ICIC Express Letters
Volume **11**, Number **1**, January **2017**

ICIC International ©2017 ISSN 1881-803X
pp. **59–64**

A NEW SCHEME OF REMOTE USER AUTHENTICATION USING SMART CARDS

Ping Yu and Wen-Gong Shieh

Department of Information Management
Chinese Culture University
No. 55, Hwa Kang Road, Yang Ming Shan, Taipei 11114, Taiwan
{ yp; wgshieh }@faculty.pccu.edu.tw

Received June 2016; accepted September 2016

Abstract. *Recently, Chen et al. proposed an authentication scheme to secure remote access against the risk of attacks over an insecure environment. The scheme provides mutual authentication, session key agreement, and forward secrecy. However, as reported by many researchers, Chen et al.'s scheme is vulnerable to the offline password-guessing attack, if the contents of the smart card and messages in the non-secure network are revealed. With the contents of the smart card and the successfully guessed password, an attacker can impersonate the user to login into the server. In addition, we point out that the scheme does not maintain the forward secrecy property. Once the user's password, a long-term secret, is compromised, it would reveal all old short-term session keys used before. Therefore, in order to avoid the above attacks, we propose a new scheme that uses the user's biometrics such as a fingerprint to avoid the weaknesses caused by the loss of the smart card.*

Keywords: Authentication, Smart card, Offline password-guessing, Forward secrecy, Biometrics

1. **Introduction.** Remote user authentication is an important issue for network applications. Since Lamport [1] proposed a remote authentication scheme in 1981, many researchers have reported their schemes to improve the efficiency and security in this field. User authentication usually depends on identities and passwords that can be forgotten, disclosed, lost or stolen. On the contrary, the distinguishing feature of biometrics, such as fingerprints, faces, and irises, provides a more reliable method to verify the user based on physiological characteristics which are universal, unique and difficult to duplicate, lose or forget. In 2010, Li and Hwang [2] proposed a biometric-based authentication scheme. Das [3] showed that the scheme contains some design flaws and proposed an improved scheme. In 2011, Sood et al. [4] proposed a scheme that is a dynamic identity based authentication protocol for a multi-server architecture. Chen et al. [5] proposed a remote authentication scheme using smart card with session key agreement, mutual authentication, and forward secrecy. However, Chen et al.'s scheme is still vulnerable to the offline password-guessing attack [6,7]. Besides, we also find that Chen et al.'s scheme does not provide perfect forward secrecy. In 2014, Sarvabhatla et al. [8] showed a secure biometrics-based scheme that is still vulnerable to user impersonation and offline password guessing attack. In 2015, Odelu et al. [9] proposed an ECC-based scheme to provide low computational and communication costs. In 2016, Jung et al. [10] proposed a scheme which is only based on the hash function to provide more efficiency and security than previous schemes.

In order to eliminate the security vulnerability of Chen et al.'s scheme to avoid the leakage of the lost smart card, we propose a new mutual authentication scheme that uses the biometrics to avoid the attack of offline password guessing and provides more reliable identification information to solve the lost/stolen smart card and non-secure network problems. In our scheme, we do not use keyed hash function but use both timestamps and challenge/response to avoid reply attack and session key partial forward secrecy is achieved. The remainder of this paper is presented as the following. In the next section, a brief review of Chen et al.'s scheme is given. After that, we point out the weakness of Chen et al.'s scheme in Section 3. Our new scheme is proposed in Section 4. The security analysis is in Section 5. Finally, we give our conclusion in the last section.

2. **Review of Chen et al.'s Scheme.** In this section, we briefly introduce Chen et al.'s scheme [5]. The notations used in their scheme are summarized as the following:

U: the user
ID: the identity of U
PW: the password of U
S: the remote server
x: the secret key maintained by the server
$h(\,)$: a cryptographic un-keyed one-way hash function
$h_p(\,)$: a cryptographic keyed one-way hash function with a secret key p
$\rightarrow$: a common channel
$\dashrightarrow$: a secure channel
$||$: string concatenation operation
$\oplus$: exclusive-or operation

2.1. **Registration phase.** Assume a user U wants to register to a server S. U computes the value $h(b \oplus PW)$ where b is a random number selected by U and PW is the password of U. Then, the user U sends her/his identity ID and $h(b \oplus PW)$ to the server via a secure channel. If the server S accepts the request, it computes $p = h(ID \oplus x)$, $R = p \oplus h(b \oplus PW)$, and $V = h_p(h(b \oplus PW))$ and gives U a smart card containing V, R, $h(\,)$, and $h_p(\,)$. When U receives the smart card, she/he enters b into the smart card that contains V, R, b, $h(\,)$, and $h_p(\,)$.

