Cryptanalysis of Kumar's Remote User Authentication Scheme with Smart Cards

Min-Shiang Hwang
Depart. of Computer Science & Inf. Eng.
Asia University
Taichung, Taiwan
and
Department of Medical Research
China Medical University Hospital
China Medical University, Taichung, Taiwan
Email: mshwang@asia.edu.tw

Eko Fajar Cahyadi
Depart. of Computer Science & Inf. Eng.
Asia University
Taichung, Taiwan
and
Department of Telecommunication Engineering
Institut Teknologi Telkom Purwokerto, Indonesia

Chia-Chun Wu*
Department of Industrial Engineering and Management,
National Quemoy University, Quemoy, Taiwan
Corresponding Author: Email: ccwu0918@gmail.com

Cheng-Ying Yang
Department of Computer Science
University of Taipei
Taipei, Taiwan

***Abstract*—One of the common needs to have secret communication through Internet is to authenticate the legality of users. The simplest and most popular authentication technique to have secret communication through Internet is the remote user authentication scheme. Recently, Kumar proposed an enhanced smart card-based remote user authentication scheme. Kumar's scheme was robust and easy to implement. Kumar claimed that his scheme could withstand explicit key authentication, replay attacks, stolen-verifier attacks, forward secrecy, denial of service attacks, impersonation attacks, mutual authentication, parallel session attack, password guessing attacks, smart card loss attacks, attacks via registered identity, and attacks via password. In this article, we will show that Kumar's scheme is vulnerable to the off-line guessing password attack. In this article, we also propose an improved Kumar's enhanced smart card-based remote user authentication scheme to withstand the vulnerability in their scheme.**

***Keywords*-password; smart card; tamper-proof; user authentication;**

I. INTRODUCTION

One of the common needs to have secret communication through Internet is to authenticate the legality of users [1], [2], [3]. The simplest and most popular authentication technique to have secret communication through Internet is a remote user authentication scheme [4], [5], [6].

In general, the basic requirement of the user authentication is able to withstand replay attack, denial of service attacks, impersonation attacks, password guessing attacks, etc. [7], [8], [9], [10], [11], [12], [13]. Many user authentication schemes have been proposed. In decades, a smart card-based user authentication has been proposed for resisting the guessing attacks [14], [15], [16], [17], [18], [19]. In order to prevent the smart card loss and stolen-verifier attacks, integrating biomatrics to the smart card has been proposed [20], [21], [22], [23], [24], [25], [26]. The other types of user authentication schemes include NFC [27], [28], [29], RFID [30], [31], [32], [33], etc.

Recently, Kumar proposed an enhanced smart card-based remote user authentication scheme [34]. Kumar's scheme was robust and easy to implement. Kumar claimed that his scheme could withstand explicit key authentication, replay attacks, stolen-verifier attacks, forward secrecy, denial of service attacks, impersonation attacks, mutual authentication, parallel session attacks, password guessing attacks, smart card loss attacks, attacks via registered identity, and attacks via password. In this article, we will show that Kumar's scheme is vulnerable to the off-line guessing password attack, and also propose an improved Kumar's user authentication scheme to withstand the vulnerability in his scheme.

The rest of this paper is organized as follows: In Section 2, we briefly review Kumar's enhanced smart card-based remote user authentication scheme. In Section 3, we analyze and show that some security flaws exist in Kumar's enhanced smart card-based remote user authentication scheme. In Section 4, we propose an improvement of Kumar's user authentication scheme. Finally, we present our conclusions in Section 5.

II. REVIEW OF KUMAR'S SCHEME

In this section, we briefly review Kumar's enhanced smart card-based remote user authentication scheme [34]. There are three participants in Kumar's enhanced smart card-based remote user authentication scheme: Remote Users ($U_i, i = 1, 2, \cdots, n$ for short); Smart Card Reader (SC for short); Authentication Server (AS for short). The scheme consists of four phases, namely the registration, the login, the

verification, and the password change phases. The notations used in this article are listed in Table I.

