ICIC Express Letters
Volume **5**, Number **6**, June **2011**

 ISSN 1881-803X
pp. **000-000**

EFFICIENT DYNAMIC ID-BASED AUTHENTICATION FOR USER ANONYMITY

Kuo-Ching Liu[1], Hui-Feng Huang[2,*], and Hui-Fang Chen[3]

[1]Department of Medical Laboratory Science and Biotechnology
China Medical University, Taichung 404, Taiwan
kchliu@mail.cmu.edu.tw

[2,*]Department of Computer Science and Information Engineering
National Taichung Institute of Technology, Taichung 404, Taiwan
phoenix@ntit.edu.tw

[3]Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology, Taichung 404, Taiwan
s18983107@ntit.edu.tw

[2,*]Corresponding author

Abstract. *User authentication is an important technology to guarantee that only the legal users can access resources from the remote server. To protect user from tracing, we proposed a new efficient dynamic ID-based authentication with smart card to achieve user anonymity property. Since only one-way hash function and simple exclusive-or ( ) operations are involved in the processes, the proposed scheme is very suitable for the hardware-limited users such as the mobile units.*
Keywords: authentication, dynamic ID, anonymity, smart card, password

1. **Introduction.** Password-based authentication scheme is very convenient for a user because a user only has to remember his/her password for logging the server. In 1981, Lamport [7] proposed a password authentication scheme using a one-way hash function. Lamport's scheme is simple and efficient, but it suffers from the replay attack and the impersonation attack caused by modifying or stealing the hashed password table maintained by the servers. To overcome such security weaknesses, there are many password-based authentication schemes have been proposed in recent years [1-3, 5-6, 8, 10, 11, 13, 17]. However, most of these previously proposed schemes are based on the static identity number (ID). Then, they are vulnerable to leak the ID of the logging user. The compromise of user's ID would lead to the tracing of the previous communications for the same user. Then, it may expose potential security threats and risks for the corporations or individuals.

Recently, to protect from the risk of ID-theft, Das et al. [4] presented the concept of dynamic ID authentication to provide the user anonymity. However, Das et al.'s scheme does not achieve mutual authentication and user anonymity properties [9, 12, 14, 15, 16]. In 2009, Wang et al. [12] proposed a new dynamic ID-based authentication scheme with smart card to achieve the user anonymity and mutual authentication properties. Their scheme is efficient since only one-way hash function and simple calculation are involved in the processes. Unfortunately, this paper will show that Wang et al.'s scheme is still vulnerable to the impersonation attack. Moreover, their scheme cannon provide the user anonymity property. Then, we will propose improved method to overcome Wang et al.'s weaknesses. In addition, the proposed dynamic ID-base authentication method can provide the following functionality: (1) a dictionary of password tables is not required for the server; (2) users can freely choose their own passwords; (3) it provides mutual authentication between the user and the server; (4) user may update their password after the registration phase; (5) user anonymity property is provided; (6) session key agreement is generated by the user and the remote server for each session.

The remainder of this paper is organized as follows. In the next section, we give a brief review of Wang et al.'s scheme. In section 3, the security weakness of Wang et al.'s scheme is given. We present the proposed scheme in section 4. In section 5, the security analyses of the proposed scheme are stated. And some conclusions will be made in the last section.

2. **Review of Wang et al.'s scheme.** We first review Wang et al.'s scheme [12], and the notations are shown as follows:
U_i: the ith user.
pw_i: the ith user's password.
S: the remote server.
$h(.)$: a one-way hash function.

Wang et al.'s scheme can be divided into four phases: registration phase, login phase, verification phase, and password change phase. These four phases are stated in the following.

2.1. **The registration phase:** The new user U_i first sends the registration request to S. The steps of registration phase are described as follows.

(1) U_i submits ID_i to S.
(2) S computes $N_i = h(pw_i) \oplus h(x) \oplus ID_i$, where x is a secret of the remote server S, where $\oplus$ is an exclusive-or operator. Here, pw_i is chosen by S. Then, S issues a smart card containing $[h(.), N_i, y]$, where y is the remote server's secret key.
(3) S sends pw_i and smart card to U_i through a secure channel. (Suppose that user cannot extract any information stored in the user's smart card)

2.2. **The login phase:** When U_i wants to login the remote server, he/she inserts the smart card into the card reader and keys the identity ID_i and password pw_i. Then, the smart card performs the following steps:

(1) Compute $CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T_1) \oplus ID_i$, where T_1 is the current timestamp.
(2) The smart card sends the message (ID_i, CID_i, N_i, T_1) to S.

