Improvement on Timestamp-based User Authentication Scheme with Smart Card Lost Attack Resistance

Heri Wijayanto[1,2], Min-Shiang Hwang[1,3]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung, Taiwan 41354, R.O.C
Department of Information Engineering, Mataram University[2]
No. 62, Majapahit Rd., Mataram, Indonesa
Department of Medical Research, China Medical University Hospital, China Medical University[3]
No.91, Hsueh-Shih Road, Taichung, Taiwan 40402, R.O.C.
(Email: heri@te.ftunram.ac.id)
(Received Nov. 12, 2014; revised and accepted Jan. 29, 2015)

Abstract

Smart card-based user authentication is a useful mechanism for performing private session over an insecure network. Tang et al have proposed a robust and efficient scheme in 2013 that is based on elliptic curve discrete logarithm problem (ECDLP). It is for eliminating the attack in Awasthi et al's scheme. However, Tang et al's scheme is still vulnerable to denial of service attack and off-line password guessing attack. In this paper, the weakness of Tang et al's scheme is presented. Furthermore, it gives the improvement of Tang et al's scheme, and is proposed for avoiding the possible attack in Tang et al's scheme.

Keywords: Authentication, ECDLP, password, smart card

1 Introduction

A user authentication scheme based on smart card is growing rapidly in this decade. It avoids a use of user authentication table that should be kept in the server [1, 4, 6, 8, 9, 11, 13, 14, 18]. Several types of the lightweight user authentications include password-based approaches, symmetric encryption approaches, public-key encryption approaches, ID-based approaches, and the hybrid approaches [2, 3, 5, 10, 15, 19].

In 2013, Tang et al proposed a user authentication that is based on Elliptic Curve Cryptography or ECC [16]. ECC is a public key cryptography (PKC) that is better than previous PKC scheme. It is because, in the same security level, ECC has a smaller key length than RSA or El-Gamal scheme [7, 17].

However, Tang et al's scheme security only depends on the secure hash function security because the private key of server stored in the smart card is wrapped by a secure hash function. Actually, guessing a message that is compressed by a secure hash function needs a long time, but it is still not proper to store the secret key of server in all users' smart cards. The server secret key must be changed periodically for a security reason that is impossible to do in Tang et al's scheme because changing the secret key mechanism is not provided in Tang et al's scheme.

Besides that, Tang et al's scheme is also vulnerable to DoS attack. Denial of service (DoS) attack is the type of attack that exhausts a victim's resources by sending large amounts of packets or requests [5]. Therefore, the victim's computer will be lack of resources and cannot serve clients properly. In this unstable condition, the system will be vulnerable for other attacking protocols.

The remaining sections of this paper are organized as follows. Section 2 gives a brief review one of Tang et al's schemes and describes its weaknesses. In Section 3, we propose the improved scheme. In section 4, the security analysis of our scheme is given. Finally, Section 6 concludes the paper.

2 Brief Review of Tang's Scheme

Tang et al's scheme is based on ECDLP that improves Awasthi et al's scheme [16]. This scheme consists of four phases. There are system setup phase, registration phase, login phase, authentication phase, and password change phase. This section describes about Tang et al's scheme and its cryptanalysis as follows.

2.1 Tang et al's Scheme

In this step, all users and server agree on ECC parameters that will be used in this scheme. The server chooses a secret key x and computes $Q = x \cdot P$. Then server keeps x secret and publishes p, a, b, n, P, h, and Q.

This registration phase consists of three steps. In the first step, User U_i chooses identity ID_i and password PW_i freely. Then, he or she selects a random number N, and computes $HPW = h(PW_i||N)$. Next, U_i sends the ID_i and HPW to server S through a pre-established secure channel.

In the second step, S computes $V_i = h(ID_i||x) \oplus h(PW_i||N)$, stores $(V_i, h(\cdot))$ in smart card, and issues the smart card to U_i through secure channel. S also maintains an ID table that contains ID_i and status bit.

In the third step, after receiving the smart card, U_i stores N into a smart card. When U_i wants to log into a remote server S, U_i enters ID_i and PW_i. Then a smart card will do these two steps. First, the smart card computes $s = V_i \oplus h(PW_i||N)$, select a random $r_1 \in Z_n^*$, computes $R_1 = r_1 \cdot P$, $R_2 = r_1 \cdot Q$, and computes $V_1 = h(ID_i||R_1||R_2||s||T_c)$ where T_c is the timestamp at the login device. Actually, s is same with $h(ID_i||x)$ because $h(ID_i||x) \oplus h(PW_i||N) \oplus h(PW_i||N)$ is equal to $h(ID_i||x)$. Second, U_i sends $M_1 = (ID_i, R_1, V_1, T_c)$ to the server S through a common channel.