Table I
LIST OF NOTATION USED

Symbol	Description
U_i	The i-th User.
ID_i	The identity of U_i.
PW_i	The password of U_i.
AS	The authentication server.
x_s	The secret key of AS.
$f(\cdot)$	A one way hash function.
$\oplus$	An XOR operation.
p	A large prime number.
S_{ID_i}	The redirected identity of ID_i.
C_{ID_i}	A check sum of ID_i.
$Red(ID_i)$	A function to redirect the identity of ID_i.
$C_K(S_{ID_i})$	A function to generate check sum of S_{ID_i}.

A. Registration Phase of Kumar's Scheme

In the registration phase, the user (U_i) registered to the server (AS) by providing his/her personal unique information over a secure channel. The server AS will generate some secret parameters and store them in a smart card for the user. This phase is executed in the following.

Step R_1:The user send the registration request and his/her personal unique identification information ID_i to the server AS.

Step R_2: Upon receiving the registration request, the AS calculate S_{ID_i}, C_{ID_i}, PW_i, and R by

$$\begin{aligned} S_{ID_i} &= Red(ID_i), \\ C_{ID_i} &= C_K(S_{ID_i}), \\ PW_i &= (S_{ID_i})^{x_s} \bmod p, \\ R &= S_{ID_i} \oplus PW_i. \end{aligned}$$

Where $Red(ID_i)$ is a function to redirect the user's identity ID_i; S_{ID_i} is a redirected identity of ID_i; $C_K(S_{ID_i})$ is a function to generate check sum of S_{ID_i}; C_{ID_i} is a checksum of ID_i; x_s is AS's secret key; p is a large prime number; PW_i is U_i's password.

Step R_3:The server sends $(ID \| C_{ID_i}, PW_i)$ and a smart card to the user. The smart card contains the parameters: $\{f, p, f(S_{ID_i}), R\}$.

B. The Login Phase of Kumar's Scheme

Whenever the user U_i wants to access resources on the AS, U_i attaches his/her smart card to the terminal device and inputs his/her Personal Identification Number (PIN) to make the smart card active. If the *PIN* code is entered incorrectly for three times, the smart card terminates itself to be inactive.

The user U_i inputs the pair of his/her identity $ID_i \| C_{ID_i}$ and password PW_i'. The smart card executes the following.

Step L_1:The smart card computes

$$f(S'_{ID_i}) = f(R \oplus PW_i').$$

Next, the smart card checks $f(S'_{ID_i})$ and the $f(S_{ID_i})$ stored in the smart card. If they are equal, the smart card accepts the password and proceeds to the next step.

Step L_2:The smart card computes C_1, t, and M by

$$\begin{aligned} C_1 &= (R \oplus S_{ID_i})^r \bmod p; && (1) \\ t &= f(T_u \oplus PW_i) \bmod (p-1); && (2) \\ M &= (S_{ID_i})^t \bmod p; && (3) \\ C_2 &= M(PW_i)^r \bmod p. && (4) \end{aligned}$$

Where r denotes a random number which generated by the smart card; T_u denotes the current time of the smart card.

Step L_3: The user U_i sends $L_R = \{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$ to the server AS.

C. The Verification Phase of Kumar's Scheme

Whenever the server *AS* receives the login request $\{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$, the server *AS* verifies the legality of the user with the login request message in the following steps.

Step V_1:The server checks the identity ID_i and the timestamp T_u. If the format of ID_i and the timestamp T_u are in the reasonable time interval, the server proceeds to the next step. Otherwise, the server rejects the login request L_R.

Step V_2: The server computes $C_K(S_{ID_i})$ and compares C_{ID_i} in the login request L_R by

$$C'_{ID_i} = C_K(Red(ID_i)).$$

The server checks whether $C_{ID} = C'_{ID_i}$ holds, if not, the server *AS* rejects the login request L_R.

Step V_3:The server computes PW_i, t, and C_2' by

$$\begin{aligned} PW_i &= R \oplus S_{ID_i} \\ t &= f(T_u \oplus PW_i) \bmod (p-1) \\ C_2' &= (C_1)(S_{ID_i})^t \bmod p. \end{aligned}$$

Next, the server checks whether C_2 and C_2' are equal. If they are not equal, the server rejects the login request.