2.3. **The verification phase:** After receiving the login request (ID_i, CID_i, N_i, T_1) at the timestamp T_2, S and smart card execute the following steps to achieve the mutual authentication between U_i and S.

(1) Check whether $T_2 - T_1 \leq \Delta T$. If it holds, S accepts the request; otherwise, the request will be rejected.
(2) S computes $h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T_1) \oplus ID_i$ and $ID_i' = N_i \oplus h(x) \oplus h'(pw_i)$. Then, checks whether ID_i' is equal to ID_i . If it holds, S accepts the request; otherwise, rejects it.
(3) S computes $a' = h(h'(pw_i) \oplus y \oplus T_2)$ and sends (a', T_2) to U_i.
(4) After receiving the reply message (a', T_2) at time T_3, U_i checks whether $T_3 - T_2 \leq \Delta T$; if it holds, U_i computes $a = h(h(pw_i) \oplus y \oplus T_2)$, and compares it with the received a'. If a' is equal to a, U_i confirms that S is legality.

2.4. **The password change phase:** When U_i wants to change the password, he/she inserts smart card into the card reader and keys the old password pw_i and the new password pw_i^{**}, then the smart card computes $N_i^* = N_i \oplus h(pw_i) \oplus h(pw_i^{**})$, and replaces the N_i with the new N_i^*.

3. **Security analysis of Wang et al.'s scheme.** In this section, we will show that the Wang et al.'s scheme cannot provide user anonymity property. Moreover, their scheme may be suffered from forgery attack.

3.1. **No anonymity:** In their scheme, U_i sends the login request message (ID_i, CID_i, N_i, T_1) to remote server. Here, ID_i and N_i are always kept the same parameters from U_i. The attacker can use ID_i or N_i to distinguish each user and to be seen as user's identification. Therefore, their scheme uses CID_i as a dynamic identity, it cannot actually provide the user anonymity property.

3.2. **Impersonation attack:** First, U_i randomly chooses new pw_i^*, and then generate ID^* such that $h(pw_i) \oplus ID_i = h(pw_i^*) \oplus ID_i^*$. That is new $ID_i^* = h(pw_i) \oplus ID_i \oplus h(pw_i^*)$. We have $h(pw_i^*) \oplus h(x) \oplus ID_i^* = h(pw_i) \oplus h(x) \oplus ID_i = N_i$. When U_i types ID_i^* and pw^*i to login the remote server. The smart card performs the following steps:

(1) Compute $CID_i^* = h(pw_i^*) \oplus h(N_i \oplus y \oplus T_1) \oplus ID_i^*$.
(2) Send the message $(ID_i^*, CID_i^*, N_i, T_1)$ to S.

In the verification phase, S checks the timestamp and then computes $h(pw_i^*) = CID_i^* \oplus h(N_i \oplus y \oplus T_1) \oplus ID_i^*$ and $ID_i' = N_i \oplus h(x) \oplus h(pw_i^*)$. Next, S checks whether ID_i' is equal to ID_i^*, and then computes $a' = h(h(pw_i^*) \oplus y \oplus T_2)$ and sends (a', T_2) to U_i. After receiving the reply message (a', T_2) at time T_3, U_i checks the timestamp T_2 and computes $a = h(h(pw_i^*) \oplus y \oplus T_2)$, and compares it with a'. Here, it will be $a' = a$. Since $h(pw_i^*) \oplus h(x) \oplus ID_i^* = h(pw_i) \oplus h(x) \oplus ID_i = N_i$, it is obvious that $ID_i' = N_i \oplus h(x) \oplus h(pw_i^*) = h(pw_i^*) \oplus h(x) \oplus ID_i^* \oplus h(x) \oplus h(pw_i^*) = ID_i^*$

From above discussions, a legal user U_i can create other identity number ID_i^* and password pw_i^* to pass the mutual authentication.

4. **The proposed scheme.** In this section, we will propose an improvement method to overcome Wang et al.'s weaknesses [12]. The detail is described in the following.

4.1. **The registration phase:** The new user U_i freely chooses an identity ID_i and a password pw_i. Then, he/she sends the registration request to S. The steps of this phase are as follows:

(1) U_i submits ID_i and pw_i to S.
(2) S computes $N_i = h(pw_i \parallel ID_i) \oplus h(x \parallel y \parallel ID_i)$ and issues a smart card containing $[N_i, y, h(.)]$, where x and y are secret keys of the remote server.
(3) S sends the smart card to U_i through a secure channel. (Suppose that user cannot extract any information stored in the smart card)

4.2. **The login phase:** When U_i wants to login the remote server, U_i inserts the smart card into the card reader and keys his/her identity ID_i and password pw_i. Then, the smart card performs the following steps:

(1) Compute $h(x \parallel y \parallel ID_i) = N_i \oplus h(pw_i \parallel ID_i)$, $CID_i = ID_i \oplus h(y \parallel T_1)$, and $Z = h(CID_i \parallel h(x \parallel y \parallel ID_i) \parallel y \parallel T_1)$, where T_1 is the current timestamp and CID_i is the dynamic ID for U_i.
(2) The smart card sends the message (CID_i, Z, T_1) to S.

