 3.1, the attacker can easily counterfeit a legal but malicious server and maliciously communicate with the victim client. After above-mentioned steps of server counterfeit attack I are finished, the attacker and the victim client compute the same session key $K' = K"$ and the attacker can employ K" to launch a malevolent communication later.

Similarly, according to Section 3.2, the attacker and the victim client compute the same session key $K_1' = K_1"$ and the attacker can employ K_1" to launch a malevolent communication later.

4. The Proposed Scheme

To overcome the above-mentioned attacks, we propose an improvement on Wang et al.'s scheme in this section. In our proposed scheme, the registration, precomputation, password change, revoking smart card and user eviction phases are the same as those in Wang et al.'s scheme. The main differences in the authentication and key agreement and user anonymity phases are briefly described in the following subsections.

4.1. Authentication and Key Agreement Phase

1. Step 1 is the same as in Wang et al.'s scheme.
2. On receiving the login request from client i, S checks its ID table to verify the validity of client i's id_i and checks if computed $T_2' = T_1 \times h(x||id_i||cid_i) = R \times h(x||id_i||cid_i) \times G$ equals received T_2. If it matches, S computes $h(x||id_i||cid_i) \times G$, $K = h(W \times T_1)$, $V_1 = h(h(x||id_i||cid_i) \times G||K)$ and $T_3 = W \times G$ and sends (T_3, V_1) back to the smart card, where W is a random number in Z_n^*.
3. On receiving the response message from S, the smart card checks if computed $V_1' = h(B_i||K')$ equals received V_1, where $K' = h(R \times T_3)$ and $Bi = h(x||id_i||cid_i) \times G$. If it matches, the client i successfully authenticates S and sends a response $V_2 = h(B_i||K'+1)$ to S. On receiving V_2 from the client, S checks if computed $h(h(x||id_i||cid_i) \times G||K+1)$ equals received V_2. If it holds, S successfully authenticates the client i.
4. The value $K = h(R \times W \times G) = K'$ computed by the client and the application server can be used as the session key for securing future communications.

4.2. User Anonymity Phase

1. The registration phase is the same as in Wang et al.'s extended scheme.
2. The precomputation phase is the same as in Wang et al.'s extended scheme.
3. The authentication and key agreement phase is extremely similar to Wang et al.'s extended scheme. The major differences are as follows:
   (a) In Step 1, the client i sends the login request (IND_i, T_1, T_2) to the application server.
   (b) In Step 2, after verification of client i's login request, S computes a symmetric encryption key $K_1 = h(W \times T_1)$ and sends a response (V_1, T_3) back to the smart card, where $V_1 = E_{K1}[h(h(x||id_i||cid_i) \times G+1)||IND_{inew}||B_{inew}]$, $B_{inew} = h(x||IND_{inew})||cid_i) \times G$ and $T_3 = W \times G$.
   (c) In Step 3, the smart card reveals V_1 by computing $D_{K1'}[V_1] = h(h(x||id_i||cid_i) \times G+1) ||IND_{inew}||B_{inew}$ and checks if computed $h(B_i+1)$ equals received $h(T_2' +1)$, where $K_1' = h(R \times T_3)$ and $B_i = h(x||id_i||cid_i) \times G$. If it matches, the application server is authenticated, the smart card sends a reply $V_2 = h(B_i+2)$ to S and S verifies whether $V_2' = h(h(x||id_i||cid_i) \times G + 2)$ is the same as V_2 or not. If it holds, the identity of the client is also authenticated.
   (d) In Step 4, the smart card replaces (IND_i, B_i) with (IND_{inew}, B_{inew}) and the server renews the ID table as (cid_i, IND_{inew}).

5. Security Analysis

In this section, we analyze the security of the proposed scheme and demonstrate its strength in terms of security. The proposed scheme is a modified form of Wang et al.'s scheme and we only discuss the improved security features of the proposed scheme.

5.1. Server Counterfeit Attack I Resistance

In Step 2 of the authentication and key agreement phase, the attacker needs to reply $V_1 = h(h(x||id_i||cid_i)\times G||K'' = h(W' \times T_1))$ and $T_3 = W' \times G$ to the client for verification, where W' is a random number chosen by the attacker. However, without knowing the server's master key x and the client's secret information $h(x||id_i||cid_i)\times G$, it is difficult for the attacker to fake a correct K''. Thus the attacker cannot counterfeit a legal server to reply a correct hash value V_1 to convince the client. Moreover, when a response of previous session is revealed or eavesdropped by an attacker, it is difficult for him/her to derive server's master key x and the client's secret information $h(x||id_i||cid_i)\times G$ because these two values are well-protected under the adoption of one-way hashing function. Therefore, the proposed system is secure against server counterfeit attack I.

5.2. Server Counterfeit Attack II Resistance

For our scheme with user anonymity, if the attacker intends to counterfeit a legal server, the attacker needs to compute a symmetric encryption key $K_1'' = h(W' \times T_1)$ with an encrypted response $V_1 = E_{K1''}[h(h(x||IND_i||cid_i)\times G +1)||IND_{ifake}||B_{ifake}]$ and replies (V_1, $T_3 = W' \times G$) to the client for verification, where W' is a random number chosen by the attacker. However, the server's master key x and the client's secret information $h(x||IND_i||cid_i)\times G$ are securely protected by the server and the client, respectively. It means that the attacker cannot fake a correct V_1 with K_1'' and nobody can counterfeit a legal server to deceive other ones. Therefore, the resistance to server counterfeit attack II can be guaranteed in our user anonymity scheme.