The third is the authentication phase that is divided into four steps. Step one, server S checks ID_i, status-bit, and T_c. If those three parameters pass the checking criteria, then continues to step two. If not, S will informs U_i about the failure. Step two, S sets the status bit to be 1, computes $R_2' = x \cdot R_1 = x \cdot r_1 \cdot P = r_1 \cdot Q$ and $s' = h(ID_i||x)$. Then S constructs $V_1' = h(ID_i||R_1||R_2'||s'||T_c)$. If V_1 is not equal to V_1', S rejects the login request and informs the user about it. On the other hand, S authenticates U_i and computes $V_2 = h(S||ID_i||R_2'||s'||T_s')$ and sends $M_2 = (V_2, T_s')$ to U_i. Steps three and four, after receiving M_2, U_i checks T_s' and V_2 by the similar way. In the end of the session, S the set status-bit to zero.

In the fourth phase or Password Change Phase, firstly, U_i needs to performs the Login Phase procedure and if it passes, U_i inputs the new password PW_i^*. In the step two, the smart card selects a random number N' and computes $V_i' = V_i \oplus h(PW_i||N) \oplus h(PW_i * ||N')$, and replaces V_i and N with the new V_i' and N'.

2.2 Cryptanalysis of Tang et al's Scheme

Tang et al's scheme is based on ECC that has two weaknesses. There are DoS attack and off-line password guessing attack.

2.2.1 DoS Attack

The main purpose of denial of service attack is turning off a service. Tang et al's scheme does not hide the ID in the login phase. The attacker can guess or steal it easily from an unsecured network connection. Then attackers will try the normal login by using stolen users ID or guessing ID, current T_c, and anything R_1, and V_1. This request will pass the ID checking and the status-bit of this ID is set to be one. Then, attackers will do the same way with different guessing ID's until all legal users can not use this service.

2.2.2 Off-Line Password Guessing Attack

In the Tang et al's scheme the secret key (x) of server is transmitted even though this is wrapped by secure hash function. In the other words, this scheme security does not depend on ECC but it is only based on the secure hash function security. Therefore, by finding the collision, the complexity of secure hash function will be decreased. There are some methods for attacking secure hash function such as Birthday attack, Joux's attack, and multi-collision attack [12].

3 The Proposed Scheme

In this paper, we propose an improvement of Tang et al's scheme. We add session key (R_2) and EC digital signature scheme.

3.1 System Setup Phase

This phase is equal to Tang et al's scheme. Server selects a secret key x and computes $Q = x \cdot P$ and keeps secret key x. After that, server publishes the public keys parameters p, a, b, P, n, h, and Q. In our scheme, server also saves random numbers k_i and M_i for ECC digital signature.

3.2 Registration Phase

Figure 1 shows the registration phase. It is done by users once in the first time they log-in to the server. Similar with Tang et al's scheme, it also uses secure communication line. It consists of three steps as follows:

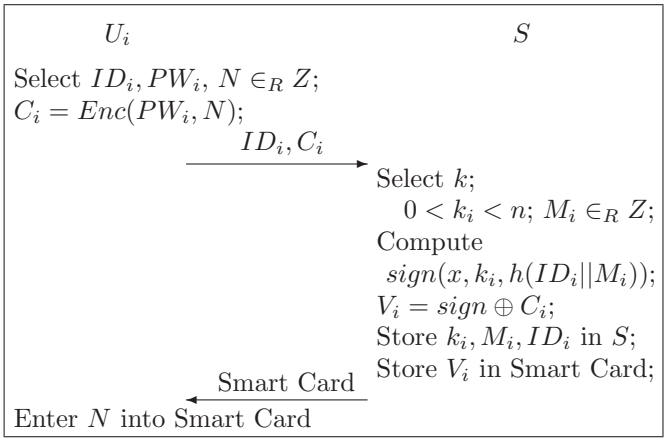

Figure 1: The registration phase of the proposed scheme

Step 1. User U_i selects an identity ID_i, password PW_i, and also a high entropy random number N. Then, users encrypt N by password PW_i as a symmetric key cryptography $C_i = Enc(PW_i, N)$. Next, user sends ID_i and C_i to the server through a secure channel.