4.3. **The verification phase:** After receiving the login request (CID_i, Z, T_i) at timestamp T_2, S executes the following steps:

(1) Check whether $T_2 - T_1 \leq \Delta T$. If it holds, S accepts the request; otherwise, the request will be rejected.
(2) S first derives $ID_i = CID_i \oplus h(y \parallel T_1)$, then S computes $h(x \parallel y \parallel ID_i)$ and $Z' = h(CID_i \parallel h(x \parallel y \parallel ID_i) \parallel y \parallel T_1)$. Then, checks whether Z' is equal to Z or not. If it holds, S accepts the request; otherwise, rejects it.
(3) S computes the session key $K = h(h(x \parallel y \parallel ID_i) \parallel CID_i \parallel T_1 \parallel T_2 \parallel y)$ and $D = h(h(x \parallel y \parallel ID_i) \parallel T_2 \parallel K)$, then sends (D, T_2) to U_i.

After receiving the message (D, T_2) at timestamp T_3, U_i's smart card performs the following operation. The smart card checks whether $T_3 - T_2 \leq \Delta T$; if it holds, it computes the session key $K = h(h(x \parallel y \parallel ID_i) \parallel CID_i \parallel T_1 \parallel T_2 \parallel y)$ and $D' = h(h(x \parallel y \parallel ID_i) \parallel T_2 \parallel K)$. Then it checks whether $D' = D$. If they are equal, U_i confirms that S is legality. Upon the mutual authentication, U_i and S can use this key K to encrypt/decrypt all communication messages in this session.

4.4. **The password change phase:** When U_i wants to update his/her password, he/she inserts smart card into the card reader and keys the old password pw_i and the new password pw_i', then the smart card computes $N_i' = N_i \oplus h(pw_i \parallel ID_i) \oplus h(pw_i' \parallel ID_i) = h(x \parallel y \parallel ID_i) \parallel h(pw_i' \parallel ID_i)$, and replaces the N_i with the new N_i'. Thus, the password can be changed. In addition, the remote serve doesn't need join this phase.

5. **Security analysis.** Next, we analyze the security of the improvement method as follows. We discuss the security of our scheme as follows.

5.1. **Anonymity:** In login phase of the proposed scheme, the user U_i sends CID_i, Z, and T_1 to the server S. Then, the server delivers $(D, T2)$ to the user U_i for the verification phase. These current parameters CID_i, Z, and D are various in each session because these parameters are embedded in current timestamp T_1 and T_2, where $CID_i = ID_i \oplus h(y \parallel T_1)$, $Z = h(CID_i \parallel h(x \parallel y \parallel ID_i) \parallel h(y) \parallel T_1)$, and $D = h(h(x \parallel y \parallel ID_i) \parallel T_2 \parallel K)$. Therefore, without knowing the secrets y, even if an attacker can obtain the current data CID_i, Z, and D in this phase, it is very hard for him to trace or identity the same user U_i for the next communication by means of CID_i, Z, and D. By the way, these parameters are indistinct on user's identity number ID_i so that the adversary does not know the real user's identities number ID_i. Since CID_i, Z, and D are different for U_i in each session, then, the adversary cannot easily trace the same user U_i from the information CID_i, Z, and D. Therefore, the proposed scheme can achieve user anonymity property.

5.2. **Replay attack:** Suppose that an adversary has interrupted a login information (CID_i, Z, T_1) between the server and the user, then he resends the login information (CID_i, Z, T_1) that have been previously transmitted by a legal user U_i. From the current timestamp T, the adversary will be detected by the server, since the validity of the information will be checked with the old timestamp T_1. The remote server will find illegal access and reject it. Hence, the replay attack will fail. Similarly, from the current timestamp, the attacker also cannot resend the K, D, and T_2 that have been previously transmitted by a legal sever S. Therefore, the proposed scheme can withstand the replay attack.