Step V_4:The server *AS* computes C_3, C_4, and C_5 by

$$\begin{aligned} C_3 &= f(C_1^{x_s} \oplus T_s), \\ S_{key} &= f(C_1^{x_s}, T_s, r_1), \\ C_4 &= C_3 \oplus r_1, \\ C_5 &= C_3 \oplus S_{key}. \end{aligned}$$

Where r_1 is a random number, and T_s is the current time of the server *AS*.

Step V_5: The server sends the mutual authentication message $\{C_4, C_5, T_s\}$ to the user U_i.

Step V_6: Whenever the U_i receives the mutual authentication message (C_4, C_5, T_s), the smart card executes in the following.

1) The smart card checks the timestamp T_s. If the timestamp is in the reasonable time interval, the smart card proceeds to the next step. Otherwise, the smart card terminates this connection.
2) The smart card computes the following parameters:

$$\begin{aligned} C_3^* &= f(C_2 M^{-1} \oplus T_s). \\ r^* &= C_3^* \oplus C_4. \\ S_{key}^* &= C_3^* \oplus C_5. \\ S_{key}^{**} &= f(C_2 M^{-1}, T_s, r^*). \end{aligned}$$

3) The smart card checks S_{key}^* and S_{key}^{**}. If they are equal, the user U_i confirms the identity of the server, and S_{key}^* will be the session secret key between U_i and the server. Otherwise, the smart card terminates this connection.

Step V_7: The user computes C_6 and sends the session key authentication (ID_i, C_6) to the server,

$$C_6 = f(C_3^*, S_{key}^*).$$

Step V_8: The server checks C_6. If C_6 is equal to $f(C_3, S_{key})$, the server assures that S_{key} is the session key shared by the server and the user U_i.

III. Cryptanalysis of Kumar's Scheme

In this section, we will analyze Kumar's remote user authentication scheme with smart cards [34]. Kumar claimed that his scheme can resist different possible attacks including smart card stolen attacks, impersonation attacks, privileged insider attacks, replay attacks, off-line password guessing attacks, theft attacks, session key recovery attacks, denial of service attacks, and cluster head capture attacks. In this section, we show that Kumar's user authentication scheme is vulnerable to off-line guessing password attacks.

A. Off-line Password Guessing Attacks

In this section, we will show that Kumar's scheme is vulnerable to off-line password guessing attacks.

The adversary is able to intercept from the public Internet. If the adversary obtains a login request message $L_R = \{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$ between the user U_i and the server AS in the Step L_3 of Kumar's scheme. The adversary guesses the user's password PW_i' and verifies it as follows:

$$\begin{aligned} S'_{ID_i} &= R \oplus PW_i' \\ t' &= f(T_u \oplus PW_i') \bmod (p-1) \\ M' &= (S_{ID_i})^t \bmod p. \end{aligned}$$

From Equations 1 and 4, the adversary obtains:

$$\begin{aligned} C_1 &= (R \oplus S_{ID_i})^r \bmod p \\ &= (S_{ID_i} \oplus PW_i \oplus S_{ID_i})^r \bmod p \\ &= PW_i^r \bmod p. \\ \frac{C_2}{M'} &= \frac{M(PW_i)^r}{M'} \bmod p. \\ &= C_1' \end{aligned}$$

The adversary checks both C_1 and C_1'. If they are equal, the guessing password PW_i' is the U_i's password PW_i. Otherwise, the adversary repeatedly guesses the other password and verifies it in the same way. Since the length of password is shorter to easily remember, the adversary will guess the legal user's password in the valid time.

IV. The Improvement of Kumar's Scheme

The main weakness of Kumar's remote user authentication scheme is that the adversary could derive the password from the login request message $L_R = \{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$. In the improved Kumar's user authentication scheme, the registration phase is the same as that of Kumar's scheme.

A. The Login Phase of the improved Kumar's Scheme

The user U_i inputs the pair of his/her identity $ID_i \| C_{ID_i}$ and password PW_i. The smart card executes the following steps:

Step L_1: This step is same as that of Kumar's scheme.