Step 2. After receiving ID_i, and C_i, server selects a random number k_i that $0 < k_i < n$ and also a high entropy random number M_i. Next, server computes an EC digital signature by secret key x, and hash function of concatenation of ID_i and M_i as $sign(x, k_i, h(ID_i||M_i))$, for a short we call it sign. Then, server computes $V_i = sign \oplus C_i$, stores V_i into smart card and sends it back to user U_i through secure channel. Finally, server maintains an ID table that contains ID_i, status-bit, k_i, and M_i.

Step 3. After receiving a smart card, user inputs N into smart card.

3.3 Login Phase

In the login phase, the interaction between users and server utilize a common channel. Firstly, user inputs his or hers identity ID_i and password PW_i into a smart card. Then smart card computes $s = V_i \oplus C_i$ that equals to sign because $V_i = sign \oplus C_i$. Secondly, and the smart card chooses a random nonce $r_1 \in_R Z_n^*$, and computes $R_1 = r_1 \cdot P$, and $R_2 = r_1 \cdot Q$. Thirdly, the smart card encrypts $C_1 = ENC(R_2, ID_i||R_1||R_2||s||T_c)$ then sends R_1 and C_1 to server. This phase is shown in Figure 2.

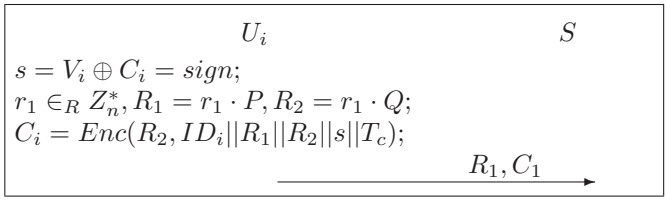

Figure 2: The login phase of the proposed scheme

3.4 Authentication Phase

The password change phase is shown in Figure 3. When a log-in requests that are R_1 and C_1 arrive to the Server S, S will do four passes that are described as bellow.

Pass 1. Server S computes the session key R_2' by secret key x as $R_2' = x \cdot R_1$. Then, Server decrypts C_1 by R_2', and this result is $ID_i||R_1||R_2||s||T_c$. If this decryption fail to produce those parameters, this login phase is rejected, and informs sender.

Pass 2. S checks the ID_i in the database. If this ID is not available in the database, S will reject this request and informs U_i in encrypted text by password R_2'.

Pass 3. S checks status-bit. If status-bit is equal to one, server rejects this request and informs U_i about it in encrypted text by password R_2', otherwise, server sets it to one.

Pass 4. S checks T_c. If $(T_s - T_c) \leq 0$ or $(T_s - T_c) > \triangle T$ server rejects this request and informs U_i in encrypted text by password R_2'.

Pass 5. Server computes its signature as $s' = sign(x, k_i, h(ID_i||M_i))$ and compares it with s. If those are not equal, S rejects this request and informs U_i about it. Otherwise, U_i has passed this authentication phase in the server side. And then, S encrypts $S||T_s$ by R_2' and sends back C_2 to user U_i in encrypted text by password R_2'. The next steps are done in the user side. U_i decrypts C_2 by R_2 and check S and T_c by the same way as server did. If those parameters do not satisfy the requirement criteria, U_i will reject this session.

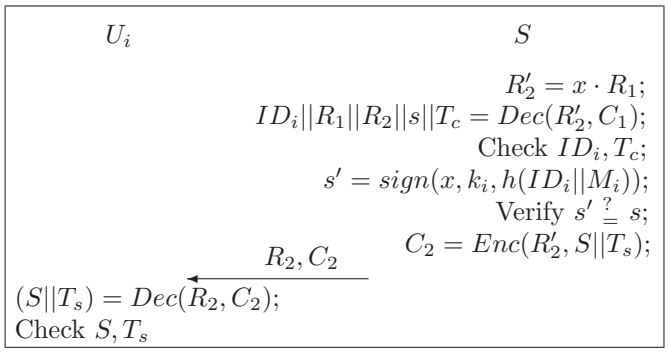

Figure 3: The authentication phase of the proposed scheme

3.5 Password Change Phase

When U_i wants to change his or her password for some reasons. U_i should keys his or her identity ID_i and password PW_i to a smart card first before changing the password. After that, Smart card will perform login protocol and if the login process is successful, U_i can input the new password $PW_{i,new}$. After that, the smart card generates new random number N_{new} and computes $V_i = V_i \oplus Enc(PW_i, N) \oplus Enc(PW_{i,new}, N_{new})$. Next, the smart card replaces V_i and N by $V_{i,new}$ and N_{new}. Finally, the smart card informs U_i that changing password is success.

4 Security Analysis

This proposed scheme also resists all attack explained in Tang et al's scheme [16]. In addition, this paper focuses to explain more about DoS attack and offline password guessing attack.