2.2. **Login and verification phase.** When U wants to login to the server, she/he inserts her/his smart card and inputs her/his ID and PW. The smart card computes $p = R \oplus h(b \oplus PW)$ and $V' = h_p(h(b \oplus PW))$, and then checks whether V' is equal to V; if not, it rejects U's login. Otherwise, it generates a random number r and computes $C_1 = p \oplus h(r \oplus b)$ and $C_2 = h_p(h(r \oplus b)||T_u)$, where T_u is the current timestamp of U. Then, it sends the message $\{ID, C_1, C_2, T_u\}$ to the server S.

After receiving the message from U at time T_s, the server S reject U's request if ID is invalid or $T_s - T_u > \Delta T$, where ΔT is the predetermined time interval for message traveling. Then, S computes $p' = h(ID \oplus x)$, ${C_1}' = p' \oplus C_1$, ${C_2}' = h_{p'}({C_1}'||T_u)$ and checks whether ${C_2}'$ is equivalent to the received C_2. If it fails, S rejects U's login request. Otherwise, it accepts U's request and, then, computes and sends the message $\{T_s, C_3\}$ to U where $C_3 = h_{p'}({C_1}' \oplus T_s||p')$. Upon receiving the message from S, U checks the validity of T_s. If T_s is invalid or $T_u = T_s$, U terminates the session. Otherwise, U computes ${C_3}' = h_p(h(r \oplus b) \oplus T_s||p)$ and checks whether ${C_3}'$ is equivalent to the received C_3. If it fails, U terminates the session. Otherwise, U successfully authenticates S and uses $h(r \oplus b)$ as the session key, a short-term secrecy.

3. **Cryptanalysis of Chen et al.'s Scheme.** Chen et al.'s scheme is still vulnerable to the offline password-guessing attack as reported in [6,7]. An attacker can perform offline password-guessing successfully using the contents of a user smart card. Assume that an attacker A gets the values V, R, and b from U's lost smart card, then A can perform offline password-guessing attack to derive U's password PW using the formula $R = p \oplus h(b \oplus PW)$ and $V = h_p(h(b \oplus PW))$. If succeed, the attacker can derive both the user password PW and the shared secret p, shared between the user and the server, at the same time. As a result, the attacker can forge the user to login into the server

successfully. In addition to the offline password-guessing attack, we also find that Chen et al.'s scheme does not provide perfect forward secrecy. If the user's long-term password PW is revealed, then the shared secret p, where $p = R \oplus h(b \oplus PW)$, can be computed using PW and the values R and b extracted from the smart card. Using p and the value C_1 in an intercepted old message, attackers can compute the corresponding old session key $h(r \oplus b)$ using $h(r \oplus b) = p \oplus C_1$. In other words, once the server's long-term secret key x is compromised, it will reveal all the old short-term keys used before. In order to avoid the above offline password guessing and other attacks, we propose a new scheme using users' biometrics such as fingerprints, to improve the security of remote mutual authentication and key agreement.

4. Our Improved New Scheme.

In this section, we propose a remote mutual authentication and key agreement scheme using smart card with biometrics and secure one-way hash function. In our scheme, we do not use keyed hash function. Besides, we use both timestamps and challenge/response to avoid reply attack. Our scheme consists of four phases: the registration phase, the login phase, the verification phase, and the password change phase. The symbols in our scheme are defined as Chen et al.'s scheme and f is the biometric template of a user such as a fingerprint.

4.1. Registration phase.

Our registration phase is partially the same as that of Chen et al.'s scheme. Assume a user U wants to register to a server S. U computes the value $h(f||b \oplus PW)$ where b is a random number selected by U, PW is the password of U, and f is the fingerprint template of U. Then, the user U sends her/his identity ID and $h(f||b \oplus PW)$ to the server for registration via a secure channel. If the server S accepts the request, it computes $p = h(ID \oplus x)$ and $R = p \oplus h(f||b \oplus PW)$ and sends U a smart card containing R and $h(\,)$ via a secure channel. When U receives the smart card, she/he enters b and PW into the smart card and uses a biometrics reader to input her/his fingerprint template f. The smart card computes $p = R \oplus h(f||b \oplus PW)$ and $V = h(p||f)$ and saves b and V into the smart card to activate the card. As such, the smart card contains V, R, b and $h(\,)$. The registration phase of our scheme is shown in Figure 1.