5.3. **Impersonation attack:** Suppose that an adversary wants to masquerade as a valid user and wants to login the remote server. To successfully perform the impersonation attack, the adversary is required to know y and $h(x \parallel y \parallel ID_i)$ for generating $CID_i = ID_i \oplus h(y \parallel T_1)$ and $Z = h(CID_i \parallel h(x \parallel y \parallel ID_i) \parallel y \parallel T_1)$. However, the adversary will fail, since it is impossible for him to obtain the user's password pw_i and y. Based on the secure hash function $h()$, it is difficult to find the information of x and y from (CID_i, Z).Without knowing the information x and y, the adversary cannot compute the exactly CID_i and Z in the login phase. Hence, the server will detect that he/she is an adversary. Then, the server will terminate this procedure. Similarly, without knowing the information of x and y, it is very hard for the attacker to masquerade the remote server. The probability of obtaining the exactly $CID_i = ID_i \oplus h(y \parallel T_1)$ and $Z = h(CID_i \parallel h(x \parallel y \parallel ID_i) \parallel y \parallel T_1)$ is equivalent to performing an exhaustive search on x and y. Therefore, the proposed scheme can withstand the impersonation attack.

Moreover, after a successful mutual authentication, the session key $K = h(h(x \parallel y \parallel ID_i) \parallel CID_i \parallel T_1 \parallel T_2 \parallel y)$ is constructed for U_i and the server. Then, even if an intruder obtains the current session key K, it is difficult for him to obtain these values x and y from K. That are protected under the hash function $h()$. Moreover, K is used for only one session. Therefore, the intruder cannot easily obtain private messages from the past. The improvement scheme can provide forward security even if the current session key K has been compromised.

6. **Conclusion.** In this paper, we propose a new efficient dynamic ID authentication scheme to improve Wang et al.s weaknesses. Our scheme is efficient since only one-way hash function and simple exclusive-or operators are involved in the protocol. It is very suitable for the mobile communications. With the user anonymity property and mutual authentication between the user and the server, the proposed scheme can provide more secure communication for the practical applications.

Acknowledgment. The author gratefully acknowledges the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] P. Shi, Limited Hamilton-Jacobi-Isaacs equations for singularly perturbed zero-sum dynamic (discrete time) games, *SIAM J. Control and Optimization*, vol.41, no.3, pp.826-850, 2002.

[2] A. K. Awasthi and S. Lal, "An enhanced remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 583-586, 2004.

[3] C. K. Chan, and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards",*IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 992-993, 2000.

[4] H. Y. Chien and C. H. Chen, "A remote authentication scheme preserving user anonymity",*the 19th International Conference on Advanced Information Networking and Applications (AINA 2005)*, Vol. 2, pp. 245-248, 2005.

[5] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 629-631, 2004.

[6] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[7] M. Kumar, "New remote user authentication scheme using smart cards",*IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 597-600, 2004.

[8] L. Lamport, "Password authentication with insecure communication", *Communications of the ACM* , Vol. 24, No. 11, pp. 770-772, 1981.

[9] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart card", *ACM operating Systems Review*, Vol. 36, No.3, pp. 46-52, 2002.

[10] M. Misbahuddin, M. A. Ahmed, A. A. Rao, C. S. Bindu, and M. A. M. Khan "A Novel Dynamic ID-Based Remote User Authentication Scheme", *2006 Annual IEEE India Conference*, pp. 1-5, 2006.

[11] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart card", *IEEE Transactions on Consumer Electronics*, Vol. 49, No.2, pp. 414-416, 2003.

[12] H. M. Sun, "An Efficient remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, 2000.

[13] Y. Wang, J. Liu , F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", *Computer Communications*, Vol. 32, No. 4, pp. 583-585, 2009.

[14] H. F. Huang and W. C. Wei, "A new efficient and complete remote user authentication protocol with smart cards," *International Journal of Innovative Computing, Information and Control*, Vol. 4, No. 11, pp. 2803-2808, 2008.

[15] X. Zhang, Q. Feng, M. Li, "A Modified Dynamic ID-based Remote User Authentication Scheme", *2006 International Conference on Communications, Circuits and Systems Proceedings*, Vol. 3, pp. 1602-1604, 2006.

[16] J. S. Lee, Y. F. Chang, and C. C. Chang, "A Novel Authentication Protocol for Multi-server Architecture without Smart Cards", *International Journal of Innovative Computing*, Information and Control, vol.4, no.6, pp.1357-1364, 2008.

[17] R. C. Wang, W. S. Juang, and C. L. Lei, "A Robust Authentication Scheme with User Anonymity for Wireless Environments", *International Journal of Innovative Computing*, Information and Control, vol.5, no.4, pp.1069-1080, 2009.

[18] W. G. Shieh and M. T. Wang, "An Improvement to Kim-Chung's Authentication Scheme", *ICIC Express Letters*, vol.3, no.4 (B), pp.1215-1220, 2009.