5.3. Security of Session Key

As shown in the authentication and key agreement phase, the client and the server agree a common session key $K = h(R\times W\times G) = K'$ and they can use the session key to secure the transmitting messages in the rest of the communication.

For security of session key, even if an attacker can obtain the client's contribution $T_1 = R \times G$ and the server's contribution $T_3 = W \times G$, the attacker still cannot derive the common session key $K = h(R\times W\times G) = K'$ because to do this is as difficult as solving the Elliptic curve computational Diffie-Hellman problem.

6. Conclusions

In this paper, we have showed security vulnerabilities on two Wang et al.'s password authentication schemes. By intercepting a victim client's login request, a malicious attacker can counterfeit an application server to spoof this victim client, endanger the security of key agreement, and damage the property of user anonymity. To resist these security threats found in their schemes, we have developed two enhanced password authentication schemes. Security analysis shows that two enhanced schemes not only inherit the merits of Wang et al.'s schemes but also enhance the security of Wang et al.'s schemes.

References

[1] **T.H. Chen, H.C. Hsiang, W.K. Shih.** Security enhancement on an improvement on two remote user authentication schemes using smart cards. *Future Generation Computer Systems*, 27(4), *April*, 2011, 377-380.

[2] **H.Y. Chien, J.K. Jan, Y.M. Tseng.** An efficient and practical solution to remote authentication: smart card. *Computers and Security*, 21(4), 2002, 372-375.

[3] **M.S. Hwang, L.H. Li.** A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 46(1), 2000, 28-30.

[4] **C.L. Hsu.** Security of Chien et al.'s remote user authentication scheme using smart cards, *Computer Standards and Interfaces*, 26(3), 2004, 167-169.

[5] **J.K. Jan, Y.Y. Chen.** "Paramita wisdom" password authentication scheme without verification tables. *The Journal of Systems and Software*, 42(1), 1998, 45-57.

[6] **P. Kocher, J. Jaffe, B. Jun.** Differential power analysis. *In Proceedings of Advances in Cryptology*, 1999, 388-397.

[7] **L. Lamport.** Password authentication with insecure communication. *Communications of the ACM*, 24(11), 1981, 770-772.

[8] **C.C. Lee, I.E. Liao, M.S. Hwang.** An extended certificate-based authentication and security protocol for mobile networks. *Information Technology and Control*, 38(1), 2009, 61-66.

[9] **C.C. Lee, C.T. Li, K.Y. Huang, S.Y. Huang.** An improvement of remote authentication and key agreement schemes. *Journal of Circuits, Systems, and Computers*, article in press, 2011.

[10] **C. C. Lee, T. C. Lin and M. S. Hwang.** A key agreement scheme for satellite communications. *Information Technology and Control*, 39(1), 2010, 43-47.

[11] **C.T. Li, M.S. Hwang, Y.P. Chu.** Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments. *Computer Communications*, 31(18), 2008, 4255-4258.

[12] **C.T. Li, M.S. Hwang, Y.P. Chu.** A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications*, 31(12), 2008, 2803-2814.

[13] **C.T. Li.** An enhanced remote user authentication scheme providing mutual authentication and key agreement with smart cards. *In Proceedings of The International Conference on Information Assurance and Security*, *IEEE CS*, 2009, 517-529.

[14] **C.T. Li, Y.P. Chu.** Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks. *International Journal of Network Security*, 8(2), 2009, 166-168.

[15] **C.T. Li, M.S. Hwang, Y.P. Chu.** An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks. *International Journal of Innovative Computing, Information and Control*, 5(8), 2009, 2107-2124.

[16] **C.T. Li, C.H. Wei, Y.H. Chin.** A secure event update protocol for peer-to-peer massively multiplayer online games against masquerade attacks. *International Journal of Innovative Computing, Information and Control*, 5(12(A)), 2009, 4715-4723.

[17] **C.T. Li, M.S. Hwang.** An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, 33(1), 2010, 1-5.

[18] **C.T. Li, M.S. Hwang.** An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. *International Journal of Innovative Computing, Information and Control*, 6(5), 2010, 2181-2188.

[19] **C.T. Li, C.C. Lee.** A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling, article in press*, 2011.

[20] **T.S. Messerges, E.A. Dabbish, R.H. Sloan.** Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5), 2002, 541-552.

[21] **R. Song.** Advanced smart card based password authentication protocol. *Computer Standards and Interfaces*, 32(5-6), 2010, 321-325.

[22] **H.M. Sun, H.T. Yeh.** Password-based authentication and key distribution protocols with perfect forward secrecy. *Journal of Computer and System Sciences*, 72(6), 2006, 1002-1011.

[23] **J.L. Tsai.** Weaknesses and improvement of Hsu-Chuang's user identification scheme. *Information Technology and Control*, 39(1), 2010, 48-50.

[24] **X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan.** Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, *Computer Standards and Interfaces*, 29(5), 2007, 507-512.

[25] **R.C. Wang, W.S. Juang, C.L. Lei.** Robust authentication and key agreement scheme preserving the privacy of secret key. *Computer Communications*, 34(3), 2011, 274-280.

Received March 2011.