4.2. Login phase.

When U wants to login to the server, she/he inserts her/his smart card into a card reader and inputs her/his ID and PW. Then, she/he uses a fingerprint reader to input her/his fingerprint template f. The smart card computes $p = R \oplus h(f||b \oplus PW)$ and $V' = h(p||f)$, and then checks whether V' is equal to V. If not equal, it rejects U's login. Otherwise, it generates a random number r and computes $C_1 = h(p||T_u||r)$, where T_u is the current timestamp and the challenge nonce of U. Then, it sends the login message $\{ID, T_u, r, C_1\}$ to the server S. The login phase of our scheme is shown in Figure 1.

4.3. Verification phase.

As shown in Figure 1, after receiving the message from U at time T_s, the server S checks the format of ID and the freshness of T_u. Reject U's request if ID is invalid or the difference between T_s and T_u is greater than the predetermined time interval T for message traveling. Then, S computes $p' = h(ID \oplus x)$, $C_1{}' = h(p'||T_u||r)$ and checks whether $C_1{}'$ is equivalent to the received C_1. If it fails, S rejects U's login request. Otherwise, it accepts U's request and computes and sends the message $\{C_2\}$ to U where $C_2 = h(T_u||r||p')$. C_2 is both a message authentication code and a response, corresponding to the challenge nonce T_u. Upon receiving the message from S, the smart card computes $C_2{}' = h(T_u||r||p)$ and checks whether $C_2{}'$ is equivalent to the received C_2. If $C_2{}' \neq C_2$, the smart card terminates the session. Otherwise, it uses $h(r||p||T_u)$ as the session key, a short-term secret key, for the communication in the session. The verification phase of our scheme is shown in Figure 1.

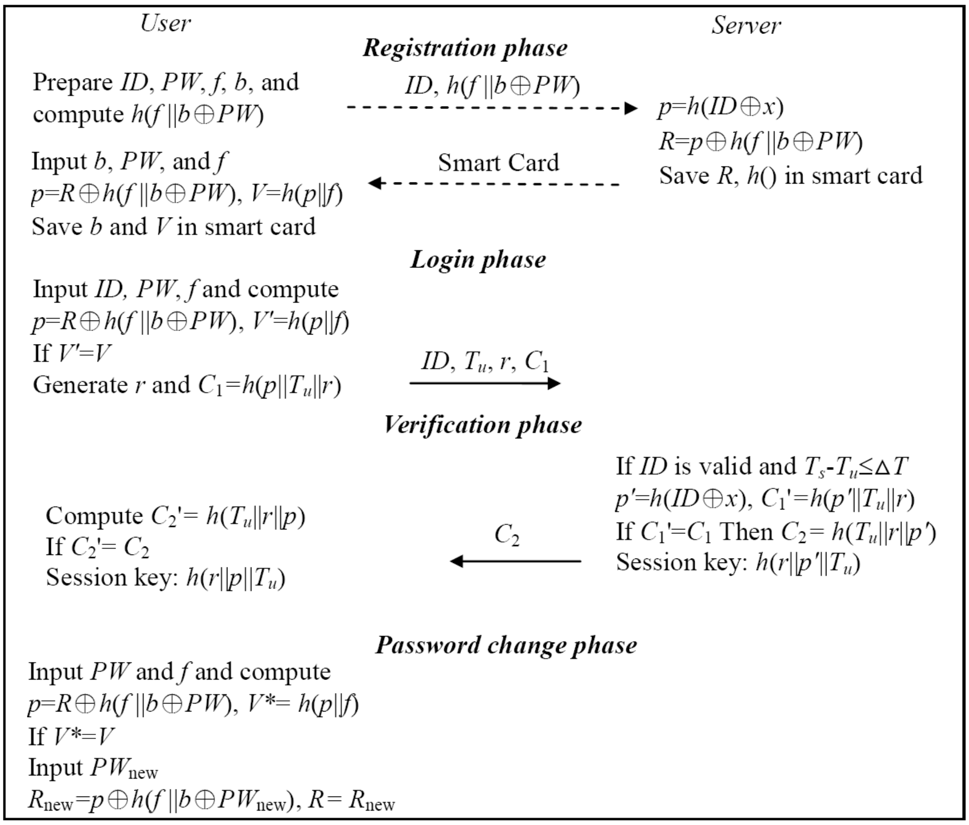
User
Server
Registration phase
Prepare ID, PW, f, b, and compute $h(f||b \oplus PW)$
$ID, h(f||b \oplus PW)$
$p=h(ID \oplus x)$
$R=p \oplus h(f||b \oplus PW)$
Save R, $h()$ in smart card
Smart Card
Input b, PW, and f
$p=R \oplus h(f||b \oplus PW)$, $V=h(p||f)$
Save b and V in smart card
Login phase
Input ID, PW, f and compute
$p=R \oplus h(f||b \oplus PW)$, $V'=h(p||f)$
If $V'=V$
Generate r and $C_1=h(p||T_u||r)$
ID, T_u, r, C_1
Verification phase
If ID is valid and T_s-$T_u \leq \Delta T$
$p'=h(ID \oplus x)$, $C_1'=h(p'||T_u||r)$
If $C_1'=C_1$ Then $C_2=h(T_u||r||p')$
Session key: $h(r||p'||T_u)$
C_2
Compute $C_2'=h(T_u||r||p)$
If $C_2'=C_2$
Session key: $h(r||p||T_u)$
Password change phase
Input PW and f and compute
$p=R \oplus h(f||b \oplus PW)$, $V^*=h(p||f)$
If $V^*=V$
Input PW_{new}
$R_{\mathrm{new}}=p \oplus h(f||b \oplus PW_{\mathrm{new}})$, $R=R_{\mathrm{new}}$