Step L_2:The smart card computes C_1, t, and M as follows:

$$\begin{aligned} C_1 &= (S_{ID_i})^r \bmod p; \\ t &= f(T_u \oplus PW_i) \bmod (p-1); \\ C_2 &= t(PW_i)^r \bmod p. \end{aligned}$$

Step L_3: The user U_i sends $L_R = \{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$ to the server AS.

B. The Verification Phase of Improved Kumar's Scheme

Whenever the server *AS* receives the login request $\{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$, the server *AS* verifies the legality of the user with the login request message in the following steps.

Steps V_1 and V_2: The steps are the same as those of Kumar's scheme.

Step V_3:The server computes PW_i, t, and C_2' as follows:

$$\begin{aligned} PW_i &= R \oplus S_{ID_i} \\ t &= f(T_u \oplus PW_i) \bmod (p-1) \\ C_2' &= t(C_1^{x_s}) \bmod p. \end{aligned}$$

Next, the server checks whether C_2 and C_2' are equal. If there are not equal, the server rejects the

login request. We show the correction as follows:

$$\begin{aligned} C_2' &= t(C_1^{x_s}) \bmod p. \\ &= t((S_{ID_i})^r)^{x_s} \bmod p. \\ &= t(PW_i)^r \bmod p \\ &= C_2 \end{aligned}$$

Steps V_4 - V_8: These steps are the same as those of Kumar's scheme.

C. Security Analysis of Improved Kumar's Scheme

The adversary is able to intercept from the public Internet. If the adversary obtains a login request message $L_R = \{ID_i \| C_{ID_i}, C_1, C_2, R, T_u\}$ between the user U_i and the server AS in the Step L_3 of improved Kumar's scheme, the adversary can guess the user's password PW_i' and verifies it as follows:

$$\begin{aligned} S_{ID_i}' &= R \oplus PW_i' \\ t' &= f(T_u \oplus PW_i') \bmod (p-1) \\ (PW_i)^r &= \frac{C_1}{t'} \bmod p. \end{aligned}$$

From the above equations, the adversary could obtain $(PW_i)^r \bmod p$, S_{ID_i}', $C_1 = S_{ID_i}^r \bmod p$, $C_2 = t(PW_i)^r$, and PW_i'. Since the adversary does not know the server's secret key x_s, the adversary is unable to guess the password from C_1 and $PW_i^r \bmod p$. Therefore, the improved Kumar's user authentication scheme can withstand the off-line guessing password attack.

V. Conclusion

In this article, we have reviewed Kumar's enhanced smart card-based remote user authentication scheme [34] and have analyzed its security. We have showed that Kumar's user authentication scheme cannot withstand the off-line guessing password attack. We also propose an improvement of Kumar's Scheme to resist the weakness.

Acknowledgment

This study was supported by the National Science Council of Taiwan under grant MOST 106-3114-E-005-001, MOST 107-2221-E-845-002-MY3, and MOST 107-2221-E-845-001-MY3.

References

[1] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", *International Journal of Informatica*, vol. 12, no. 2, pp. 297-302, 2001.

[2] C. S. Tsai, C. C. Lee, M. S. Hwang, "Password authentication schemes: Current status and key issues", *International Journal of Network Security*, vol. 3, pp. 101-115, 2006.

[3] S. K. Sood, A. K. Sarje, K. Singh, "Inverse cookie-based virtual password authentication protocol", *International Journal of Network Security*, vol. 13, no. 2, pp. 172-181, 2016.

[4] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm", *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, 2016.

[5] G. Hou, Z. Wang, "A robust and efficient remote authentication scheme from elliptic curve cryptosystem", *International Journal of Network Security*, vol. 19, no. 6, pp. 904-911, 2017.

[6] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703-714, 2005.

[7] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an efficient password authentication scheme", *International Journal of Network Security*, vol. 18, no. 2, pp. 362-368, 2016.

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

[9] R. Amin, "Cryptanalysis and efficient dynamic id based remote user authentication scheme in multi-server environment using smart card", *International Journal of Network Security*, vol. 18, no. 1, pp. 172-181, 2016.

[10] 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. 350-356, 2013.