1) The Proposed Scheme Resists of DoS Attack.
In this scheme, User's ID is encrypted by using symmetric key cryptography before it is transmitted over an unsecured communication line. Therefore, attackers cannot steal it or guess it for DoS attack explained in Section 2.2.1 above. This improvement also fulfills the purpose of Chang et al's scheme [1].

2) The Proposed Scheme Resists of Offline Password Guessing Attack.
The weakness of Tang et al's scheme presented in Section 2.2.2 is storing hash value of the concatenation between user identity ID_i and server secret key x in the smart card. It is because of knowing x, the entire system will be down. In this proposed scheme, the secret key of elliptic curve cryptography (x) is not stored in the user's smart card. In this scheme, this hash value is replaced by EC signature.

5 Conclusions

In this paper, the weaknesses of a timestamp-based user authentication scheme with the smart card losing attack resistance have been discussed. Furthermore, the improvement of Tang et al's scheme is given by adding the session key and digital signature that are still based on the elliptic curve cryptography. Therefore, this scheme resists the denial of service attack and also offline password guessing attack.

Acknowledgments

This study was supported by the Ministry of Science and Technology of Taiwan under grant NSC102-2811-E-468 -001, MOST103-2622-E-468-001-CC2, and MOST103-2622-H-468-001-CC2. The authors gratefully acknowledge the anonymous re- viewers for their valuable comments.

References

[1] Chin-Chen Chang and Chia-Yin Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139–147, 2013.

[2] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environ-ments," *International Journal of Network Security*, vol. 16, no. 4, pp. 318–321, 2014.

[3] D. He, W. Zhao, and S. Wu, "Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards," *International Journal of Network Security*, vol. 15, no. 5, pp. 282–292, 2013.

[4] Debiao He, Jianhua Chen, and Jin Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.

[5] Min-Shiang Hwang, Song-Kong Chong, and Te-Yu Chen, "Dos-resistant id-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, pp. 163–172, Jan. 2010.

[6] Min-Shiang Hwang, Jung-Wen Lo, Chi-Yu Liu, and Shu-Chen Lin, "Cryptanalysis of a user friendly remote authentication scheme with smart card," *Pakistan Journal of Applied Sciences*, vol. 5, no. 1, pp. 99–100, 2005.

[7] Min-Shiang Hwang, Shiang-Feng Tzeng, and Chwei-Shyong Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[8] M. Kumar, M. K. Gupta, and S. Kumari, "An improved efficient remote password authentication scheme with smart card over insecure networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 167–177, 2011.

[9] Manoj Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.

[10] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[11] C. T. Li and Min-Shiang Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, pp. 1–5, 2010.

[12] M. Nandi and D. R. Stinson, "Multicollision attacks on some generalized sequential hash functions," *IEEE Transcactions on Information Theory*, vol. 53, pp. 759–767, Feb. 2007.

[13] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, vol. 14, no. 3, pp. 180–186, 2012.

[14] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[15] S. K. Sood, A. K. Sarje, and K. Singh, "Inverse cookie-based virtual password authentication protocol," *International Journal of Network Security*, vol. 13, no. 2, pp. 98–108, 2011.

[16] H. B. Tang, X. S. Liu, and L. Jiang, "A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance," *International Journal of Network Security*, vol. 15, pp. 446–454, Nov. 2013.

[17] Shiang-Feng Tzeng and Min-Shiang Hwang, "Digital signature with message recovery and its vari-

ants based on elliptic curve discrete logarithm problem," *Computer Standards & Interface*, vol. 26, no. 2, pp. 61–71, 2004.

[18] L. Yang, J. F. Ma, and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing," *International Journal of Network Security*, vol. 14, no. 3, pp. 156–163, 2012.

[19] X. Zhuang, C. C. Chang, Z. H. Wang, and Y. Zhu, "A simple password authentication scheme based on geometric hashing function," *International Journal of Network Security*, vol. 16, no. 4, pp. 271–277, 2014.

Heri Wijayanto earned his BS and MS degrees in Electrical Engineering Gadjah Mada University Indonesia in 1998 and 2002. He works as a lecturer in Mataram University Indonesia since 2002 and currently, he continues his study in Computer Science and Information Engineering, Asia University Taiwan started in 2014. His research interest are data mining, and computer security.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China (ROC), in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field Electronic Engineer in 1988. He also passed the National Telecommunication Special Examination in field Information Engineering, qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He is currently a chair professor of the department of Computer Science and Information Engineering, Asia University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 200+ articles on the above research fields in international journals.