FIGURE 1. Our proposed remote user authentication using smart card scheme

4.4. **Password change phase.** When the user U wants to change her/his password from PW to PW_{new}, U inputs PW and f into her/his smart card through a smart card reader and a fingerprint reader correspondingly. The smart card computes $p = R \oplus h(f||b \oplus PW)$ and $V^* = h(p||f)$ and then checks whether V^* is equivalent to the stored V. If not equal, the smart card rejects the request. Otherwise, U enters the new password PW_{new}. The smart card computes $R_{new} = p \oplus h(f||b \oplus PW_{new})$ and uses R_{new} to replace R. The password change phase of our proposed scheme is shown in Figure 1.

5. **Security Analysis.** In this section, we analyze the security of our scheme as the following.

A. The server's secret key x and the shared secret p are secure. The server's secret key x is protected by the secure one-way hash function $h(\,)$. It is computationally infeasible to derive x from the value $h(ID \oplus x)$. In the same way, the shared secret $p = h(ID \oplus x)$, shared between U and the server, cannot be derived from $V = h(p||f)$, stored in the smart card, or from $C_1 = h(p||T_u||r)$ and $C_2 = h(T_u||r||p') = h(T_u||r||p)$ in the transmitted messages. Besides, instead of p, only the ciphertext R of p is stored in the smart card, encrypted by $h(f||b \oplus PW)$ as $R = p \oplus h(f||b \oplus PW)$. No one can derive p from R without knowing both the fingerprint template f and the password PW at the same time.

B. Session key partial forward secrecy is achieved. Session keys in our scheme are computed, using the shared secret p, as $h(r||p||T_u)$. As given above, no one can derive p from $R = p \oplus h(f||b \oplus PW)$ without knowing both the fingerprint template f and the password PW at the same time. That is, even if the user password PW is revealed, the shared secret p is still secure. Therefore, any old session key, $h(r||p||T_u)$, is still secure even if the long term user password PW is revealed. Note that, we call this property partial forward secrecy because it is achieved only when the long term secret x remains to be a secret.

C. Offline password guessing is impossible in our scheme. We design the shared secret p, in the formula $V = h(p||f)$, to be computed from $p = R \oplus h(f||b \oplus PW)$, instead of $p = R \oplus h(b \oplus PW)$. Thus, both f and PW in the formula $V = h(p||f) = h(R \oplus h(f||b \oplus PW)||f)$ are unknown to the attacker. Since the attacker cannot guess both f and PW at the same time, V in the smart card will not become the comparison target, for testing if $V' = V$ holds in the login phase or password change phase, required in an offline password guessing attack. Similarly, we can see that C_1 and C_2 will not become the comparison targets for offline password guessing. Again, for the same reasons, both f and PW are unknown to the attacker, in the formula $C_1 = h(p||T_u||r) = h(R \oplus h(f||b \oplus PW)||T_u||r)$ and $C_2 = {C_2}' = h(T_u||r||p) = h(T_u||r||R \oplus h(f||b \oplus PW))$.