[11] Y. Wang and X. Peng, "Cryptanalysis of two efficient password-based authentication schemes using smart cards", *International Journal of Network Security*, vol. 17, no. 6, pp. 728-735, 2015.

[12] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on an anonymous multi-server authenticated key agreement scheme based on trust computing using smart card and biometrics", *International Journal of Network Security*, vol. 18, no. 5, pp. 997-1000, 2016.

[13] M. Stanek, "Weaknesses of password authentication scheme based on geometric hashing", *International Journal of Network Security*, vol. 18, no. 4, pp. 798-801, 2016.

[14] M. S. Hwang, 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.

[15] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments", *The Journal of Supercomputing*, vol. 66, no. 2, pp. 1008-1032, 2013.

[16] H. Tang, X. Liu, 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, no. 6, pp. 360-368, 2013.

[17] H. F. Huang, H. W. Chang, P. K. Yu, "Enhancement of timestamp-based user authentication scheme with smart card", *International Journal of Network Security*, vol. 16, pp. 463-467, 2014.

[18] J. Moon, D. Lee, J. Jung, D. Won, "Improvement of efficient and secure smart card based password authentication scheme", *International Journal of Network Security*, vol. 19, pp. 1053-1061, 2017.

[19] Y. Liu, C. C. Chang, S. C. Chang, "An efficient and secure smart card based password authentication scheme", *International Journal of Network Security*, vol. 19, no. 1, pp. 1-10, 2017.

[20] E. Tarek, O. Ouda, A. Atwan, "Image-based multimodal biometric authentication using double random phase encoding", *International Journal of Network Security*, vol. 20, no. 6, pp. 1163-1174, 2018.

[21] L. Han, Q. Xie, W. Liu, "An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem", *International Journal of Network Security*, vol. 19, no. 3, pp. 469-478, 2017.

[22] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards", *International Journal of Network Security*, vol. 18, no. 6, pp. 1010-1021, 2016.

[23] H. Zhu, Y. Zhang, H. Li, L. Lin, "A novel biometrics-based one-time commitment authenticated key agreement scheme with privacy protection for mobile network", *International Journal of Network Security*, vol. 18, no. 2, pp. 209-216, 2016.

[24] H. Zhu, Y. Zhang, X. Wang, "A novel one-time identity-password authenticated scheme based on biometrics for e-coupon system", *International Journal of Network Security*, vol. 18, no. 3, pp. 401-409, 2016.

[25] P. Annamalai, K. Raju, D. Ranganayakulu, "Soft biometrics traits for continuous authentication in online exam using ica based facial recognition", *International Journal of Network Security*, vol. 20, no. 3, pp. 423-432, 2018.

[26] A. Prakash, R. Dhanalakshmi, "Stride towards proposing multi-modal biometric authentication for online exam", *International Journal of Network Security*, vol. 18, no. 4, pp. 678-687, 2016.

[27] Y. Ma, "NFC communications-based mutual authentication scheme for the internet of things", *International Journal of Network Security*, vol. 19, no. 4, pp. 631-638, 2017.

[28] J. Ling, Y. Wang, W. Chen, "An improved privacy protection security protocol based on NFC", *International Journal of Network Security*, vol. 19, no. 1, pp. 39-46, 2017.

[29] Y. L. Chi, C. Chen, I. C. Lin, M. S. Hwang, "The secure transaction protocol in NFC card emulation mode", *International Journal of Network Security*, vol. 17, no. 4, pp. 431-438, 2015.

[30] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20-24, 2011.

[31] S. Y. Chiou, W. T. Ko, E. H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and its application", *International Journal of Network Security*, vol. 20, no. 2, pp. 396-402, 2018.

[32] P. Y. Cui, "An Improved ownership transfer and mutual authentication for lightweight RFID protocols", *International Journal of Network Security*, vol. 18, no. 6, pp. 1173-1179, 2016.

[33] N. Chikouche, F. Cherif, P. L. Cayrel, M. Benmohammed, "Improved RFID authentication protocol based on randomized McEliece cryptosystem", *International Journal of Network Security*, vol. 17, no. 4, pp. 413-422, 2015.

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