D. Replay attacks are impossible in our scheme. The server checks the freshness of timestamp T_u to avoid the replay of the login message $\{ID, T_u, r, C_1\}$ while the smart card uses the challenge/response approach to detect any replay of the message $\{C_2\}$ from the server. The values T_u and r, as challenges, are fresh if they pass the check by the server. The value C_2, as a response, includes T_u and r in its calculation. That is, $C_2 = h(T_u||r||p')$. Note that the smart card and the server will not generate repeat challenges and responses due to the timestamp T_u and the random number r. Especially, timestamps will never repeat due to the different combination of year, month, day, hour, minute, and second in each timestamp. In addition, C_1 and C_2, as message authentication codes, guarantee the integrity of the contents of the transmitted messages. It is impossible to create C_1 and C_2 without knowing the shared secret value p. Therefore, replay attacks are eliminated.

E. Mutual authentication between the user U and the server is achieved. Using the timestamp and challenge/response approach to prevent replay attackers, U and the server can authenticate each other now by checking the message authentication codes C_2 and C_1, respectively. Since no one can create the correct authentication codes C_2 and C_1 without knowing the shared secret value p, p is used to confirm the legitimacy of each party while PW and f are used to confirm the legitimacy of U. In other words, it is infeasible for an intruder or a pretended server to masquerade as a legal party.

6. **Conclusion.** In this paper, we review the weaknesses of Chen et al.'s remote user authentication scheme. In their scheme, when the contents of user's smart card are revealed, an attacker can perform an offline password-guessing attack to derive weak user password, and then forge the user to login into the server successfully. In addition, when the user password PW, which is a long-term secret, in their scheme is compromised, we show that all the used session keys, which are short-term secrets, will be revealed. That is, Chen et al.'s authentication scheme does not satisfy the property of perfect forward secrecy. In order to avoid the above offline password guessing attack, we propose a new scheme that uses the user's biometrics such as fingerprints, faces, and irises, to provide more reliable identification information to solve the problems caused by smart card content leakage and non-secure network. Our scheme does not increase much computation cost while providing a framework for mutual authentication and key agreement with partial forward secrecy. We plan in the future to implement the perfect forward secrecy for a more secure scheme. The use of the biometric information for more general authentication activity also belongs to our future plan.

REFERENCES

[1] L. Lamport, Password authentication with insecure communication, *Communications of the ACM*, vol.24, pp.770-772, 1981.

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

[3] A. K. Das, Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards, *Information Security*, vol.5, pp.145-151, 2011.

[4] S. K. Sood, A. K. Sarje and K. Singh, A secure dynamic identity based authentication protocol for multi-server architecture, *Journal of Network and Computer Applications*, vol.34, pp.609-618, 2011.

[5] T.-H. Chen, H.-C. Hsiang and W.-K. Shih, Security enhancement on an improvement on two remote user authentication schemes using smart cards, *Future Generation Computer Systems*, vol.27, pp.377-380, 2011.

[6] S. Kumari, M. K. Gupta and M. Kumar, Cryptanalysis and security enhancement of Chen et al.'s remote user authentication scheme using smart card, *Central European Journal of Computer Science*, vol.2, pp.60-75, 2012.

[7] Q. Jiang, J. Ma, G. Li and Z. Ma, An improved password-based remote user authentication protocol without smart cards, *Information Technology and Control*, vol.42, pp.150-158, 2013.

[8] M. Sarvabhatla, M. Giri and C. S. Vorugunti, A secure biometrics-based remote user authentication scheme for secure data exchange, *International Conference on Embedded Systems*, pp.110-115, 2014.

[9] V. Odelu, A. K. Das and A. Goswami, An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card, *Journal of Information Security and Applications*, vol.21, pp.1-19, 2015.

[10] J. Jung, D. Lee, J. Kim, Y. Lee, D. Kang and D. Won, Cryptanalysis and improvement of efficient password-based user authentication scheme using hash function, *The 10th International Conference on Ubiquitous Information Management and Communication*, Danang, Vietnam, 2016.